MAGNET FORENSICS
DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") applies to the extent that Magnet Forensics Processes Personal Data on your ("Customer") behalf in the course of providing Services to Customer in connection with a Magnet Forensics product ("Magnet Product"). For certainty, this DPA does not apply to the extent that Magnet Forensics is the Controller of personal data. This DPA serves as a modification to the Agreement, and the Magnet Forensics entity that is party to such Agreement is party to this DPA and designated "Magnet Forensics". In the event of a conflict or ambiguity between: (a) any provision contained in this DPA and the terms of the Agreement, the terms of this DPA shall prevail with respect to the subject matter of this DPA; and (b) any provisions contained in the body of this DPA and any provision contained in Appendix 2, the provisions in Appendix 2 will prevail.

All terms not otherwise defined in this DPA shall have the meanings ascribed to them in the Agreement. Any words following the words "include", "includes", "including", "in particular" or any similar words or expressions will be construed without limitation and accordingly will not limit the meaning of the words preceding them.

"Agreement"	Magnet Forensics End User License Agreement or such other terms the Customer has agreed to with Magnet Forensics for the use of a Magnet Product.
"Agreement Personal Data"	Personal Data which is to be processed under the Agreement on behalf of the Customer.
"Data Protection Laws"	means all data protection and privacy laws applicable to the Processing of Personal Data, including, where applicable, European Data Protection Law; and references to **"Controller"**, **"Data Subjects"**, **"Personal Data"** and **"Processor"** have the meanings set out in and will be interpreted in accordance with such laws.
"Data Protection Supervisory Authority"	any regulatory authority responsible for the enforcement, regulation or governance of any Data Protection Laws and any replacement or successor body or person for any such authority from time to time.
"**Data Transfer Agreement**"	means: (i) Module 2 (Controller to Processor) of the EU SCCs; and (ii) the ICO's International Data Transfer Addendum to the EU SCCs, which are set out at Appendix 2 of this DPA.
"**EU SCCs**"	means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
"European Data Protection Law"	means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data ("General Data Protection Regulation" or "GDPR") and associated national laws, and (ii) the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Addendum etc.) (EU Exit) Regulations 2019 ("UK GDPR"), together with the Data Protection Act 2018; in each case as may be amended or replaced from time to time.

"Personal Data Security Incident"	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Agreement Personal Data transmitted, stored or otherwise processed.
"Processing"	has the meaning set out in the Data Protection Laws; and for the purposes of Section 0 "**process**", "**processing**" and "**processed**" will be interpreted accordingly.
"Restricted Transfer"	a transfer of Agreement Personal Data which is undergoing processing or which is intended to be processed after transfer, to a country or territory to which such transfer is prohibited or subject to a requirement to take additional steps to adequately protect the Agreement Personal Data for the transfer to be lawful under the Data Protection Laws.
"Services"	the services provided to Customer by Magnet Forensics in connection with a Magnet Product pursuant to the Agreement.
"Sub-Processor"	any third party (including any Magnet Forensics group company and authorised subcontractor) appointed, engaged or permitted by Magnet Forensics to process Agreement Personal Data.

1. DATA PROTECTION

1.1 The Customer authorises Magnet Forensics to process the Agreement Personal Data during the term of the Agreement as a Processor for the purpose of providing the Customer with Services. The subject matter, duration, nature and purpose of the processing are set out in Appendix 1.

1.2 Customer warrants to Magnet Forensics that:

1.2.1 it has all necessary rights to authorise Magnet Forensics to process Agreement Personal Data in accordance with this Agreement and the Data Protection Laws; and

1.2.2 its instructions to Magnet Forensics relating to processing of Agreement Personal Data will not put Magnet Forensics in breach of Data Protection Laws, including with regard to Restricted Transfers.

1.3 If Magnet Forensics considers that any instructions from the Customer relating to processing of Agreement Personal Data may put Magnet Forensics in breach of Data Protection Laws, Magnet Forensics will be entitled not to carry out that processing and will not be in breach of this DPA or the Agreement or otherwise liable to the Customer as a result of its failure to carry out that processing.

1.4 The Customer will comply with the Data Protection Laws in respect of Agreement Personal Data.

1.5 Magnet Forensics may use Sub-Processors from time to time, including, without limitation, affiliates of Magnet Forensics, and Customer authorises Magnet Forensics to engage such Sub-Processors. Magnet Forensics will inform Customer of any intended changes concerning the addition or replacement of Sub-Processors, thereby giving Customer the opportunity to object to such changes. If the Customer objects to such a change and such objection cannot be resolved by the parties within ten (10) days, Customer will be entitled to terminate the Agreement upon written notice to Magnet Forensics.

1.6 If Magnet Forensics appoints a Sub-Processor, Magnet Forensics will enter into an agreement with the Sub-Processor that specifies the Sub-Processor's processing activities and imposes on the Sub-Processor similar (in substance) terms to those imposed on Magnet Forensics in this Section 1.

1.7 Magnet Forensics will:

1.7.1 process the Agreement Personal Data only on documented instructions from the Customer (unless Magnet Forensics or the relevant Sub-Processor is required to process Agreement Personal Data to comply with applicable law, in which case Magnet Forensics will notify the Customer of such legal requirement prior to such processing (unless prohibited from doing so)). For the purpose of this Section 1.7.1, the obligations on Magnet Forensics to perform the Services, and/or afford Customer use of the functionality thereof, are documented instructions from the Customer;

1.7.2 ensure that any Magnet Forensics personnel authorised to process Agreement Personal Data are subject to confidentiality obligations or are under an appropriate statutory obligation of confidentiality;

1.7.3 Magnet Forensics shall delete any Agreement Personal Data stored in its servers after the end of the provision of Services relating to processing. Magnet Forensics will be entitled to retain any Agreement Personal Data which it has to keep to comply with any applicable law or which it is required to retain for accounting purposes and/or record-keeping purposes. Notwithstanding the foregoing, Magnet Forensics may retain and process certain de-identified data relating to the Customer's use of the Services for benchmarking and product development purposes.

1.7.4 implement appropriate technical and organisational measures to protect the Agreement Personal Data, in accordance with the Agreement;

1.7.5 notify the Customer without undue delay after becoming aware of a Personal Data Security Incident;

1.7.6 taking into account the nature of processing and the information available to Magnet Forensics, provide reasonable assistance to the Customer (at the Customer's cost) in relation to the Customer's obligations under the Data Protection Laws relating to:

1.7.6.1 the security of processing Agreement Personal Data;

1.7.6.2 responding to requests for exercising Data Subjects' rights under the Data Protection Laws, including by appropriate technical and organisational measures, insofar as this is possible;

1.7.6.3 documenting any Personal Data Security Incidents and reporting any Personal Data Security Incidents to any Data Protection Supervisory Authority and/or Data Subjects; and

1.7.6.4 conducting privacy impact assessments of any processing operations and consulting with Data Protection Supervisory Authorities, Data Subjects and their representatives accordingly.

1.7.7 on written request, make available to the Customer all information reasonably necessary to demonstrate compliance with the obligations set out in this Section 1 and

allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer, provided that the Customer gives Magnet Forensics at least thirty (30) days' prior written notice of each such audit and that each audit is carried out at the Customer's cost, during business hours, so as to cause the minimum disruption to Magnet Forensics' business and without the Customer or its auditor having any access to any data belonging to a person other than the Customer. Any materials disclosed during such audits and the results of and/or outputs from such audits or information-gathering will be kept confidential by the Customer.

1.8 The Customer hereby authorises Magnet Forensics to make a Restricted Transfer in respect of the Agreement Personal Data, as necessary to provide the Services. Magnet Forensics will demonstrate or implement an appropriate safeguard for that Restricted Transfer in accordance with Data Protection Laws. Such appropriate safeguards may include:

1.8.1 that the country or territory to which the Restricted Transfer is to be made ensures an adequate level of protection for processing of Personal Data pursuant to a valid adequacy decision made in accordance with Data Protection Laws; or

1.8.2 appropriate safeguards in accordance with Data Protection Laws. On request, the Customer will execute any documents (including EU SCCs for the transfer of personal data to Processors established in third countries) relating to that Restricted Transfer which the relevant Processor requires it to execute from time to time.

1.9 The Parties acknowledge and agree that certain Personal Data, the processing of which is subject to European Data Protection Laws ("**European Personal Data**") may be shared by Magnet Forensics with Magnet Forensics USA Inc. ("**Magnet US**") to assist with the provision of the Services to the Customer. Any Restricted Transfer of European Personal Data to Magnet US (whether transferred directly by the Customer to Magnet US or made available by Magnet Forensics to Magnet US) shall be governed by the Data Transfer Agreement set out in Appendix 2, which the Customer enters into with Magnet US by signing up to the Agreement and this DPA.

1.10 For the avoidance of doubt, the obligations on Magnet Forensics under Section 1.8 will not apply in circumstances where the Customer processes or is processing the Agreement Personal Data outside the European Economic Area and/or United Kingdom (as applicable).

1.11 The qualifications at Section 1.8 will not apply if Magnet Forensics or the relevant Sub-Processor is required to make a Restricted Transfer to comply with European Union law or European Union member state law or United Kingdom law to which Magnet Forensics is subject, in which case Magnet Forensics will notify the Customer of such legal requirement prior to such Restricted Transfer unless such law prohibits notice to the Customer on public interest grounds.

Appendix 1: Description of Processing

Subject matter: Provision of the Magnet Forensics Services.

Duration of the processing: For the duration that the Customer is authorized to access the Services.

Nature and purpose of the processing: To enable Magnet Forensics to provide the Services.

Type of personal data: Personal data contained in any data collected and/or uploaded as part of the Customer's use of the Services. This may include names, contact details, email correspondence, images, and other personal data.

Categories of data subjects: Data subjects whose personal data is collected and/or uploaded by the Customer as part of the Services. This may include employees or business contacts of the Customer's end-customer.

Appendix 2: Data Transfer Agreement

The Parties acknowledge and agree that European Personal Data (hereinafter, "**Personal Data**") may be processed by Magnet Forensics USA Inc., (the "**data importer**") to assist with the provision of the Services under the Agreement to the Customer (the "**data exporter**"). Accordingly, to legitimise the Restricted Transfer of Personal Data from the data exporter to the data importer, the data importer and data exporter are entering into this Data Transfer Agreement which comprises: (a) Module Two (Controller to Processor) of the EU SCCs (as set out in Part One); and (b) the UK Addendum to the EU SCCs (as set out in Part Two). The Parties agree that this Data Transfer Agreement ("Clauses") shall only apply if and to the extent the Personal Data is processed by Magnet Forensics USA Inc., on behalf of the Customer.

Part One: EU SCCs (Controller to Processor)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) 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 Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update

information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) 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) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause – Not used

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons

for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. 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 Clause 14, in particular the requirement for the data importer under Clause 14(e) 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 under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) 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 authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular 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.

8.7 Sensitive data

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 Annex I.B.

8.8 Onward transfers

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 (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 benefitting 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 defence 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.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The 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.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) 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 sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) 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 Annex II the appropriate technical and organisational 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.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) 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 authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) 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.

(c) 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 pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) 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.

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

(f) 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 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) 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.

(c) Notwithstanding paragraph (b), the data exporter 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 exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) 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.

(e) 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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.

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

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2), the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices 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 and practices 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) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its 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.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation.The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If 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. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the 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; or

(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.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the

documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) 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.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

(b) 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. This is without prejudice to Clause 14(f).

(c) 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 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.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) 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.

(e) 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

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Republic of Ireland.

(c) 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.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The relevant ”Customer” that will receive Services under the Agreement, whose details are as set out in the Quote issued by Magnet Forensics for the Services (“Quote”)

Address: As stated on the Quote

Contact person’s name, position and contact details: As set out on the Quote

Activities relevant to the data transferred under these Clauses: To facilitate support tickets and/or to confirm license key usage in connection with Services

Role (controller/processor): Controller

Data importer(s):

Name: Magnet Forensics USA Inc.

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

Contact details: dpo@magnetforensics.com

Activities relevant to the data transferred under these Clauses: To facilitate support tickets and/or to confirm license key usage in connection with Services

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred

Data subjects whose personal data is collected and/or uploaded by the Customer as part of the Services. This may include employees or business contacts of the Customer's end-customer.

2. Categories of personal data transferred

Personal data contained in any data collected and/or uploaded as part of the exporter's use of the Services. This may include names, contact details, email correspondence, images, and other personal data.

3. Sensitive data transferred and applicable restrictions of safeguards

N/A

4. The frequency of the transfer

Continuous transferring of Personal Data to assist with the ongoing provision of Services to the data exporter

5. Nature of the processing

Provision of digital forensics software and services

6. Purpose of the data transfer and further processing

For the importer to assist Magnet Forensics with the provision of digital forensic services to the exporter

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

Personal Data shall be retained by the data importer for the duration of the services, unless otherwise agreed with the data exporter

8. Sub-processing

Details of any sub-processing are set out in Annex III.

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

ACQUISITION, DEVELOPMENT AND MAINTENANCE OF IT SYSTEMS

Application Development Security

Our application development lifecycle follows industry recognized SDLC frameworks. Additionally, we have a Secure Development Policy as a component of our ISO 27001 implementation. Controls employed include, but are not limited to, monitoring security vulnerabilities, code security reviews, approval of pre-rollout changes, and software developer training on secure software development practices.

Security Test on Applications and Operations Infrastructures

We test the security of our applications at least annually through external penetration testing, and at least quarterly through automated application vulnerability scanning and whenever a major security infrastructure change is being considered.

These tests include vulnerability and intrusion scanning and are carried out by qualified staff or third parties (where applicable) according to recognized testing standards.

Management of Security Patches and Vulnerabilities

We follow a defined process for managing and implementing security patches to combat vulnerabilities with our applications and products, based on recognized industry standards. We use up-to-date supported technologies and software that are supplied by top-tier providers. We take appropriate action to identify and prevent the exploitation of vulnerabilities.

Detection and Removal of Malware

We implement prevention, mitigation, detection and recovery measures to protect against malware.

Vendor Management

We perform security testing validation on vendor-supplied systems before implementation, and at regular intervals to ensure we are using secure and robust systems.

MANAGEMENT OF INFORMATION SECURITY INCIDENTS

Information Security Incidents

We have a defined and implemented process for managing information security incidents. The process is based on the norms and standards recognized in the field of information security incident management. If customer data is involved in a security incident, we take steps to notify customers in a timely fashion after the security incident is detected

Part Two: UK Addendum to the EU SCCs

Date of this Addendum:

1. The Clauses are dated on the date the Agreement was signed. This Addendum is effective from the date stated on page one of the Agreement.

Background:

2. The Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the EU SCCs those terms shall have the same meaning as in the EU SCCs. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
UK	The United Kingdom of Great Britain and Northern Ireland

4. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.

5. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.

6. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy:

7. In the event of a conflict or inconsistency between this Addendum and the provisions of the EU SCCs or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

Incorporation of the Clauses:

8. This Addendum incorporates the EU SCCs which are deemed to be amended to the extent necessary so they operate:

8.1 for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and

8.2 to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR.

9. The amendments required by Section 7 above, include (without limitation):

9.1 References to the "Clauses" means this Addendum as it incorporates the Clauses

9.2 Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer."

9.3 References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws.

9.4 References to Regulation (EU) 2018/1725 are removed.

9.5 References to the "Union", "EU" and "EU Member State" are all replaced with the "UK"

9.6 Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;

9.7 Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".

9.8 Clause 18 is replaced to state:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."

9.9 The footnotes to the Clauses do not form part of the Addendum.

Amendments to this Addendum:

10. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.

11. The Parties may amend this Addendum provided it maintains the appropriate safeguards required by Article 46 UK GDPR for the relevant transfer by incorporating the EU SCCs and making changes to them in accordance with Section 7 above.