GENERAL CONDITIONS OF USE (GCU)

Version dated 25 January 2023

These GCU define the terms and conditions which apply between YesWeHack, a simplified joint stock company with a share capital of EUR 45,262.84, with its seat at 14 rue Charles V - 75004 Paris, registered in the Paris Trade Register under number 814 037 214 (the "**Company**") and any individual registering on the Company's platform (the "**User**") accessible via the address: *https://yeswehack.com/auth/register* (the "**Platform**"). The Platform offers three (3) different types of services: (i) Bug Bounty Programs, (ii) VDPs, and/or (iii) Pentest Management (together, the "**Services**") to which a Company customer can subscribe (the "**Customer**").

A User can refer to (i) a **Customer User** or (ii) a **Hunter**. Certain specific provisions in these GCU will apply either to a Customer User or a Hunter and a User should refer to the provisions relevant to them. Any capitalized terms used herein shall have the meaning given to them in Appendix 1.

The Company reserves the right to make any changes at any time to these GCU, the Platform and any of its related Services. Users will be notified upon next login to their account and asked to accept the new GCU. In case of disagreement with the new provisions, the User understands and acknowledges that he/she can no longer use the Platform and its related Services.

1. PREREQUISITE

Acceptance of incorporated terms: Access to and use of the Services is subject to the prior acceptance of these GCU and use of the Wallet for the payment of Rewards to Hunters is subject to the prior and unconditional acceptance of the Terms and Conditions of MANGOPAY available https://www.mangopay.com/terms/MANGOPAY_Terms-EN.pdf which are hereby incorporated.

Age requirement: The Services are forbidden to minors. The age of minority may differ depending on nationality and applicable law.

2. USER STATUS

Independence of Hunters. The Platform is designed for the purpose of putting in touch Hunters and Customer Users. As such, the Hunter expressly acknowledges that he/she has no link of dependence or subordination, whether direct or indirect with the Company or a Customer. The Hunter acknowledges that he/she acts on an occasional and non-exclusive basis.

Authority of Customer Users. Customers designate their Customer Users who will use the Platform and the Services to which Customers have subscribed. Any action or omission of the Customer User shall be deemed an action or omission of the Customer. The Customer User is informed that, if necessary, additional documents may be requested, such as any document attesting to the power of attorney of the person authorized to represent the Customer. In the event that a Customer User is also a Hunter, he/she undertakes not to participate in its own Customer programs, unless expressly agreed otherwise or unless the Customer User is a Penetration Tester.

3. REGISTRATION PROCESS

Creating a User account and accessing the Wallet. A User must provide certain information when filling out the registration form available on the Platform. Additional information will be required to create a Wallet. A User is responsible for updating his/her personal information and expressly acknowledges that the Company cannot be held liable for any misrepresentation regarding his/her identity. If any information proves to be false, incomplete, or obsolete, the Company reserves the right to refuse or rescind registration and/or interrupt access to the Platform and use of the Services.

Hunter's Wallet. Subject to providing the required information, Hunters will have a Wallet opened in EUR currency in the Platform for the settlement of his/her Rewards. For each Bug Bounty Program under a different currency, a new Wallet will be created in the relevant currency.

Customer's Wallet. Upon activation of a Customer's subscription and subject to the acceptance of the T&Cs, a Customer Wallet will be created for the payment of Rewards to Hunters as part of a Bug Bounty Program.

Management of Wallet. Payments for Rewards are deposited, stored, and paid through the relevant Wallet managed and controlled by MANGOPAY, an authorized and regulated payment service provider used by the Company. The Hunter or Customer User is informed of the balance of the Wallet, through their relevant account on the Platform. Hunters will also receive the summary of amounts paid on an annual basis.

4. SERVICES

4.1 Users' role

Hunters' Participation. When invited to a Bug Bounty Program, the Hunter is free to decide whether he/she wishes to participate and determines at his/her sole discretion the means to be used to conduct Tests, subject to compliance with the rules of the relevant Bug Bounty Program. When performing the Tests, the Hunter acknowledges to be tacitly bound by the rules of the Bug Bounty Program set forth by the Customer without the need to expressly agree to those rules. The Hunter accepts that the rules of the Bug Bounty Program have a contractual value between him/her and the Customer and may not, therefore, contest the admissibility, opposability and/or enforceability of these rules.

Customer Users' Program Management. A Customer User, who is the Customer's person of choice to represent the Customer in the management of the Services (the "**Customer Representative**"), designates Customer Users of his/her choice for the publication and management of the Customer's Bug Bounty Program, including the selection of Hunters. The Customer Representative will be able to define a role with specific access rights for each User depending on their function and intended involvement. The Bug Bounty Program is described by the Customer User in the description/dedicated sheet online on the Platform, including scope, configuration of public or private mode, designation of the systems, type of tests, eligibility, periodicity, exclusions, Rewards, etc. Once a Bug Bounty Program is published and a Vulnerability Report is submitted by a Hunter, the Customer User can validate said report and reward the Hunter as described in Article 4.3. The Customer User can also attribute points to the Hunter according to the criteria defined in the Platform's Helpcenter : Helpcenter.

4.2 Tests

Hunters' scope. Hunters do not need to consult the Customer prior to performing Tests and will act at their convenience to carry these out as long as there are acting within the rules of the Bug Bounty Program defined by the Customer. Hunters understand and agree that Tests can only be performed subject to the strict rules of the relevant Customer's Bug Bounty Program and that failure to comply with these could trigger their civil and/or criminal liability.

As such, Hunters agree to the following:

- Strictly limit their action to the scope defined in the relevant Bug Bounty Program.
- Not repeat any Test whatsoever outside the scope strictly defined by a Bug Bounty Program, or once a Bug Bounty Program is closed.
- Comply with any data privacy policy set out in a Bug Bounty Program.
- Keep strictly confidential the Customer's information to which they may have had access during the Tests, including the Vulnerabilities and, if applicable, any Personal Data, (together the "Data") meaning that Hunters shall:
    - Use the Data only for purposes strictly necessary for the proper performance of the Tests.
    - Not communicate the Data to any third party in any way and by any means whatsoever (in particular, oral, paper, digital).
    - Report any obvious anomaly to the Company if Hunters notice security failures on the Platform as well as to the Customer for any obvious anomaly noticed during the Tests.
    - Not to use the Data for the development, production or marketing of a system that infringes Customer's rights, its activity and/or competes directly or indirectly with it.
    - Warrants to respect Customer's Intellectual Property Rights, at all times and in particular, during the performance of the Tests, including but not limited to the software used and operating licenses.
- Not participate in any private Bug Bounty Program to which they have not been invited by a Customer.

Hunters acknowledge and agree that the Company acts as an intermediary and does not intervene in any way in the relationship with the Customer. In case Hunters have contacts with Customers, they remain solely responsible for the content of their exchanges with the Customer.

Hunter collaboration. When allowed by the Customer Representative in the Bug Bounty Program, the Hunter can collaborate with several Hunters to submit a report together and share the reward. Hunter collaboration shall be effective only for Hunters using the Platform and accepting these GCU. It is the Hunter's responsibility to ensure that any such collaboration is compliant with this section.

Customer User's involvement. The Customer User shall carry out and maintain the backup of its data, files, supports against destruction, loss or alteration. The Customer User expressly acknowledges that it will not be consulted prior to the completion of the Tests during the period of time defined in the Bug Bounty Program. In other words, Hunters will test the System during the period of time specified in the Bounty Bug Program without consulting the Customer User. The Customer User acknowledges having been informed by the Company of the importance of preparing the Tests. Various tips on how to prepare the Tests can be found in the Platform's Helpcenter.

4.3 Vulnerability Reports

The Customer User will determine whether Vulnerabilities are valid and their severity level. Hunters who were first to uncover a valid Vulnerability and who established a clear Vulnerability Report with a severity level in accordance with the relevant Bug Bounty Program will be rewarded by the Customer in the form of Rewards. Hunters will also gain points in the Hunters' ranking which is displayed on the Platform.

4.4 Security

Platform's Bug Bounty Program. The Company's Platform is subject to its own Bug Bounty Program. Users shall inform the Company without delay, by any means, of any error, fault or irregularity that they find when using the Platform and/or Services, as soon as they become aware of it. Users shall not attempt to alter the headers or attempt to manipulate the pages of the Platform in such a way as to disguise, hijack, or modify the Platform. It is also prohibited to create a work or site derived from all or part of this Platform, or to resell or redistribute the Company's data.

Means of authentication. The login/password combination allowing a User to access his/her account is strictly personal and confidential. The User shall keep them secret, shall not communicate them to third parties in any form whatsoever. Users acknowledge that any use of the Services is made under their full and complete responsibility. Consequently, Users acknowledge that the actions carried out on their account are presumed to be made by them and will be charged to them, it being up to the User to provide proof to the contrary. The Company reserves the right to suspend a User's access to his/her account in case of proven compromise or in case of suspicion of compromise of his/her means of authentication.

Technical means to access Services. It is the responsibility of Users to equip themselves in an appropriate manner, notably in terms of computer and electronic communications, to access the Platform and Services and to take all appropriate measures to protect themselves, the Company and the tested systems from any attack or damage that could affect the data, software or contents stored on the Platform. The Company is not responsible for any depreciation of a User's computer media. Furthermore, the User acknowledges that it knows and understands the Internet and its limitations and, in particular, its functional characteristics and technical performance, the risks of interruption, the response times for consulting, querying or transferring information or the risks inherent in any transfer of data. The Company is not liable for the unavailability of networks that are not entirely under its direct control.

Hunters' responsibility. Hunters shall not hinder the proper functioning of the Platform and/or the Services in any way whatsoever, notably by transmitting any element likely to contain a virus or malicious Bug Bounty Program likely to damage or affect the Platform and/or the Services and, more broadly, the information system of the Company and any of its Customers or business partners. All costs and authorizations required to connect, access, and use the Platform and/or Services are and remain the Hunter's sole responsibility.

4.5 Availability of Services

Platform Maintenance. Except in cases of Force Majeure, the Company shall, as part of a duty of best endeavors, ensure the availability and accessibility of the Platform. Nevertheless, control and maintenance operations can be carried out at any time. The Company endeavors to prevent, as much as possible, the occurrence of such an operation within at least twenty-four (24) hours before the beginning of the actual operation in the event that a schedule maintenance lasts for more than 30 minutes. The Company cannot be held liable for any resulting consequences for the User.

4.6 Suspension / Termination

The Company reserves the right to temporarily suspend all or part of the Services and a User's account for reasons related to the security of the Platform and/or Services, a User's security or a breach or suspected breach by the User of any of his/her obligations hereunder. The Company also reserves the right to unilaterally terminate these GCU in the event that a User demonstrates serious and/or repeated breaches of any of his/her obligations hereunder. Such termination will be done as of right, without delay and without prejudice to the damages that the Company could seek.

A User may, at any time, without prior notice and without having to justify the reasons, deactivate its account. Deactivation of the User's account will result in immediate termination of these GCU.

5. FINANCIAL CONDITIONS *(applicable only to Hunters)*

Invoicing mandate. To allow the Company to invoice in their name and on their behalf the Rewards awarded to them, Hunters expressly and unconditionally agree to the terms of the Invoicing Mandate (Appendix 2). It is expressly agreed that the Invoicing Mandate must be duly completed and accepted by the Hunter in his/her personal account. Failing this, any operation initiated by the Hunter will not give rise to payment.

Rewards. The Hunter will collect Rewards awarded by the Customer User in his/her e-Wallet account, at the Customer User's discretion and in accordance with the relevant Bug Bounty Program. The Rewards are expressed in the program currency, VAT included. The Hunter agrees to regularly consult the FAQ by clicking the following link: FAQ

Hunters' status. Hunters are informed that their activity on the Platform is likely to be subject to affiliation to a specific legal status. Hunters shall therefore make the necessary enquiries and carry out the required formalities to acquire the legal status relevant to their situation. Hunters are also made aware that the income derived from their activity on the Platform is subject to various legal, social, accounting and tax requirements, notably depending on fiscal territoriality. Hunters hereby expressly acknowledge that it is their sole responsibility to enquire about these requirements and to comply with them. Hunters shall make all declarations required by tax authorities and social security bodies to which they belong, depending on status and country of residence in and outside of the European Union.

Company's obligations towards Hunters. The Company can under no circumstances be involved in any of the above steps and its liability can, under no circumstances and for any reason whatsoever, be sought in relation to any of these legal, social, accounting and tax obligations. The Company's obligations are strictly limited to:

- informing Hunters of the existence of such requirements which are to be carried out by the Hunters, at their own expense, and
- providing them with a document summarizing all transactions made on the Platform.

6. INTELLECTUAL PROPERTY

The Platform and/or Services. The Platform (including all accessible information, in particular in the form of downloadable text, photos, images, sounds, data, databases and the Bug Bounty Program, including the underlying software and other technology) and Services are protected by Intellectual Property Rights and/or other rights that the Company owns or is authorized to use. The User may not under any circumstances (except under the limited exception of VDP) store, reproduce, represent, modify, transmit, publish, adapt on any medium whatsoever, by any means whatsoever, or use in any way whatsoever, the elements of the Platform and/or Services without the prior written permission of the Company.

Each party is and will remain owner, as far as it is concerned, of its distinctive signs, namely trademarks, corporate and other names, trade names, brand names and domain names. Reproduction, imitation or affixing, in whole or in part, of trademarks or designs or models belonging to the Company is strictly prohibited without its prior written consent. The User shall respect all mentions relating to the Intellectual Property Rights appearing on the Platform and/or the Services and shall not alter, delete, modify or otherwise infringe upon them.

Assignment of Intellectual Property Rights (IPRs) on the Vulnerability Reports. The Hunter agrees to assign, free of charge, its IPRs on the Vulnerability Reports to the relevant Customer for all countries where they are protected, in all languages, for the entire duration of the legal IPRs of the authors or their successors, according to all applicable laws, both current and future, including any extensions that may be made to this duration and in all forms, presentations and by all processes both current and future. If a Vulnerability Report is written by more than one Hunter, this assignment is valid for the share of which each Hunter is author.

Hunter IPRs Warranty on the Vulnerability Reports. The Hunter warrants to be the sole and exclusive author of whole or part (in case of a Hunter collaboration as specified in 4.2) of the Vulnerability Report. Consequently, to the fullest extent permitted by applicable law, the Hunter shall be held liable, under the conditions provided for

in the GCU, by the Customer in the event of a breach of this provision and in particular with regard to the legislation on intellectual property rights or authors rights infringement.

7. CONFIDENTIALITY

Users have an obligation to keep confidential all information to which they have access or which they possess in the context of the Services. Users shall not disclose such information to any third party for any reason whatsoever and this regardless of the legal and/or economic ties that a User may have with such third party.

At the end of a Bug Bounty Program, a Hunter will delete all information related to it, namely, data of any kind, including Personal Data but also reports made by the Hunters.

8. PERSONAL DATA

The Protection of Personal Data Appendix (Appendix 3) details the information on the processing of Personal Data, the purposes and legal basis of the processing carried out, the categories of data concerned, the recipients of the data, the retention period and the rights of the Users.

As part of the performance of the Tests and depending on the scope of a Bug Bounty Program, Hunters may have access to Personal Data processed by the Customer. Hunters shall ensure the security and confidentiality of said Personal Data and shall take all necessary technical and organizational measures to prevent the destruction, loss, alteration, unauthorized disclosure or access to the Personal Data, whether accidental or illicit. Hunters shall not make any use or process such Personal Data, and shall comply with any data privacy policy set out in a Bug Bounty Program.

A User can exercise their privacy rights by writing to the following address: privacy@yeswehack.com

9. LIABILITY

Company's liability. The Company shall under no circumstance be liable for:

i. use or misuse of the Platform and/or Services by a User;
ii. non-performance, failure, malfunction, or unavailability of the Platform and/or Services resulting from a third party's or a User's (with the exception of any data processors of the Company, if applicable) action or omission;
iii. failure of the Customer User to fulfil its obligations (e.g., inaccuracy, error, omission) in the definition and management of a Bug Bounty Program;
iv. non-compliance with these GCU, violation of the rules of the Program or any other agreement by the Hunters;
v. suspension of access to the Platform and/or the Services under the conditions defined in Article 4.6; and
vi. incidents due to the use of Internet (e.g., loss of connectivity…).

Any reputation, classification, or description of a Hunter's skills in connection with the Services is for information purposes only. Any selection of a Hunter is made by a Customer User and as such, shall be decided at the Customer's discretion and under its sole responsibility.

The Company provides support in the drafting of the Bug Bounty Programs and Vulnerability Reports and intervenes, as part of a Bug Bounty Program, only as an intermediary to introduce Hunters to the Customers and its related Customer Users. The Company shall therefore not be liable for any damage caused by a Customer, a User, a Hunter's failure to perform their obligations, whether partially or totally.

The Company does not propose nor make any modification/adaptation on the Vulnerability Reports. Therefore, the Company shall not be liable in any way for the content of any Vulnerability Report, including but not limited to (i) any error or omission, or (ii) any loss or damage of any kind resulting from the use of a Vulnerability Report.

Hunters' liability. The Hunter is responsible for all damage he/she causes to the Company and/or other Users. The Hunter agrees to indemnify the Company and/or Users, in case of any order to pay damages and interest that the Company or Users might incur as a result of non-compliance with these GCU or to damages caused to others or to itself. Any action taken outside the limits set by a Bug Bounty Program may result in civil and/or criminal liability.

10. COMPLIANCE

Users may not use any of the Services if they are the subject or the target of any economic or financial sanctions imposed, administered or enforced by the U.S. government (including by the Office of Foreign Assets Control of the U.S. Department of the Treasury or the U.S. Department of State), the European Union or any of its member states, the United Nations Security Council or the United Kingdom (including by the Office of Financial Sanctions Implementation of Her Majesty's Treasury).

11. GOVERNING LAW AND JURISDICTION

These GCU are governed by French law. The Parties shall endeavor to settle amicably any dispute that may arise between them. Any dispute or claim arising out of or in connection with these GCU or their subject matter or formation (including any non-contractual dispute or claim) shall be subject to the exclusive jurisdiction of the competent courts of Paris, and the Parties hereby irrevocably submit to the exclusive jurisdiction of those courts for these purposes.

12. GENERAL PROVISIONS

Force Majeure. Neither party shall be liable to the other for any delay or non-performance of its obligations under these GCU arising from a Force Majeure event. The affected party must immediately notify the other party and shall make every effort to reduce as much as possible the harmful effects resulting from this situation. Each party shall bear all costs incumbent upon it resulting from the occurrence of the Force Majeure event.

Survival. In the event of termination or early termination of these GCU for any reason, or discontinuance or cancellation of the Services, the Platform or a User account, any provision or condition of these GCU intended to survive such termination shall survive and shall not affect the validity of the rights and obligations set forth in the sections entitled "Personal Data", "Confidentiality", "Intellectual Property", "Liability", "Governing Law and Jurisdiction", and any other provision of these GCU which, by their nature or by virtue of specific provisions, extend beyond the end or expiry of these GCU.

Rules on evidence: In the event of a dispute, Users and the Company agree that data such as clicks and double clicks, timestamp tokens and digitally certified dates, connection data relating to actions carried out from the account and the certificates and electronic signatures transmitted shall be admissible in court and shall prove the data and facts contained therein as well as the signatures and authentication procedures they express.

Hypertext Links. The GCU may contain hypertext links to third-parties legal documents over which the Company has no control. The User acknowledges and accepts that the documents to which reference may be made through these links may be modified, amended and/or altered and such modification, amendment and/or alteration shall be opposable and enforceable toward the User.

Notices: Any notice provided pursuant to these GCU, including any notice of complaint or event triggering liability, shall be given in writing, by registered letter with acknowledgement of receipt, by e-mail with acknowledgement of receipt or by any other means where receipt can be proven, at the address indicated at the start of these GCU.

APPENDIX 1 – DEFINITIONS

Bug Bounty Program: means the program created by the Customer to invite Hunters to conduct Tests on its systems, and which shall contain a comprehensive description of the terms, conditions and requirements to which Hunters must agree, including the scope of the Tests defined and authorised by the Customer (designation of systems, type of Tests, eligibility, periodicity, exclusions, bonuses, etc.) and the Rewards, if any, that the Customer grants to Hunters who are invited to and participate in such Program. The Customer may choose to run the Program in (i) private mode, where only Hunters invited by the Customer are informed of the existence of such a Program and are entitled to participate ("**Private Program**"), or (ii) public mode, in which case the Program is published on the Platform and any Hunter meeting the conditions set out in the Program may participate ("**Public Program**").

Customer User: means the individual appointed by and representing the Customer to use the Platform and the Services.

Force Majeure: means an event or circumstance beyond the reasonable control of the affected Party, which could not be reasonably foreseen and the effects of which cannot be avoided by appropriate measures, including but not limited to acts of God, fire, explosion, adverse weather conditions, flood earthquake, terrorism, riot, civil commotion, war, hostilities, strikes, work stoppages, slow-downs, or other industrial disputes, accidents, riots or civil disturbance, acts of government, lack of power and delays by suppliers or materials shortages of transportation, facilities, fuel, energy, labour, or materials.

Hunter: an independent individual or legal entity, IT security researcher, who may act in a professional or non-professional capacity and who participates in a Bug Bounty Program.

Intellectual Property Rights (IPRs): means all intellectual property rights, including but not limited to copyright, software rights, computer program rights, database rights, patent rights, invention rights, trademark rights, distinctive marks, design rights, trade secrets and know-how, domain names, and all other intellectual property rights, whether registered or not, including all filings (or the right to file with any competent national or foreign office), renewals or extensions of such rights and all similar or equivalent rights or forms of protection existing or to be created anywhere in the world.

Penetration Tester: means an independent entity or individual who works for the Customer and under the latter's responsibility for the purpose of conducting penetration tests and who participates in a Pentest Management at the Customer's request and as part of a separate agreement between the Penetration Tester and the Customer.

Pentest Management: means the solution allowing the Customer to manage and optimize, as a whole, the project of penetration tests carried out by Penetration Testers (from kick off to reporting).

Personal Data: as well as the terms "**Data Subject**", "**Processing**", "**Controller**", "**Data Processor**", "**Recipient**", "**Third Party**", and "**Personal Data Breach**" refer to the definitions in Article 4 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of Personal Data.

Reward: means the financial reward to be awarded to the Hunter, by the Customer, in the context of a Program, if the Hunter successfully completes the Tests, i.e., if he/she reports a Vulnerability recognised as valid as defined by the rules of the Program in the Platform. For each Vulnerability, only the Hunter who submitted the first valid report is rewarded.

Tests: means the tests which the Customer wishes to have carried out by a Hunter and which comply with the Bug Bounty Program defined by the Customer. These Tests include any action to reach or enter a Customer's system, analyse the level of security in place and search for Vulnerabilities.

Vulnerability: refers to any defect, bug, or security flaw which, individually or cumulatively, has repercussions on the use or operation of the System's functionalities.

Vulnerability Disclosure Policies (VDP): means a secure and structured channel that allows the Security Researcher to report security issues and vulnerabilities to exposed organisations.

Vulnerability Report: means the report(s) issued by a Hunter, describing the Vulnerability discovered in the Bug Bounty Program and submitted to the Customer through a secure communication channel.

Vulnerability Report Management Services (or "Triage"): means the additional service consisting for the Company in accessing the information contained in the Vulnerability Reports and performing a series of actions, including validating the Vulnerability Reports submitted by the Hunter, communicating with these Hunters and (if applicable) carrying out actions on the Customer systems in the context of Vulnerability reproduction.

Wallet: means the online payment tool used on the Platform for the payment of the Rewards by the Customer to the Hunters. This is not a bank account.

APPENDIX 2 – INVOICING MANDATE (FOR HUNTERS ONLY)

FOR FRENCH HUNTERS:

In accordance with the provisions of Article 289-I of the General Tax Code (CGI) and the extract from the Official Bulletin of Public Finance (BOFIP) "VAT - Taxation regimes and reporting and accounting obligations - Rules relating to the preparation of invoices - Issue of invoices", BOI-TVA-DECLA-30-20-10-20140113:

By checking the box "I have read and accept the terms of this invoicing mandate", the Hunter expressly authorises YesWeHack to invoice in his or her name and on his or her behalf the rewards that are due to him or her as part of a Bug Bounty program.

The Hunter certifies on his or her honour that he or she is aware of and complies with the social, fiscal and accounting requirements imposed on him or her in France. YesWeHack cannot be held liable in the event of failure of the Hunter regarding this verification.

The agent (YesWeHack):

- shall archive or have archived in a secure manner the present invoicing mandate in order to demonstrate its existence to the tax authorities if requested;
- shall carry out all the necessary acts for the issue and availability of invoices to the Hunter in his or her personal account;
- shall archive or have archived in a secure manner the digital invoices and the data contributing to the establishment of the invoice in such a way that the principal can access them as soon as possible.

The principal (the Hunter)

- shall archive or have archived in a secure manner the present invoicing mandate in order to demonstrate its existence to the tax authorities if requested;
- shall archive or have archived in a secure manner its electronic invoices and data contributing to the establishment of the invoice;
- shall inform YesWeHack of the information concerning its identification and that relating to the content of the invoices issued in its name and on its behalf and shall transmit the supporting documents as soon as possible by digital means;
- shall bring to the attention of the agent, in case of dispute on an invoice, the information necessary for the modification of the invoice, as soon as possible;
- shall pay to the Public Treasury the tax mentioned on the invoices drawn up in his or her name and on his or her behalf;
- shall claim as soon as possible the double of an invoice if he or she has not received it;
- shall accept any invoice that YesWeHack has issued in his or her name and on his or her behalf. This acceptance is done by clicking on the invoice when reading it. For evidentiary purposes, YesWeHack keeps the proof of the click and ensures its reliable time stamping during the invoice archiving period. The Hunter acknowledges having a fourteen (14) day period from the reading of the invoice to modify its content. Failing this, the Hunter acknowledges having fully accepted it;
- acknowledges being fully responsible for the obligations and consequences in terms of invoicing with regard to VAT;

- acknowledges that he or she will not be able to argue of the failure or delay of YesWeHack in the establishment of the invoices to avoid the obligation to declare the collected tax when it falls due;
- acknowledges that it remains liable for the VAT due, if applicable pursuant to Article 283, paragraph 3 of the French General Tax Code, when it is wrongly invoiced.

The Invoice established by YesWeHack expressly mentions:

- That it is issued by YesWeHack in the name and on behalf of the Hunter expressly identified;
- The exchange rate applied for the conversion into EUR currency;
- The mandatory invoicing information such as the identity of the Hunter, the identity of the User, the invoice number, the invoice date, the date of the Bug Bounty service, the value added tax (VAT) identification, the legally applicable VAT rate, the precise designation of the Bug Bounty, the date or terms of payment, if applicable, for Hunters not subject to VAT the mention "VAT not applicable - Article 293 B of the CGI".

FOR NON-FRENCH HUNTERS

By checking the box "I have read and agree to the terms and conditions of this Invoicing Mandate", the Hunter expressly authorises YesWeHack to invoice on his or her behalf and for his or her account the rewards owed to him or her under a Bug Bounty program.

The Hunter certifies on his or her honour that he or she is aware of and complies with the social, tax and accounting requirements applicable to him or her. YesWeHack cannot be held liable in the event of failure of the Hunter regarding this verification.

The agent (YesWeHack):

- shall archive or have archived in a secure manner the present invoicing mandate in order to demonstrate its existence to the tax authorities if requested;
- shall carry out all the necessary acts for the issue and availability of invoices to the Hunter in his or her personal account;
- shall archive or have archived in a secure manner the digital invoices and the data contributing to the establishment of the invoice in such a way that the principal can access them as soon as possible.

The principal (the Hunter)

- shall archive or have archived in a secure manner the present invoicing mandate in order to demonstrate its existence to the tax authorities if requested;
- shall archive or have archived in a secure manner its electronic invoices and data contributing to the establishment of the invoice;
- shall inform YesWeHack of the information concerning its identification and that relating to the content of the invoices issued in its name and on its behalf and shall transmit the supporting documents as soon as possible by digital means;
- shall bring to the attention of the agent, in case of dispute on an invoice, the information necessary for the modification of the invoice, as soon as possible;
- shall pay to the tax authorities on which it depends the sums due to it in respect of the invoice;
- shall claim as soon as possible the double of an invoice if he or she has not received it;

- shall accept any invoice that YesWeHack has issued in his or her name and on his or her behalf. This acceptance is done by clicking on the invoice when reading it. For evidentiary purposes, YesWeHack keeps the proof of the click and ensures its reliable time stamping during the invoice archiving period. The Hunter acknowledges having a fourteen (14) day period from the reading of the invoice to modify its content. Failing this, the Hunter acknowledges having fully accepted it;
- acknowledges being fully responsible for the obligations and consequences in terms of invoicing in respect of any sums owed to the tax authorities on which he or she depends;
- acknowledges that he or she will not be able to argue of the failure or delay of YesWeHack in the establishment of the invoices to avoid the obligation to declare the collected tax owed to the tax authorities on which he or she depends when it falls due;
- acknowledges that he or she remains liable for the sums owed to the tax authorities on which he or she depends.

The Invoice established by YesWeHack expressly mentions:

- That it is issued by YesWeHack in the name and on behalf of the Hunter expressly identified;
- The exchange rate applied for the conversion into EUR currency;
- The mandatory invoicing information such as the identity of the Hunter, the identity of the User, the invoice number, the invoice date, the date of the Bug Bounty service, the value added tax (VAT) identification, the legally applicable VAT rate, the precise designation of the Bug Bounty, the date or terms of payment, if applicable, for Hunters not subject to VAT if it is applicable, the mentions imposed by the tax administration on which he or she depends.

APPENDIX 3 – PROTECTION OF PERSONAL DATA

The purpose of this Appendix is to set out the rights and obligations with regard to the protection of Personal Data under these GCU and any agreement between the Company and a Customer (the "Agreement").

The Company has appointed an external DPO: privacy@yeswehack.com

For the interpretation of the concepts related to the protection of Personal Data contained in this Appendix, please refer to the definitions of Article 4 of Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation, hereinafter "GDPR"), and these GCU.

In the context of the Services, the Company processes Personal Data relating to the Customer and Users, as Data Controller, in accordance with Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation) and Law No 78-17 of 6 January 1978 as amended. **(1)**

The Company hosts Vulnerability Reports. In connection with the provision and performance of the Vulnerability Report Management Services, the Company may access Personal Data contained in Vulnerability Reports. In both cases, YesWeHack acts as a Data Processor of the Customer, in accordance with Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation) and Law No 78-17 of 6 January 1978 as amended. **(2)**

For the Wallet, the Company processes Personal Data relating to the Customer's representative that is necessary for the creation and management of the Wallet, as Data Controller jointly with MANGOPAY, also Data Controller, in accordance with Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation) and Law No 78-17 of 6 January 1978 as amended. **(3)**

1. **Processing of Personal Data performed by the Company as Data Controller**

1.1. Data Subjects and Personal Data concerned

The Data Subjects of the processing of Personal Data carried out by the Company are: the Customer's representative and the User.

The Personal Data processed by the Company is:

- the Customer's representative: identification data (surname, first name); Date of birth; Nationality; Country of residence; Email address; Phone number.
- the User: identification data (surname, first name, username/pseudo); login details (Email address, Password); Country.

This data is necessary for the purposes described below.

1.2. Purposes and legal basis for processing

Purpose	Legal basis
• Administration and technical and/or commercial management of the Services; • User Account Management.	Article 6 (1) (b) of the GDPR: *Performance of the Agreement*

• Management of Platform Security, Services and Programs (legitimate interest: *ensure the proper functioning and security of the activity of the Platform*); • Statistics on the activity of the Platform (legitimate interest: *measurement and development of the activity of the platform based on overall indicators*); • Dispute management (legitimate interest: *defence of the Company's rights*) • Sending information about the Company (events, news, etc.) and its commercial offers corresponding to services similar to those already provided (legitimate interest: the Company's commercial development)	Article 6 (1) (f) of the GDPR: *pursuit of legitimate interests, while respecting the fundamental rights and freedoms of data subjects*
• Management of requests related to the exercise of rights granted to data subjects concerned by the processing of personal data.	Article 6 (1) (c) of the GDPR: *compliance with a legal obligation* (Article 12 of the GDPR)

1.3. Recipients of Personal Data

The Personal Data of the Customer's representative and the User is communicated to the authorised staff of the Company and to its Processors performing the Services.

Upon acceptance of the GCU, the Processors are:

- OVH for Site hosting (private cloud/dedicated server) - 2 rue Kellermann - 59100 ROUBAIX;
- Encrypted back up of dedicated servers - OVH Germany (Frankfurt)/Scaleway (Ile-de-France).

1.4. Retention of Personal Data

As part of the management and performance of the Services, the Personal Data of the Customer's representative shall be kept throughout the term of the GCU / the Agreement and/or the last current purchase order. It is kept in intermediate archives for an additional period of 6 years for evidentiary purposes (criminal requirement in accordance with Article 8 of the French Code of Criminal Procedure), from the end of the Agreement and/or the last purchase order. It is deleted at the end of this period.

In the context of the performance of the Services and for the management of Platform security, Services and Programs, Users' Personal Data is kept for the entire life of the account. It is kept in intermediate archives for an additional period of 6 years for evidentiary purposes (criminal requirement in accordance with Article 8 of the French Code of Criminal Procedure) as from the closure of the account by the User. It is deleted at the end of this period.

For commercial communication, the contact details (email address) of the Customer's representative and those of the User are kept for a maximum period of 3 years from the last contact with the Data Subjects. It is deleted at the end of this period.

The Personal Data of the Data Subjects (Customer's representative or User) necessary for the management of the dispute is retained until all legal remedies have been exhausted.

Requests to exercise the rights of Data Subjects (Customer's representative or User) are retained for evidentiary purposes for one year from the Company's response.

1.5. Rights of Data Subjects

The rights granted to Data Subjects (the Customer's representative or the User) are:

- the right of access, rectification and erasure of their data under the conditions provided for by the regulations (Articles 15 to 17 of the GDPR);
- the right to restrict the processing of this data under the conditions provided for by the regulations (Article 18 of the GDPR);
- the right to data portability under the conditions provided for by the regulations (Article 20 of the GDPR);
- the right to object to the processing of data under the conditions provided for by the regulations (Article 21 of the GDPR);
- the right to lodge a complaint with the CNIL;
- the right to define guidelines for access to their data in the event of death.

Requests relating to these rights can be exercised by email to the following address: privacy@yeswehack.com, specifying the purpose of the request (right concerned) and attaching any supporting documents identifying the requester (in case of doubt of the Company) or attesting to the mandate in case of representation.

2. Data processing performed by the Company as the Customer's Processor

For the hosting of Vulnerability reports or when the Customer has subscribed to the VDP Services, the Company acts as Processor for the access/consultation of any Personal Data that may be produced. In both cases, the Company acts on behalf of the Customer, having the capacity of Data Controller, and under its instructions as defined below.

It is the Customer's responsibility to inform the data subjects of the processing that may be carried out by the Company.

2.1. General obligations

The Company undertakes to:

- Process Personal Data in accordance with the Customer's documented instructions and only for the specific purpose(s) of the Processing, unless otherwise instructed by the Customer.
- Ensure that its staff duly authorised to process the Personal Data are subject to a confidentiality obligation.
- Raise awareness among and train such staff on the protection of personal data.

- Assist the Customer and provide it with all the information necessary to demonstrate compliance with its obligations regarding the protection of Personal Data and to enable the Customer to comply with the GDPR. In particular, it assists the Customer and sends it all useful documentation for:
    - the security of Personal Data;
    - the notification of a Personal Data Breach;
    - conducting the data protection impact assessment and consulting the supervisory authority where required;
- promptly and adequately processing Customer requests regarding the Processing of Personal Data in accordance with this Appendix; and
- assisting and cooperating with the Customer for the subcontracted Personal Data Processing, in particular vis-à-vis the supervisory authority.

2.2. Processor(s)

☐ No Processors

☒ Use of Processors

The Company undertakes to:

- recruit exclusively Processors who provide sufficient guarantees as to the implementation of physical, technical and organisational security measures so that the subcontracted Processing meets the requirements of the GDPR, taking into account the state of the art, implementation costs, nature, scope, context and purposes of the Processing;
- impose on its Processors all the requirements of this Appendix.

The Company's Processors existing at the time of acceptance of the GCU are deemed to have been authorised by the Customer under a general authorisation.

Upon signing these GCU, the Processors authorised by the Customer are:

- OVH for Site hosting (private cloud/dedicated server) - 2 rue Kellermann - 59100 ROUBAIX;
- Encrypted back up of dedicated servers - OVH Germany (Frankfurt)/Scaleway (Ile-de-France).

In the event of a change or replacement of Processor, the Company undertakes to:

- inform the Customer as soon as possible. In the event that the Customer raises objections, and if the Processor not approved by the Customer is necessary for the provision of the Services, the Company and the Customer undertake to reach an agreement on a solution accepted by both Parties;
- keep the list of Processors up to date;
- subject the Processor to the same obligations regarding the protection of Personal Data as set forth in this Appendix.

- ensure that the Processor complies with the obligations to which it is subject under this Appendix and the GDPR;
- upon first request, provide the Customer with a copy of the agreement with the Processor (s) and any subsequent amendments thereto;
- prohibit its Processors from transferring the Personal Data that is the subject of the CGU to third countries that do not have an equivalent level of protection to that of the EU without the Customer's prior written consent.

The Company remains fully liable to the Customer for any breach of the Personal Data protection obligations attributable to its Processors. The Company shall inform the Customer of any breach by the Sub-Processor of its contractual obligations.

2.3. Transfer of Personal Data to third countries

☒ No transfer outside the EU

☐ Transfer outside the EU

The Company undertakes not to transfer Personal Data to third countries or an international organisation that does not have a level of protection equivalent to that of the EU without the Customer's prior written consent. Any transfer of Personal Data to a third country or an international organisation by the Company shall be performed solely on the basis of documented instructions from the Customer.

In the event of a transfer authorised by the Customer, the Company undertakes to verify the existence of appropriate guarantees to regulate said transfer of Personal Data (standard contractual clauses of the European Commission, Binding Corporate Rules, etc.).

In the event that the Company is required to transfer Personal Data to a third country or an international organisation, under EU law or the law of the Member State to which it is subject, it must inform the Customer in advance of this obligation, unless the law in question prohibits such information for important reasons of public interest.

2.4. Security of processing

The Company undertakes to:

- take all appropriate technical and organisational measures to ensure the security, integrity, availability and confidentiality of the Personal Data it processes, including the use of pseudonymisation and encryption of Personal Data where necessary.
- grant members of its staff access to the Personal Data subject to the Processing only to the extent strictly necessary for the performance, management and monitoring of the agreement.
- ensure that the persons authorised to process the Personal Data undertake to respect confidentiality or are subject to an appropriate obligation of confidentiality.
- communicate to the Customer, at the latter's request, any useful documentation relating to the security of Personal Data (ISSP, SAP, etc.).

2.4.1. Sensitive data

If the Processing concerns special categories of Personal Data within the meaning of Article 9 of the GDPR, the Company applies specific limitations and/or appropriate safeguards.

2.5. Rights of Data Subjects

The Company undertakes to send to the Customer, to the contact address indicated by the latter, requests to exercise the rights of the Data Subjects of the Processing of Personal Data that it carries out, within FORTY-EIGHT (48) hours. It does not itself respond to these requests unless the Customer has expressly authorised it to do so.

The Company shall assist the Customer in fulfilling its obligation to respond to requests from Data Subjects to exercise their rights, taking into account the nature of the Processing.

2.6. Notification of Personal Data Breaches

The Company undertakes to notify the Customer of any Personal Data Breach as soon as possible and no later than within FORTY-EIGHT (48) hours after becoming aware of it. This notification shall contain at least:

- A description of the nature of the breach found (including, where possible, the categories and approximate number of data subjects affected by the breach and of Personal Data records affected);
- The contact details of a point of contact from whom additional information about the Personal Data Breach can be obtained;
- Its likely consequences and the measures taken or proposed to remedy the breach, including mitigation of any adverse consequences.

When and to the extent it is not possible to provide all the information at the same time, the initial notification shall contain the information available at that moment with additional information being provided as soon as it becomes available.

In the event of a Personal Data breach, the Company shall provide all relevant documentation to the Customer to enable it to notify the relevant supervisory authority and, where applicable, the Data Subjects.

2.7. Processor's Register/Data Protection Officer

In accordance with Article 30 of the GDPR, the Company declares that it keeps a written record of the Personal Data Processing carried out on behalf of the Customer which may be made available to the supervisory authority upon request.

2.8. Audit

The Company undertakes to cooperate with the Customer in the context of audits or inspections conducted by the Customer or any auditor appointed in agreement with the Company. Audits may also include inspections at the Company's premises or physical facilities and are, where applicable, conducted upon reasonable notice of FIFTEEN (15) days. Audits are conducted at the Customer's expense, once a year, during the Company's working days and opening hours. When deciding on an audit, the Customer may take into account the relevant certifications held by the Company.

Hosting of Vulnerability Reports - The Customer's Instructions as Data Controller

Categories of data subjects	Depending on the scope of the Program
Categories of Personal Data	Depending on the scope of the Program
Purpose of the processing	Hosting of Vulnerability Reports
Nature of the processing performed by the Company	Hosting of Personal Data contained in Vulnerability Reports
Categories of recipients	Processor: • Hosting OVH - France • Encrypted back up of dedicated servers - OVH Germany (Frankfurt)/Scaleway (Ile-de-France).
Fate of Personal Data	Intermediate archiving as of the request to close the Client account (Article 8 of the French Code of Criminal Procedure)
Security measures	YesWeHack ISSP

Management of Vulnerability Reports - The Customer's instructions as Data Controller

Categories of data subjects	Depending on the scope of the Program
Categories of Personal Data	Depending on the scope of the Program
Purpose of the processing	Management of Vulnerability Reports
Nature of the processing carried out by the Company	Access to Personal Data contained in Reports
Categories of recipients	Processor: not applicable
Fate of Personal Data	Access to Personal Data in the Customer area
Security measures	YesWeHack ISSP

3. Data processing carried out by the Company as joint data controller with MANGOPAY

The Company processes Personal Data relating to the Customer that is necessary for the creation and management of the eWallet, as Data Controller together with MANGOPAY, also Data Controller, in accordance with Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation) and Law No 78-17 of 6 January 1978 as amended.

MANGOPAY, a public limited company incorporated under Luxembourg law, having its registered office at 10 Boulevard Royal, L-2449 Luxembourg, registered with the Luxembourg Trade and Companies Register under number B173459, is authorised to provide payment and electronic money services as an electronic money institution authorised by the Financial Sector Supervisory Commission, 283 route d'Arlon L-1150 Luxembourg, www.cssf.lu.

MANGOPAY provides payment and electronic money services related to the payment of Hunters' Rewards through YesWeHack.

The Company and MANGOPAY, as joint data controllers for the processing of Personal Data, have entered into an agreement to govern their respective obligations with regard to the protection of Personal Data collected and processed in accordance with Article 26 of the GDPR.

3.1. Data Subjects and Personal Data concerned

The Data Subjects of the processing of Personal Data carried out by the Company are: the Customer's representative.

The Personal Data processed by the Company is:

- Identification data (surname, first name); Date of birth; Nationality; Country of residence; Email address; Telephone number
- Wallet data: Mangopay Wallet ID; management of Rewards; list of transactions

The above Personal Data is communicated by the Company to MANGOPAY, as it is necessary to subscribe to the MANGOPAY services and to open the account (Wallet). The details relating to the categories of Personal Data processed by MANGOPAY for the provision of its payment services can be found in the MANGOPAY T&Cs, which can be accessed at the following address: https://www.mangopay.com/terms/MANGOPAY_Terms-EN.pdf and in its Privacy Policy.

3.2. Purposes and legal basis for processing

Purposes and legal basis for the processing carried out by the Company

Purpose	Legal basis
• Creation of the Wallet (Collecting data on the Platform for transmission to MANGOPAY) • Management of the Wallet (management of Rewards, list of transactions) • Customer Relationship Management	Article 6 (1) (b) of the GDPR: *Performance of the Agreement*

• Management of requests related to the exercise of rights granted to data subjects by the processing of personal	Article 6 (1) (c) of the GDPR: *compliance with a legal obligation* (Article 12 of the GDPR)

Purposes of the processing carried out by MANGOPAY

Purpose	Legal basis
• Subscription to services and opening of the account (Wallet) in the books of MANGOPAY • The management of these accounts and the execution of payment transactions • The management of payment orders	Article 6 (1) (b) of the GDPR: *Performance of the Agreement* (validation of MANGOPAY T&Cs)
• The fight against identity fraud • The fight against external fraud • The fight against card payment fraud • Maintaining the security of both the MANGOPAY API and services in general • Statistics	Article 6 (1) (f) of the GDPR: *pursuit of legitimate interests, while respecting the fundamental rights and freedoms of data subjects* (legitimate interests deemed necessary for payment service provider activities)
• The fight against money laundering and terrorist financing • RNIPP consultation for inactive accounts • Cooperation with public authorities or any law enforcement or prudential supervision authority as part of an inspection or investigation	Article 6 (1) (c) of the GDPR: *compliance with a legal obligation*

3.3. Recipients of Personal Data

For the Company, the Personal Data of the Customer's representative is communicated to the authorised staff of the Company and its processor.

Upon acceptance of these GCU, the Processors are:

- OVH for Site hosting (private cloud/dedicated server) - 2 rue Kellermann - 59100 ROUBAIX;
- Encrypted back up of dedicated servers - OVH Germany (Frankfurt)/Scaleway (Ile-de-France).

For MANGOPAY, the recipients of the Personal Data that is processed for the provision of its services and for the achievement of its own purposes set out above can be found in the MANGOPAY T&Cs, which can be accessed at this address: https://www.mangopay.com/terms/MANGOPAY_Terms-EN.pdf and in its Privacy Policy.

3.4. Retention of Personal Data

As part of the management and performance of the Services, the Personal Data of the Customer's representative shall be retained throughout the term of the GCU / the Agreement and/or the last current purchase order. It is kept in intermediate archives for an additional period of 6 years for evidentiary purposes (criminal requirement in accordance with Article 8 of the French Code of Criminal Procedure), from the end of the Agreement and/or the last purchase order. It is deleted at the end of this period.

For MANGOPAY, the retention periods of the Personal Data that is processed for the provision of its services and for the achievement of its own purposes set out above can be found in the MANGOPAY T&Cs, which can be accessed at this address: https://www.mangopay.com/terms/MANGOPAY_Terms-EN.pdf and in its Privacy Policy.

3.5. Rights of Data Subjects

The rights granted to Data Subjects by the processing carried out by the Company are:

- the right of access, rectification and erasure of their data under the conditions provided for by the regulations (Articles 15 to 17 of the GDPR);
- the right to restrict the processing of this data under the conditions provided for by the regulations (Article 18 of the GDPR);
- the right to data portability under the conditions provided for by the regulations (Article 20 of the GDPR);
- the right to lodge a complaint with the CNIL;
- the right to define guidelines for access to their data in the event of death.

Requests relating to these rights can be exercised by email to the following address: privacy@yeswehack.com, specifying the purpose of the request (right concerned) and attaching any supporting documents identifying the requester (in case of doubt of the Company) or attesting to the mandate in case of representation.

The rights granted to Data Subjects by the processing carried out by MANGOPAY are:

- the right of access, rectification and erasure of their data under the conditions provided for by the regulations (Articles 15 to 17 of the GDPR);
- the right to restrict the processing of this data under the conditions provided for by the regulations (Article 18 of the GDPR);
- the right to data portability under the conditions provided for by the regulations (Article 20 of the GDPR);
- the right to object to the processing of data under the conditions provided for by the regulations (Article 21 of the GDPR);
- the right to lodge a complaint with the CNIL;
- the right to define guidelines for access to their data in the event of death.

For MANGOPAY, the details of the rights and the procedures for exercising these rights can be found in the MANGOPAY T&Cs, which can be accessed at this address: https://www.mangopay.com/terms/MANGOPAY_Terms-EN.pdf and in its Privacy Policy.