TERMS AND CONDITIONS (T&Cs)

Version dated 25 January 2023

These Terms and Conditions ("**T&Cs**") 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 Company customer subscribing to the Company's Services, as agreed in a Quote and/or Purchase Order (the "**Customer**") and registering on the Company's Platform accessible via the address: *https://yeswehack.com/auth/register* (the "**Platform**").

The Platform allows the Customer to choose amongst three (3) different types of Services: (i) Bug Bounty Programs, (ii) VDPs, and/or (iii) Pentest Management. Access to the Platform's Services is granted to the Customer only to the prior and unconditional acceptance of these T&Cs. This acceptance will be required at the time of registration of the Customer's account by the Customer's person of choice to represent the Customer in the management of the Services (the "**Customer Representative**"). Any action or omission of the Customer Representative shall be deemed an action or omission of the Customer.

In the event that the Customer has entered into a separate agreement (e.g., "Master Services Agreement" or "MSA") with the Company, terms of said agreement shall prevail over these T&Cs. Any capitalized terms used herein shall have the meaning given to them in Appendix 1.

1. SERVICES

The Platform. By subscribing to the Services, the Customer is allowed to use the Platform for the entire world and for the duration set out in the relevant Quote and/or Purchase Order. It is non-exclusive, personal, and non-transferable. It is given only to the Customer and solely for the purposes of creating the Programs and providing the Services.

The Customer shall not, and shall accordingly ensure that Users shall not:

i. reproduce, arrange or adapt all or part of the Platform, including but not limited to the integration of all or part of the Platform into any computer system, or other software solution, other than those provided for under these T&Cs, and
ii. carry out any form of commercial exploitation of the Platform or transfer, provide, lend, rent, sub-let, or otherwise use the Platform, or more generally, communicate to a third party, or an affiliated company, all or part of the Platform.

Access and Use of the Platform and the Services. The Company undertakes to procure all reasonable efforts and to implement all necessary technical means, in accordance with best practices, to ensure the availability and accessibility of the Platform and associated Services. For purposes of development, performance, or maintenance, the Company may modify all or part of the Platform.

The Company reserves the right to suspend all or part of the Services in the event of (i) a proven risk to the stability and/or security of the Platform, the Company's systems and environments, or the Services, (ii) a request from a competent administrative or judicial authority, (iii) an unlawful or fraudulent use of the Services, or use in violation of the rights of a third party, or (iv) any failure from the Customer or any of its Users to comply with any terms of these T&Cs. Such suspension may occur immediately and without notice in case of emergency or necessity, including, but not limited to, the situations described in (i), (ii) and (iii), and more generally, any use for which the Company is liable.

2. PROGRAM MANAGEMENT

Management by the Customer. Although the Company provides the Customer and its related Users, with support and assistance in the preparation and management of its Program, the Customer is solely responsible for the content, management, and administration of its Program. Therefore, it is to the sole responsibility of the Customer to define the scope of the Program, configure it in public or private mode, designate the Systems subject to the Tests, define the type(s) of the Tests, their periodicity, the exclusions, the amount of the Rewards, etc.

Inactive Program. When a Program is inactive (i.e., no interaction between the Customer and Hunters on the Platform for more than ninety (90) calendar days), the Company reserves the right to deactivate the Program, subject to a fourteen (14) business day prior written notice provided to the Customer, and to which the Customer failed to respond and/or to take corrective action.

3. PAYMENT

Fees and Rewards. In consideration for the Services, the Customer undertakes to pay a lump-sum and flat-rate agreed with the Company, as detailed in the Quote and/or Purchase Order (the "**Fees**"). The Customer shall also make a pre-payment of the agreed Hunter Rewards which the Company agrees to process on behalf of the Customer for use within the Platform. The Fees are not refundable. Any additional use or service shall be subject to a separate and new Quote and/or Purchase Order approved by the Parties.

Payment Terms and Consequences for Non-Payment. Prices are quoted exclusive of VAT. Amounts on invoices are to be paid in full and free of any tax deduction or levy of any kind, including without limitation withholding tax, or any other similar charge at the applicable rate. The Customer shall be responsible for payment of all such taxes, and any related penalties and interest.

Invoices shall be drawn up according to the price agreed in the Quote and/or Purchase Order, and payable net and without discount, upon receipt of the invoice, unless otherwise stated in the Quote and/or Purchase Order. Upon request from the Customer to the Company, the Company shall issue further invoices for the Customer to top-up its Wallet when needed. Shall the customer be in arrears with payments, the Company may charge late payment penalties equal to three (3) times the applicable legal interest rate besides a lump indemnity of forty euros (40€) for collection costs as set by the applicable legislation or its updated amount. The starting date of the calculation of the aforementioned will be the day following the due date of the invoices.

In the event of a payment default, the Company reserves the right to restrict, limit or suspend access to the Platform and/or use of the Services. The Company also reserves the right to terminate these T&Cs, including any separate agreement, Quote and/or Purchase Order.

The Customer cannot, under any circumstance, claim any compensation from the Company due to the restriction, limitation, or suspension of the Platform and/or the Services as a consequence of a payment default.

Wallet for Payment of Hunters' Rewards. Hunters' Rewards are deposited, stored, and paid through a Wallet managed and controlled by an authorised and regulated payment service provider used by the Company. A Wallet will be created subject to the Customer Representative providing the required information and accepting the T&Cs on the Platform. The Customer and its Users are informed of the balance of the Wallet through the Customer account on the Platform.

Payment of Rewards to Hunters. Rewards to Hunters shall be awarded immediately through the Platform. Relevant Users of the Customer shall first validate the amount via the dedicated account on the Platform and make payments online using the Wallet.

4. TERM - TERMINATION

Term. These T&Cs will come into force on the date of creation of the Customer account by the Customer representative using the dedicated registration form on the Platform. They will remain in force until the completion of the last Purchase Order in effect and until a Customer decides to close its account on the Platform.

Termination. The Company may, as of right, revoke access to the Platform and use of the Services, in the event of (i) the Customer's or any of its User's breach of these T&Cs or any other agreement in place, if said breach hasn't been remedied within fifteen (15) calendar days of receipt of a notice of default via registered letter with acknowledgement of receipt, (ii) a total or partial payment default by the Customer, (iii) the filing of voluntary or involuntary bankruptcy or insolvency proceedings by the Customer, subject to applicable law, and (iv) malicious, unlawful, or fraudulent use of the Platform and/or Services or use in violation of the rights of any third party or any mandatory provisions, by email and without prior notice. This right is without prejudice to any damages that may be claimed by the Company to the Customer.

Archiving and Destruction. Upon expiry or termination of the Services for any reason whatsoever, all information relating to the use of the Services, i.e., data of any kind, including Confidential Information, Personal Data, as well as Vulnerability Reports, will be retained by the Company to comply with its applicable legal obligations in accordance with statutory periods. At the expiry of such statutory periods, they will be completely removed from the Company's databases and systems.

5. INTELLECTUAL PROPERTY

IPRs. All IPRs owned directly or indirectly by the Company and all materials made available to the Customer by the Company (including but not limited to all accessible information, text, photos, images, sounds, data, databases, and downloadable Bug Bounty Programs, including software and other underlying technology) as part of the Services and the performance of the T&Cs, shall remain the exclusive property of the Company or the third parties that have granted the Company the right to use them. The Company grants the Customer the right to use said materials made available to it, on a non-exclusive basis, solely in connection with the use of the Platform and the Services and within the limits and during the Term of these T&Cs. The Customer shall not reproduce, imitate, or affix, in whole or in part, any trademarks, designs, or any Company's IPRs without the Company's prior written consent.

Warranty. The Company warrant that it owns all IPRs necessary to enable it to perform its obligations under these T&Cs.

Ownership of the Customer's Programs and Right to Use the Systems. The Customer is the owner of its Systems and grants the Hunters the right to use said Systems for the entire duration of the Bug Bounty Program as defined by the Customer, on a personal, free, and non-exclusive basis, for the entire world. This right is granted to the Hunters alone, exclusively for the purpose of carrying out the Tests, subject to the rules and restrictions of the Program. As part of these T&Cs and the performance of the Services, the Customer hereby grants the Company a non-exclusive, non-transferable, global, and royalty-free licence (which cannot be sub-licenced) to use, copy, reproduce, display, and transmit copies of the Customer's Program to the designated Hunters under a Private Program or to all Hunters under a Public Program.

Hunters' Vulnerability Reports. The Customer agrees to transfer automatically to the Company the rights to all or part of the Vulnerability Reports under the express prior condition that the Company only processes Anonymised Data (i.e., not identifiable, or traceable to the Customer), and solely and exclusively within the following limits: the Company collects certain aggregated and anonymised statistical information from Vulnerability Reports and the Customer's use of the Platform and Services for, among other purposes, reports,

research, statistics, improvements to the Platform and Services. Anonymized Data does not constitute Personal Data nor Confidential Information.

6. CONFIDENTIALITY

Confidential Information. All information exchanged between the Company and the Customer, whether in oral or written form and whatever the medium, (and in particular any document, file, object, record, data, study, letter, project, plan, diagram, software, material, program or production, processes, methods, components) as well as activities, strategies, products and services (current or future), commercial policies, financial and legal information or data, research and development activities, projects, trade secrets and know-how, personnel concerning directly or indirectly the Parties, any company or related entity, shall be deemed confidential (hereinafter "**Confidential Information**").

The Company and the Customer expressly undertake:

i. to keep strictly confidential all Confidential Information and not to disclose it to third parties, in whole or in part, directly or indirectly, without the prior written consent of the other;
ii. not to make duplications or reproductions, by any means, in any manner whatsoever, in whole or in part, of the Confidential Information except for those strictly necessary for the performance of the Services, and
iii. not to use the Confidential Information directly or indirectly, for any purpose other than the performance of the Services.

These confidentiality obligations extend to all employees, staff, trainees, managers, and agents, as well as their affiliated counsel and co-contracting parties, to whom Confidential Information may only be sent if they are bound by the same confidentiality obligations as set out herein.

Confidentiality obligations do not apply when:

i. it can be proven that the Confidential Information was lawfully known prior to the Quote and/or Purchase Order;
ii. the Confidential Information was in the public domain at the time of disclosure;
iii. the Confidential Information is publicly available by publication or any other means of communication, unless this is the result of a fault or negligence on the part of the party receiving such information;
iv. where the party receiving the information can prove that it has been provided or can be provided to it by a third person without a breach of confidentiality, and
v. by operation of law, regulation, or order of a competent authority (including a regulatory or governmental body or stock exchange authority), one of the parties is obliged to disclose it, provided that, where practicable, the other party has been notified as soon as possible to enable it to pursue any legal remedy for protection.

The Company and the Customer undertake to immediately notify each other of any event, whether dependent on or beyond its control, likely to affect the confidential nature of Confidential Information (such as theft or loss of Confidential Information, etc.).

7. PERSONAL DATA

Appendix 2 to these T&Cs details information about the processing of Personal Data carried out by the Company, in its capacity as either data controller, data processor or joint data controller, in accordance with the GDPR. It sets out the purposes and legal basis for the processing activities been carried out, the data subjects and data concerned, the recipients of the data, the retention period, and the data subjects' rights.

8. LIABILITY

The Customer's Liability. The Customer shall:

i. undertake to use the Platform and Services in accordance with these T&Cs;
ii. be solely responsible for its Customer Representative and Users, including the management of User accounts and the means of authentication (such as identifiers, passwords, etc.) associated therewith;
iii. ensure that the conditions under which the Services ordered are made available comply with its requirements, and are suitable for the relevant legal and regulatory requirements; it being specified, without limitation, that abusive or fraudulent uses of the Services and of the resources made available to the Customer are prohibited, notably uses which may jeopardise the stability and security of the Company's systems or which may lead to a deterioration in the performance of the Services provided to other Company's customers.

Subject to the Hunter's compliance with the rules set by the Bug Bounty Program and the General Conditions of Use, the Customer acknowledges that:

i. any Test conducted by the Hunters as part of a Bug Bounty Program is authorised and operated with the Customer's express consent and under its sole responsibility;
ii. the acts carried out by the Hunters are free of fraudulent character, and cannot, in such cases, be qualified as a breach of an automated data processing system under the law nor classified as acts of infringement under the law;
iii. it may not sue the Hunter for acts performed in the context of a Bug Bounty Program under criminal or civil law, being specified that the Company cannot be held liable for any breach by the Hunter of its obligations; and
iv. it expressly waives, in advance, the civil interest that may result from the prosecution by the public prosecutor's office or any other prosecuting authority of an offence committed within the framework of a Bug Bounty Program.

As such, the Customer shall hold the Company harmless against any third-party claims relating to the performance of the Tests, provided that the Company shall (i) promptly notify the Customer in writing of the claim, (ii) authorise the Customer to conduct the defence and all settlement negotiations on its own, and (iii) fully cooperate with the Customer.

The Company's Liability. The Company undertakes to provide all reasonable efforts (obligation of means) to:

i. provide the Customer with the necessary resources (T&Cs, FAQ, Documentation, demonstration, advice and assistance) enabling the Customer to become aware of and understand the characteristics and use of the Services;
ii. exercise all due care and diligence in providing quality Services;
iii. have a team dedicated and in charge of supporting the Customer;
iv. promptly notify the Customer of any difficulties it may encounter in providing the Services; and
v. notify the Customer within seventy-two (72) hours of any incident that has had a direct impact on the confidentiality or integrity of Customer data, other than Personal Data (see Appendix 2). No liability shall arise if the Company has been prevented from giving timely notification.

The Company's liability is strictly limited to the obligations set forth in these T&Cs and to direct losses actually suffered by the Customer resulting from the Company's breach of these T&Cs, provided that such losses were foreseeable at the time the T&Cs were entered into and is a direct and immediate result of the breach of these T&Cs by the Company.

The Company shall under no circumstance be liable for:

i. use or misuse of the Platform and/or Services by the Customer, the User, the Hunter, the Security Researcher and the Penetration Tester;

ii. non-performance, failure, malfunction, or unavailability of the Platform and/or Services resulting from a third party's, the Customer's, the User's, a Hunter's, a Security Researcher's or Penetration Tester's (with the exception of any data processors of the Company, if applicable) action or omission;
iii. failure of the Customer to fulfil its obligations (e.g., inaccuracy, error, omission) in the definition and management of the Program;
iv. non-compliance with the 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 set out herein; 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 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. The Company shall therefore not be liable for any damage caused by a Customer, a User, a Hunter or a Security Researcher's failure to partially or totally perform its/their obligations.

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.

Limitation of Liability. The Company shall not be liable for any indirect damages, loss of profits, revenue, anticipated revenue, data, use, goodwill or for any incidental, special, punitive or consequential damages of any nature suffered by the Customer in connection with the Services or any act or omission arising out of or in relation to the Services, whether or not the possibility of such damages was disclosed or could have been reasonably foreseen. The foregoing limitation of liability and exclusion of certain damages shall apply regardless of the success or effectiveness of other remedies.

Except for liability which cannot by applicable law be excluded or restricted, the Company's aggregate liability for any loss or damage in connection with the Services will not in any case exceed the total amounts paid by the Customer to the Company during the twelve (12) months preceding the claim of damages. Under penalty of foreclosure, the period of action against the Company may not exceed two (2) years after the Customer has been aware of the event or circumstances leading to the claim.

Infringement of IPRs. Nothing herein shall restrict, limit, or cap in any way the rights of a party for violation or infringement of its IPRs by the other party.

9. GENERAL

Force Majeure. The Company shall not be liable for any delay or non-performance of the Services arising from a Force Majeure event. The Company will immediately notify the Customer and shall make every effort to reduce as much as possible the harmful effects resulting from this situation. The Company shall bear all costs incumbent upon it resulting from the occurrence of the Force Majeure event. If an event of Force Majeure results in the Company having to suspend the performance of the Services for more than thirty (30) calendar days, the Company may terminate as of right the Services with immediate effect and without any compensation being due to the Customer.

For the avoidance of doubt, any sums invoiced or to be invoiced by the Company for Services rendered prior to the occurrence of the Force Majeure event shall remain due to the Company. The same shall apply with regards to any damages due by the Customer to the Company for a breach which occurred prior to the Force Majeure event.

Independence of the Parties. The Company and the Customer shall be and act as independent contractors and nothing herein shall render them as partners or joint venture parties.

Notices. Any notice 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 in the relevant Quote and/or Purchase Order or at any other address notified in accordance with this article. A notice shall be deemed as received by a party on the first business day following the first presentation to that party.

No Waiver. No failure to exercise and no delay in exercising any right, remedy, power, or privilege hereunder shall operate as a waiver hereof; nor shall any single or partial exercise of any right, remedy, power, or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.

Severability. If one or more provisions of these T&Cs are held to be invalid or null and void pursuant to a law, a public policy provision, a regulation or following the final decision of a court, it shall be deemed unwritten, but it shall not affect the validity of the other provisions.

Survival. Any provision or condition of these T&Cs intended to survive such their end or expiry 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 T&Cs which, by their nature or by virtue of specific provisions, extend beyond the end or expiry of these T&Cs.

Assignment. No prior consent will be required if the Company assigns, sells or otherwise transfers to an affiliate or a successor in interest by way of merger, reorganization, change of control, consolidation or amalgamation; or as part of a sale of all or substantially all (50% or more) of the Company's assets.

Hypertext Links. The T&Cs may contain hypertext links to third-parties legal documents over which the Company has no control. The Customer 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 Customer.

Governing Law and Jurisdiction. These T&Cs are governed by French law. The Parties shall endeavour to settle amicably any dispute that may arise between them. Any dispute or claim arising out of or in connection with these T&Cs 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.

APPENDIX 1: DEFINITIONS

Anonymised Data: refers to data that has undergone transformation by anonymisation techniques in combination with assessment of the risk of re-identification and that does not allow to identify individuals. Anonymised Data shall not be deemed Personal Data nor Confidential Information.

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**").

Documentation: means the User documentation made available by the Company in connection with the use of the Services consisting of online documentation and in general, all technical, operational, or functional information relating to the Platform.

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.

GDPR: means "General Data Protection Regulation" (EU) 2016/679, the regulation on data protection and privacy in the European Union (EU) adopted on 14 April 2016 and became enforceable beginning 25 May 2018.

Hunter: means an independent individual or legal entity, IT security researcher, who may act in a professional or non-professional capacity, 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.

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).

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.

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.

Program: means either the Bug Bounty Program and/or the VDP, as applicable.

Purchase Order: means the document accepted by the Parties setting out the description of the Services being ordered, their price, and payment terms, and which confirms the Customer's subscription to the Services.

Quote: means the commercial proposal communicated by the Company and accepted by the Customer in the corresponding Purchase Order.

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.

Security Researcher: means, in the context of the Vulnerability Disclosure Policies (VDP), the security researcher who is allowed to publicly provide information on the Vulnerability through a security online form on the Platform.

Services: means access to the Platform and any Services made available to the Customer by the Company and purchased by the Customer in accordance with a Purchase Order and/or a Quote.

Systems: means the Customer's systems (including servers, websites, applications, software, modules, interfaces, connected objects etc.) on which the Tests shall be carried out by the Hunter.

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.

User: means the individual or Penetration Tester appointed by and representing the Customer to use the Platform and the Services. Any action or omission of the User shall be deemed an action or omission of the Customer.

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, as set forth in a Quote and/or a Purchase Order or otherwise mutually agreed by the Company and the Customer, 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 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: PROTECTION OF PERSONAL DATA

The purpose of this Appendix is to set out the rights and obligations of the Customer and the Company with regard to the protection of Personal Data under these T&Cs.

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 T&Cs.

In the context of these T&Cs and/or a Quote or a Purchase Order, 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 agreement between the Company and the Customer; • 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	Article 6 (1) (f) of the GDPR: *pursuit of legitimate interests, while respecting the fundamental rights and freedoms of data subjects*

(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)	
• 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 T&Cs, 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 agreement between the Company and the Customer, the Personal Data of the Customer's representative shall be kept throughout the term of the relevant Quote and/or 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 relevant Quote and/or Purchase Order. It is deleted at the end of this period.

In the context of the performance of these T&Cs 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 these T&Cs are deemed to have been authorised by the Customer under a general authorisation.

Upon acceptance of the T&Cs, 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 covered by the T&Cs, 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 T&Cs 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 between the Company and the Customer.
- 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 the T&Cs, 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 a relevant Quote and/or Purchase Order, the Personal Data of the Customer's representative shall be retained throughout the term of such Quote and/or 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 relevant Quote and/or 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.