HACKERONE DATA PROCESSING ADDENDUM

THIS HACKERONE DATA PROCESSING ADDENDUM ("DPA") is entered into and made effective as of the date of the last signature below, (the "**Effective Date**"), by and between: _____ incorporated in _____ with registration number (if applicable) _____ and an address at _____ ("**Customer**") and HackerOne Inc. ("**HackerOne**"), a Delaware corporation with an address at 548 Market Street, PMB 24734, San Francisco, CA 94104, United States. Each of Customer and HackerOne may be referred to herein as a "**party**" and together as the "**parties**".

The parties confirm that this DPA has been executed by its duly authorized representatives set out below.

On behalf of the Data Exporter (legal entity identified as "Customer") in the DPA:

Name (written out in full):

Position: Authorized Signatory

Address:

Date:

Signature:

On behalf of the Data Importer (legal entity identified as "HackerOne") in the DPA:

Name (written out in full): Ilona Cohen

Position: Authorized Signatory

Address: 548 Market Street, PMB 24734, San Francisco, CA 94104, United States

Date: 04/27/26

Signature: DocuSigned by: Ilona Cohen 3D48C7937169405...

This DPA has been pre-signed on behalf of HackerOne. By completing this DPA and sharing it with HackerOne by email to dpa@hackerone.com., Customer agrees that this DPA will be validly executed by the parties and binding on the Customer and any of its successors and assigns.

RECITALS

(A) HackerOne provides to Customer certain services ("**Services**") pursuant to one or more separate agreement(s) between the parties (each an "**Agreement**"**)**. In connection with the Services, the parties anticipate that HackerOne may from time to time process certain Personal Data in respect of which the Customer or any member of the Customer Group (as defined below) may be a controller under Data Protection Laws.

(B) The parties have agreed to enter into this **DPA** in order to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data as required by the Data Protection Laws.

1. Definitions

1.1 The following terms are used in this DPA:

(a) "**Adequate Country**" means a country or territory that is recognized under Data Protection Laws from time to time as providing adequate protection for Personal Data;

(b) "**Affiliate**" means with respect to a party, any corporate entity that directly or indirectly, Controls, is Controlled by, or is under Common Control with such party (but only for so long as such Control exists);

(c) "**Customer Group**" means Customer and any of its Affiliates;

(d) "**Data Protection Laws**" means all data protection and privacy laws applicable to any Personal Data processed under or in connection with this agreement, including, without limitation, all privacy laws and regulations of the European Union, the

EEA and their member states, Switzerland and the United Kingdom applicable to any Personal Data processed under or in connection with this DPA, including, without limitation, the General Data Protection Regulation 2016/679 (the "GDPR"), UK Data Protection Act 2018 and UK GDPR (as defined in the Data Protection Act), the Privacy and Electronic Communications Directive 2002/58/EC (as the same may be superseded by the Regulation on Privacy and Electronic Communications, ("ePrivacy Regulation")), all national legislation implementing or supplementing the foregoing and all associated codes of practice and other guidance issued by any applicable data protection authority, and the California Consumer Privacy Act of 2018 ("CCPA"), all as amended, re- enacted and/or replaced and in force from time to time;

(e) "**Data Subject Request**" means a request from or on behalf of a data subject relating to access to, or rectification, erasure or data portability in respect of that person's Personal Data or an objection from or on behalf of a data subject to the processing of its Personal Data;

(f) "**EEA**" means European Economic Area;

(g) "**HackerOne Group**" means HackerOne and any of its Affiliates;

(h) "**SCCs**" means Module 2 of the standard contractual clauses approved by the European Commission pursuant to implementing Decision (EU) 2021/914, which as a result of this DPA is incorporated by reference;

(i) "**Personal Data**" means all data which is defined as 'Personal Data' under Data Protection Laws and which is provided by the Customer to HackerOne or accessed, stored or otherwise processed by HackerOne on behalf of Customer in HackerOne providing the Services;

(j) "**Restricted Transfer**" means the disclosure, grant of access or other transfer (as applicable), to HackerOne Group and: (a) is subject to the GDPR, and is transferred to a country or territory outside the EEA which is not an Adequate Country as declared by the European Commission (an "**EEA Restricted Transfer**"); (b) is subject to the FADP, and is transferred to a country or territory outside Switzerland which is not an Adequate Country as declared by the Swiss Government or Federal Data Protection and Information Commissioner ("**FDPIC**") (a "**Swiss Restricted Transfer**") and/or (c) is subject to the UK GDPR, and is transferred to a country or territory outside the UK which is not an Adequate Country as declared by the UK Government (a "**UK Restricted Transfer**"); and where such transfer would otherwise be prohibited under Chapter V of the GDPR.

(k) "**UK Addendum**" means the UK Addendum to the SCCs available at ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, issued by the UK Information Commissioner's Office (ICO) and which as a result of this DPA is incorporated by reference; or (b) where that addendum is superseded, such terms as are approved or issued by the ICO to replace it; and

(l) "**controller**", "**data subject**", "**processor**", and "**supervisory authority**" shall have the meanings ascribed to them in the Data Protection Laws.

1.2 An entity "**Controls**" another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract; and two entities are treated as being in "**Common Control**" if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

2. Status of the parties

The type of Personal Data processed pursuant to this DPA and the subject matter, duration, frequency, nature and purpose of the processing, retention periods of data and the categories of data subjects are as described below:

(a) **Subject Matter of the Processing**: HackerOne's provision of the Services to Customer.

(b) **Nature and Purpose of the Processing**: collection, analysis, storage, duplication, deletion, and disclosure as necessary to provide the Services and as may be further instructed by Customer in writing.

(c) **Duration and frequency of Processing**: HackerOne will process the Personal Data on a continuous basis for the duration of the Agreement, or until the data upon which processing is no longer necessary for the purposes of either party performing its obligations under the Agreement (to the extent applicable) unless otherwise agreed between the parties in writing.

(d) **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:** HackerOne will retain the Personal Data until the data is no longer necessary for the purposes of this DPA as set out under clause 2(b) above.

(e) **Types of Data**: data relating to individuals provided to HackerOne via the Services, by (or at the direction of) Customer which may include but is not limited to: name, phone number, job title, address, email address, location, username, password, personal data found in vulnerability information and IP addresses. Subject to further instructions by Customer and agreement as to 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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures, the Customer warrants that the transferred data will not include sensitive or special category personal data.

(f) **Categories of Data Subjects**: data subjects may include Customer's employees, contractors, agents, and affiliates about whom data is provided to HackerOne via the Services by (or at the direction of) Customer.

(g) **For transfers to (sub)processors:** the details of processing are as set out above in this clause 2 of the DPA.

2.2 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties acknowledge and agree that the Customer is the Controller and HackerOne is the Processor and accordingly HackerOne agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA.

2.3 Each party warrants in relation to Personal Data that it will comply (and will procure that any of its personnel comply), with the Data Protection Laws insofar as they are applicable to a controller (in the case of the Customer) or a processor (in the case of HackerOne). As between the parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data.

2.4 Each party shall appoint an individual within its organization authorized to respond from time to time to enquiries regarding the Personal Data and party shall deal with such enquiries promptly.

3. HackerOne obligations

3.1 With respect to all Personal Data, HackerOne shall:

(a) only process the Personal Data in order to provide the Services and shall act only in accordance with this DPA and (ii) the Customer's written instructions;

(b) in the event that applicable law requires HackerOne to process Personal Data other than pursuant to the Customer's instruction, HackerOne will notify the Customer (unless prohibited from so doing by applicable law);

(c) as soon as reasonably practicable upon becoming aware, inform the Customer if, in HackerOne's opinion, any instructions provided by the Customer under Clause 3.1(a) infringe the GDPR or UK GDPR;

(d) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out at https://www.hackerone.com/terms/security;

(e) take reasonable steps to ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under obligations of confidentiality;

(f) as soon as reasonably practicable upon becoming aware, notify the Customer of any actual or alleged material incident of unauthorized or accidental disclosure of or access to any Personal Data by any of its staff, sub-processors, or any other identified or unidentified third party (a "**Security Breach**");

(g) provide the Customer with reasonable cooperation and assistance in respect of a Security Breach as may be required to mitigate against the effects of, and comply with any reporting obligations which may apply in respect of, any such Security Breach;

(h) promptly notify the Customer if it receives a Data Subject Request. HackerOne shall not respond to a Data Subject Request received by HackerOne without the Customer's prior written consent except to acknowledge receipt of the request and/or to confirm that such request relates to the Customer to which the Customer agrees. To the extent Customer does not have the ability to address a Data Subject Request, HackerOne shall upon the Customer's request provide reasonable assistance to facilitate a Data Subject Request to the extent HackerOne is able to, consistent with applicable law, provided the Customer shall pay HackerOne's charges for providing such assistance, at HackerOne's then-current professional services rates;

(i) as soon as reasonably practicable following termination or expiry of the Agreement or completion of the Services, upon Customer's written request, , HackerOne will delete or return to the Customer (at the Customer's direction) all Personal Data (including copies) for which HackerOne is the Processor and that is processed pursuant to this DPA, save that this requirement shall not apply to the extent that Personal Data exists within back-ups where such data is put beyond practicable use and deleted in accordance with HackerOne's separate retention timeframes for archival media.

(j) provide such assistance as the Customer reasonably requests (taking into account the nature of processing and the information available to HackerOne) to Customer in relation to the Customer's obligations under Data Protection Laws with respect to:

(i) data protection impact assessments (as such term is defined in applicable Data Protection Laws);

(ii) notifications to the supervisory authority under Data Protection Laws and/or communications to data subjects by the Customer in response to any Security Breach; and

(iii) the Customer's compliance with its obligations under the applicable Data Protection Laws with respect to the security of processing,

provided the Customer shall pay HackerOne's charges for providing the assistance in clause 3.1(j), at HackerOne's then-current professional services rates.

(k) HackerOne acknowledges that it does not receive any Customer Personal Data as consideration for any products or services that HackerOne provides to Customer. HackerOne shall not sell any Customer Personal Data as the term "selling" is defined in the CCPA or similar or equivalent applicable privacy laws and agrees to refrain from any transfers of Customer Personal Data to or from a sub-processor that qualifies as "selling" under the CCPA or similar or equivalent privacy laws. Except as

strictly necessary to provide the Services to Customer: (i) HackerOne shall not collect, share or use any Customer Personal Data; and (ii) shall not have, derive or exercise any rights or benefits from Customer Personal Data.

4. Sub-processing

4.1 The Customer grants a general authorization (a) to HackerOne to appoint other members of HackerOne Group as sub-processors and (b) to HackerOne and other members of HackerOne Group to appoint third party data center operators, third party cloud services providers, and outsourced support providers as sub-processors to support the performance of the Services.

4.2 HackerOne will maintain a list of sub-processors at the following URL: https://www.hackerone.com/terms/subprocessors, will add the names of new and replacement sub-processors to the list prior to them starting sub-processing of Personal Data and shall provide a mechanism at such URL for Customer to obtain notice of such changes including any information necessary for the Customer to exercise its right to object. If the Customer has a reasonable objection to any new or replacement sub-processor, it shall notify HackerOne of such objections in writing within ten (10) days of the notification, and the parties will seek to resolve the matter in good faith. If HackerOne is reasonably able to provide the Services to the Customer in accordance with an Agreement without using the sub-processor and decides in its discretion to do so, then the Customer will have no further rights under this clause 4.2 in respect of the proposed use of the sub-processor. If HackerOne requires use of the sub-processor in its discretion and is unable to satisfy the Customer as to the suitability of the sub-processor or the documentation and protections in place between HackerOne and the sub-processor within sixty (60) days from the Customer's notification of objections, the Customer may within thirty (30) days of the end of the sixty (60) day period referred to above terminate the Agreement only in relation to the Services to which the proposed new sub-processor's processing of Personal Data relates or would relate by providing written notice to HackerOne having effect thirty (30) days after receipt by HackerOne. If the Customer does not provide a timely objection to any new or replacement sub-processor in accordance with this clause 4.2, Customer will be deemed to have consented to the sub-processor and waived its right to object. HackerOne may use a new or replacement sub-processor whilst the objection procedure in this clause 4.2 is in process.

4.3 HackerOne will ensure that any sub-processor it engages to provide an aspect of the Services on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Personal Data than those imposed on HackerOne in this DPA (the "**Relevant Terms**"). HackerOne shall procure the performance by such sub-processor of the Relevant Terms and shall be liable to the Customer for any breach by such person of any of the Relevant Terms.

5. Audit and records

5.1 HackerOne shall, in accordance with Data Protection Laws, make available to the Customer such information in HackerOne's possession or control as the Customer may reasonably request with a view to demonstrating HackerOne's compliance with the obligations set out in this DPA.

5.2 The Customer may exercise its right of audit under Data Protection Laws, through HackerOne providing:

(a) an audit report not older than 12 months by a registered and independent external auditor demonstrating that HackerOne's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard (such as ISO 27001 or SSAE 18 SOC 2); and

(b) additional information in HackerOne's possession or control to the UK Information Commissioner and/or an EU supervisory authority when it requests or requires additional information in relation to the data processing activities carried out by HackerOne under this DPA.

6. Data transfers

6.1 To the extent that performance of this DPA involves:

(a) an EEA Restricted Transfer, the parties shall comply with their respective obligations set out in the SCCs;

(b) a UK Restricted Transfer, the parties shall comply with their respective obligations set out in the SCCs, which are deemed to be varied to address the requirements of the UK GDPR in accordance with the UK Addendum; and/or

(c) a Swiss Restricted Transfer, the parties shall comply with their respective obligations set out in the SCCs, which are deemed to be varied to address the requirements of the revised Swiss Federal Act on Data Protection ("**FADP**") in accordance with clause 6.2(c) below.

The parties agree that data transfers may rely on any other specifically approved safeguards for data transfers (as recognized under the Data Protection Laws) and/or a competent authority's adequacy decision, provided that if the Services are covered by more than one transfer mechanism, the transfer of Personal Data will be subject to a single mechanism as agreed by the parties.

6.2 With respect to any SCCs entered into pursuant to clause 6.1 above:

(a) each of the parties is deemed to have signed the SCCs at the relevant signature block in Annex I to the Appendix to the SCCs, and Module Two of the SCCs applies to that Restricted Transfer. The parties agree that:

(i) in Clause 7, the 'Docking Clause' is not included;

(ii) For the purpose of clause 9(a) EU SCCs OPTION 2 shall apply with notification time period of 10 days;

(iii) in Clause 11, the optional language is not used;

(iv) For the purpose of clause 13(a) and Annex I.C. EU SCCs, if the data exporter is established in an EU Member State or has appointed a representative pursuant to Article 27(1) GDPR (which shall in each case be indicated in the details set out at the head of the DPA) then the competent supervisory authority shall be that of the country where the data exporter is established or where it has appointed such representative. Otherwise, if the data exporter is not established in an EU Member State and has not appointed a representative but the GDPR applies, the competent supervisory authority for the purpose of Clause 13 EU SCCs shall be Ireland;

(v) in Clause 17, 'OPTION 1' applies, and the parties agree that the SCCs shall be governed by the law of Ireland in relation to any EEA Restricted Transfer;

(vi) in Clause 18(b), the parties agree that any dispute arising from the SCCs in relation to any EEA Restricted Transfer shall be resolved by the courts of Ireland; and

(vii) Annex I to the SCCs is populated with the corresponding information set out in clause 2 with HackerOne a as 'data importer' and the Customer as 'data exporter'; and Annex II to the SCCs is populated with the details in clause 3.1(d) and

(b) the SCCs apply to any UK Restricted Transfers as varied by the UK Addendum in the following manner:

(i) 'Part 1 to the UK Addendum': (A) the parties agree Tables 1, 2 and 3 to the UK Addendum are deemed populated with the corresponding details set out in clause 2; and Table 4 to the UK Addendum is completed with 'Neither Party';

(ii) 'Part 2 to the UK Addendum': the parties agree to be bound by the UK Mandatory Clauses of the UK Addendum and that the SCCs shall apply to any UK Restricted Transfers as varied in accordance with those UK Mandatory Clauses. Where applicable, as permitted by section 17 of the UK Mandatory Clauses, the parties agree to the presentation of the information required by 'Part 1: Tables' of the UK Addendum in the manner determined by this clause 6.2(b); provided that the parties further agree that nothing in the manner of that presentation shall operate or be construed so as to reduce the Appropriate Safeguards (as defined in section 3 of the UK Mandatory Clauses);

(iii) in relation to any UK Restricted Transfer to which they apply in accordance with the UK Addendum, where the context permits and requires, any reference in the foregoing parts of this clause 6.2(a) to the SCCs, shall be read as a reference to those SCCs as varied in the manner set out in this Section 6.2(b) and

(c) the SCCs apply to any Swiss Restricted Transfers as varied in the following manner:

(i) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" in the EU SCCs shall be deemed to include Switzerland. This includes references to the court in a member state in Clause 18 c, that shall also include the Swiss courts as an alternative place of jurisdiction for data subjects residing in Switzerland;

(ii) References to "competent supervisory authority" and "supervisory authority" are to be considered the FDPIC;

(iii) References to "GDPR" "Regulation (EU) 2016/679", "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)" and "that Regulation" are to include the FADP. References to specific Article(s) of "Regulation (EU) 2016/679" are to include also the equivalent or more similar Article of the FADP;

(iv) References to the "European Commission" shall include Swiss competent authorities as well;

(v) To the extent the data transfer is exclusively subject to the FADP, reference to the governing law in clause 17 of the EU SCCs shall be referred to the FADP or the law of an EU country in accordance with the EU SCCs, provided that it allows and grants rights as a third-party beneficiary for contractual claims regarding data transfers; and

(vi) In Clause 18(b), the parties agree that any dispute arising from the SCCs in relation to any Swiss Restricted Transfer shall be resolved by the courts of Switzerland.

6.3 The Customer acknowledges and accepts that the provision of the Services under the Agreement may require the processing of Personal Data by sub-processors in countries outside the UK, Switzerland and EEA from time to time.

6.4 If, in the performance of this DPA, HackerOne transfers any Personal Data to a sub-processor (which shall include without limitation any Affiliates of HackerOne) and without prejudice to clause 4 where such sub-processor will process Personal Data outside the UK, Switzerland and EEA except if in an Adequate Country, HackerOne shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place such as:

(a) the requirement for HackerOne to execute or procure that the sub-processor execute on behalf of the Customer SCCs (or part of the SCCs); or

(b) the existence of any other specifically approved safeguard for data transfers (as recognized under the Data Protection Laws) and/or a European Commission finding of adequacy.

6.5 As between Customer and HackerOne, the limitations and exclusions of liability set out in the Agreement that govern the provision of Services by HackerOne Group to Customer (including reward services, and associated analytics and business services) apply to the SCCs and UK Addendum entered into (where applicable) by the parties, to the extent that such limitations and exclusions do not contradict or undermine the liability regime or allocation of responsibility anticipated by the SCCs and UK Addendum.

6.6 In addition to the SCCs and UK Addendum, the parties agree to comply with the supplementary clauses set out under **Exhibit A** attached.

7. General

7.1 This DPA is without prejudice to the rights and obligations of the parties under any Agreement which shall continue to have full force and effect and shall apply solely to the extent that there is an existing Agreement between the parties. In the event of any conflict between the terms of this DPA and the terms of any Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data. A material breach by HackerOne of this DPA shall be deemed a material breach of the Agreement.

7.2 To the extent there is an EEA or Swiss Restricted Transfer, the parties agree that in the event of any conflict or inconsistency between the DPA and the EU SCCs, the EU SCCs shall prevail. To the extent there is an UK Restricted Transfer, the parties agree that in the event of any conflict or inconsistency between the DPA, the EU SCCs and the UK Addendum, the UK Addendum shall prevail.

7.3 Save where indicated in the SCCs, this DPA does not confer any third-party beneficiary rights, it is intended for the benefit of the parties only and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

7.4 Without prejudice to the SCCs, this DPA shall be governed by and construed in accordance with the laws of the country of territory stipulated for this purpose in the Agreement and each of the parties agrees to submit to the choice of jurisdiction as stipulated in the Agreement in respect of any claim or matter arising under this DPA.

7.5 This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA. No modification of, amendment to, or waiver of any rights under the DPA will be effective unless in writing and signed by an authorized signatory of each party. This DPA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. Each person signing above represents and warrants that he or she is duly authorized and has legal capacity to execute and deliver this DPA. Each party represents and warrants to the other that the execution and delivery of this DPA, and the performance of such party's obligations hereunder, have been duly authorized and that this DPA is a valid and legally binding agreement on each such party, enforceable in accordance with its terms.

EXHIBIT A – SUPPLEMENTARY CLAUSES TO SCCs

1. Non-receipt of directives under FISA Section 702 rep

HackerOne represents and warrants that, as of the date of this contract, it has not received any national security orders of the type described in Paragraphs 150-202 of the judgment in the European Court of Justice Case C- 311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ("Schrems II").

2. FISA Section 702 ineligibility rep

HackerOne represents that to the best of HackerOne's knowledge, it is not eligible to be required to provide information, facilities, or assistance of any type under Section 702 of the Foreign Intelligence Surveillance Act ("**FISA**") because:

(a) No court has found HackerOne to be the type of entity eligible to receive process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C§ 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition.

(b) If HackerOne were to be found eligible for Section 702, which it believes it is not, it is nevertheless also not the type of provider that is eligible to be subject to Upstream collection ("bulk" collection) pursuant to FISA Section 702, as described in paragraphs 62 & 179 of the Schrems II judgment.

HackerOne will promptly notify the data exporter if the circumstances in this clause 2 change.

3. Court-review safeguard

HackerOne shall promptly assess, and use all reasonable legal mechanisms to challenge, any demands for data access through national security processes it receives in relation to data exporter's data as well as any non-disclosure provisions attached to such a request.

To the extent available HackerOne will seek interim measures to suspend the effects of any such order or demand until a court has finally decided that it is lawful and effective. For the avoidance of doubt, HackerOne shall not disclose the personal data requested until required to do so under the applicable procedural rules and will provide only the minimum amount of information permissible when responding to such order, based on a reasonable interpretation of that order.

In the event such an order or demand is received, HackerOne shall, as far as is lawfully practicable: inform the requesting public authority of the incompatibility of any such order with the safeguards comprised in the Clauses and the resulting conflict of obligations on HackerOne; and simultaneously and as soon as reasonably possible, notify the data exporter and/or competent supervisory authority within the EEA, Switzerland or UK of the order.

4. EO 12333 non-cooperation

HackerOne represents that to the best of HackerOne's knowledge, it is not required to take any action pursuant to

U.S. Executive Order 12333.

5. Notice of non-compliance

HackerOne shall promptly notify the data exporter if HackerOne can no longer comply with the SCCs and shall do so as far as practicable in advance to the receipt of personal data from the data exporter. Such notification shall take place without undue delay and within 72 hours of HackerOne determining that it can no longer (or will no longer be able to) comply. Under such circumstances (including, for the avoidance of doubt, where HackerOne is able to identify ahead of their implementation, any legal or policy developments which may lead to an inability to comply with obligations under the EU SCCs or UK IDTA Addendum) the data exporter authorizes HackerOne to promptly secure or return, or delete or securely encrypt, all relevant personal data, without the need for further instructions from the data exporter.

6. Further reassurance

HackerOne:

(a) Certifies that it has not purposefully created back doors or similar programming that could be used to access its systems and/or personal data; not purposefully created or changed its business processes in a manner which facilitates access to personal data or systems; and that national law or government policy does not require it to create or maintain back doors or to facilitate access to personal data or systems or for HackerOne to be in possession of or to hand over encryption keys in respect of personal data transferred under the Clauses.

(b) Shall provide all assistance reasonably requested by the data exporter to support data subjects in exercising their rights and the data exporter shall provide all information, cooperation and assistance reasonable required by HackerOne to do so.