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 the customer specified in the table below ("**Customer**") and HackerOne Inc. ("**HackerOne**").

HackerOne: HackerOne Inc.	Customer:
Entity type / incorporated in: Delaware corporation	Entity type / incorporated in:
Address: 180 Geary Street 5th Floor, San Francisco CA 94108	Address:
	Legal Jurisdiction (for the purposes of relevant supervisory authority).
Contact for data protection inquiries: Privacy Officer privacy@hackerone.com	DPO / Contact for data protection inquiries:

Each of Customer and HackerOne may be referred to herein as a "**party**" and together as the "**parties**".

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA and the Exhibits A and B (where applicable) (including Appendices 1 and 2).

2. This DPA has been pre-signed on behalf of HackerOne. Exhibit A incorporating the relevant Standard Contractual Clauses have been pre-signed by HackerOne as the data importer.

3. To complete this DPA, Customer must:
    a. Complete the information in the table on page 1.
    b. Complete the information in the signature boxes and sign on page 7.
    c. Complete the information in the signature boxes of Exhibit A and sign on page 12.

4. Send the completed and signed DPA to HackerOne by email, indicating the Customer's Name (as set out on the applicable HackerOne Order Form or invoice), to dpa@hackerone.com.

Upon receipt by HackerOne of Customer's validly completed DPA at this email address, this DPA will become legally binding.

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.

Definitions

1.1 The following expressions 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 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 and Switzerland;

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

(h) "**Standard Contractual Clauses**" means the Standard Contractual Clauses set out in Exhibit A and/or Exhibit B to this DPA, which forms a part of this DPA;

(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 in connection with the Services;

(j) "**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, nature and purpose of the processing, 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 of Processing**: HackerOne will process the Personal Data 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) **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.

(e) **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.

2.2 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. 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.

2.3 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby 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.

2.4 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 (i) this DPA and (ii) the Customer's written instructions;

(b) in the unlikely 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) promptly provide the Customer with reasonable cooperation and assistance in respect of a Security Breach and all reasonable information in HackerOne's possession concerning the Security Breach insofar as it affects Customer and/or any member of a Customer Group, including the following:

(i) the possible cause and consequences of the Security Breach;

(ii) the categories of Personal Data involved;

(iii) a summary of the possible consequences for the relevant data subjects;

(iv) a summary of the unauthorized recipients of the Personal Data; and

(v) the measures taken by HackerOne to mitigate any damage;

(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 confirm that such request relates to the Customer to which the Customer hereby 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 thereof) 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 URLfor 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 of processors under Data Protection Law in relation to its processing of Personal Data.

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 HackerOne makes available the transfer mechanisms which shall apply in the order of precedence set out below to the extent any Processing of Personal Data under this DPA takes place in any country outside the UK or EEA (except if in an Adequate Country):

(i) **Standard Contractual Clauses** referred to at *Exhibit A* to this DPA apply to the Services, and HackerOne will comply with the obligations of the 'data importer' and the Customer will comply with the obligations of the 'data exporter'; or

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

In the event that the Services are covered by more than one transfer mechanism, the transfer of Personal Data will be subject to a single mechanism in accordance with the priority identified above.

6.2 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 and EEA from time to time.

6.3 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 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 Standard Contractual Clauses (or part thereof); 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.

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 Save where indicated in the Standard Contractual Clauses, this DPA does not confer any third-party beneficiary rights, it is intended for the benefit of the parties hereto 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.

7.3 Without prejudice to the Standard Contractual Clauses, 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.

7.4 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 below 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.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed as of the Effective Date by their duly authorized representatives.

HACKERONE:	**CUSTOMER:**
By: Tilly McAdden	By:
Name: Tilly McAdden	Name:
Title: Assistant General Counsel	Title:
Date: 07 / 19 / 2022	Date:

SIGNATURE PAGE TO DATA PROCESSING ADDENDUM

Exhibit A

Standard Contractual Clauses (processors)

Part 1 - Introduction

To the extent any Processing of Personal Data by HackerOne under the DPA to which this Exhibit relates takes place in any country outside the UK or EEA (except if in an Adequate Country) this Exhibit (the "**Standard Contractual Clauses**") shall apply to the Services and be incorporated into and form part of the DPA, where HackerOne is the 'Data Importer' and the Customer is the 'Data Exporter.'

Where this Exhibit applies and the transfer of Personal data to HackerOne by Customer is subject to the laws of: (a) the European Economic Area or Switzerland, Part 3 applies; and/or (b) the United Kingdom, Part 4 applies. Parts 1, 2, 5 and 6 apply in both cases.

Part 2 – Details of the transfer

A. List of Parties

Data importer	
Name, Address, Contact Person, Role of Contact Person and Contact Person Contact details	HackerOne, details as set out at the head of the DPA.
Activities relevant to the data transferred under the Standard Contractual Clauses	Provision of the Services.
Role	Processor
Data exporter	
Name, Address, Contact Person, Role of Contact Person and Contact Person Contact details	Customer, details as set out at the head of the DPA
Activities relevant to the data transferred under the Standard Contractual Clauses	Use of the Services provided by HackerOne.
Role	Controller

B. Description of Transfer

Categories of data subjects whose personal data is transferred	As set out in s.2 of the DPA.
Categories of personal data transferred	As set out in s.2 of the DPA.
Sensitive data transferred	None, subject to clause 2(d) of the DPA.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)	Personal data is transferred on a continuous basis in accordance with the instructions of the Customer, for the Term of each Agreement (as defined in the DPA).
Nature of the processing	As set out in s.2 of the DPA.

Purpose(s) of the data transfer and further processing	The transfer of Personal Data enables HackerOne to provide the Services, as further set out in s.2 of the DPA.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	The period for which HackerOne may retain and use the transferred Personal Data is as set out in the DPA.
For transfers to (sub-) processors, subject matter, nature and duration of the processing	As set out in s.2 of the DPA.

C. Technical and organisational measures

Technical and organisational measures implemented by the Data Importer (as per Clauses 4(d) and 5(c) of the UK SCCs and Annex 2 of the EU SCCs)	Technical and organisational security measures are set out at https://www.hackerone.com/terms/security Technical and organisational measures by which HackerOne will provide assistance to the Customer in responding to data subjects' requests are set out at https://www.hackerone.com/privacy

Part 3 (EU Standard Contractual Clauses) (processors)

The Parties hereby agree to the terms in the Annex to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance), C/2021/3972, incorporating the terms of Module Two (controller to processor) (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj) ("**EU SCCs**").

The details of the data transfer and technical and organisational measures are set out at Part 2 and shall be deemed incorporated as Annex 1 and 2 of the EU SCCs respectively.

For the purpose of clause 9(a) EU SCCs OPTION 2 shall apply with notification time period of 10 days. 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 identified at the head of the DPA.

For the purpose of clause 17 EU SCCs OPTION 2 shall apply and the agreed law shall be the law of the country identified in the details set out at the head of the DPA. For the purpose of clause 18(b) EU SCCs, the parties agree to the courts of the same country. The optional clause 7 (docking clause) shall be included in the EU SCCs.

Part 4 (UK Standard Contractual Clauses) (processors)

The Parties hereby agree to the terms of the HackerOne UK Standard Contractual Clauses as set out in **Exhibit B** ("**UK SCCs**").

The details of the data transfer and technical and organisational measures are set out at Part 2 and shall be deemed incorporated as Appendix 1 (Part 2(A & B)) and 2 (Part 2(C)) of the UK SCCs respectively. Rights and obligations of the controller are set out in the Agreement and this DPA.

Part 5 (Additional Terms)

(A) INTERPRETATION

Without prejudice to the EU SCCs and UK SCCs, these additional terms set out the Parties' interpretation of their obligations under specific terms of the EU SCCs and UK SCCs. Where a Party complies with the interpretations set out in this Part 5, that Party shall be deemed by the other Party to have complied with its commitments under the Clauses.

1. **Appointment of new sub-processors**
   Pursuant to 5(h) of the UK SCCs and 9(a) EU SCCs, Data Exporter acknowledges and expressly agrees that Data Importer will appoint sub-processors in accordance with Section 4.1 of the DPA.

2. **Notification of new sub-processors and Objection Right for new sub- processors**
   Pursuant to 5(h) of the UK SCCs and 9(a) EU SCCs, Data Exporter acknowledges and expressly agrees that Data Importer may engage new sub-processors as described in Section 4.2 of the DPA.

3. **Copies of sub-processor agreements**
   The Parties agree that the requirement for copies of the sub-processor agreements for the purpose of audit or inspection (pursuant to 5(j) of the UK SCCs and 9(c) EU SCCs) may be met by way of the audit and records provisions at Section 5.2 of the DPA.

4. **Audit and Records**
   Data Exporter acknowledges and agrees (unless otherwise required by law) that it exercises its audit right under 5(f) of the UK SCCs and 8.9(c) EU SCCs by instructing Data Importer to comply with the audit measures described in Section 5.2 of the DPA.

5. **Obligation after the termination of personal data-processing services**
   Data Exporter agrees that the Data Importer may fulfil its obligation to return or destroy all the personal data on the termination of the provision of data-processing services under Clause 12 UK SCCs and 8.5 EU SCCs by complying with the measures described in Section 4(i) of the DPA.

6. **Conflict**
   In the event of any conflict or inconsistency between the DPA, the EU SCCs and UK SCCs, and this Exhibit, the EU SCCs and UK SCCs shall prevail.

(B) SUPPLEMENTARY CLAUSES

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 thereto.

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 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 Standard Contractual Clauses 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 SCCs) the data exporter hereby 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.

Part 6 (Execution)

By signing below, the Parties agree to the terms of this Exhibit A including the terms of the EU SCCs and UK SCCs (in Exhibit B, to the extent applicable as set out in Part 1).

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

Name (written out in full):
Position: **Authorised Signatory**
Address
Date:
Signature:

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

Name (written out in full): **Tilly McAdden**
Position: **Authorised Signatory**
Address: **HackerOne Inc.**
Date: 07 / 19 / 2022
Signature: 

SIGNATURE PAGE FOR EXHIBIT A

EXHIBIT B

Standard Contractual Clauses (UK) (processors)

INTRODUCTION

Both Parties have agreed on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1 (Appendixes 1 and 2 are set out in the DPA which incorporates these Clauses).

AGREED TERMS

Clause 1 Definitions

For the purposes of the Clauses:

(a) **'personal data'**, 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'Commissioner' shall have the same meaning as in the UK GDPR;

(b) **'the Data Exporter'** means the controller who transfers the personal data;

(c) **'the Data Importer'** means the processor who agrees to receive from the Data Exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;

(d) **'the sub-processor'** means any processor engaged by the Data Importer or by any other sub-processor of the Data Importer who agrees to receive from the Data Importer or from any other sub-processor of the Data Importer personal data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) **'the applicable data protection law'** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;

(f) **'technical and organisational security measures'** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the Data Exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and to (j),

Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the Data Importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Data Exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the Data Exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the Data Exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the Data Exporter

The Data Exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner) and does not violate the applicable data protection law;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the Data Importer to process the personal data transferred only on the Data Exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the Data Importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;

(g) to forward any notification received from the Data Importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner if the Data Exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-

processor providing at least the same level of protection for the personal data and the rights of data subject as the Data Importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the Data Importer

The Data Importer agrees and warrants:

(a) to process the personal data only on behalf of the Data Exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Exporter of its inability to comply, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Data Exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the Data Exporter as soon as it is aware, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the Data Exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the Data Exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the Commissioner with regard to the processing of the data transferred;

(f) at the request of the Data Exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the Data Exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Data Exporter, where applicable, in agreement with the Commissioner;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the Data Exporter;

(h) that, in the event of sub-processing, it has previously informed the Data Exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11; and

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the Data Exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the Data Exporter for the damage suffered.

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

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

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

Clause 7

Mediation and jurisdiction

1. The Data Importer agrees that if the data subject invokes against it, third-party beneficiary rights and/or claims compensation for damages under the Clauses, the Data Importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;

(b) to refer the dispute to the UK courts.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Co-operation with supervisory authorities

1. The Data Exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the Commissioner has the right to conduct an audit of the Data Importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the Data Exporter under the applicable data protection law.

3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the Data Importer, or any sub-processor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the country of the United Kingdom in which the Data Exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the Data Importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the sub- processor's obligations under such agreement.

2. The prior written contract between the Data Importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK in which the Data Exporter is established.

4. The Data Exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Commissioner.

Clause 12

Obligation after the termination of personal data processing services

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

2. The Data Importer and the sub-processor warrant that upon request of the Data Exporter and/or of the Commissioner, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Clause 13

Additional commercial clause

Without contradiction to the Clauses, the parties agree that the Clauses are incorporated into the services agreement that governs the provision of services by the Data Importer and/or its affiliate(s) to the Data Exporter (including payment services, and associated analytics and business services) (the "Agreement"). As between the Data Exporter and the Data Importer, the limitations and exclusions of liability set out in the HackerOne Agreement apply to the Clauses.