TERMS AND CONDITIONS (T&Cs)

Version 7.0 dated 22nd January 2025

These Terms and Conditions ("**T&Cs**") define the terms and conditions which apply between the Yes We Hack contracting entity as specified in the Purchase Order (the "**Company**") and any company customer subscribing to the Company's Services, as agreed in a Purchase Order (the "**Customer**") and registering on the Company's Platform accessible via the address: https://yeswehack.com/auth/register (the "**Platform**").

The Customer acknowledges that Customer's physical address will determine (i) the Company contracting entity (as specified in the Purchase Order), (ii) the address to which the Customer should direct notices under these T&Cs, (iii) the law that will apply in any dispute or lawsuit arising out of or in connection with these T&Cs, and (iv) the courts that have jurisdiction over any such dispute or lawsuit.

The Platform allows the Customer to choose amongst five (5) different types of Services: (i) Bug Bounty, (ii) VDPs, (iii) Featured VDP, (iv) Pentest Management and/or (v) Attack Surface 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 (i.e., "**Master Services Agreement**" or "**MSA**") with the Company, terms of said agreement shall prevail over these T&Cs. Otherwise, these T&Cs constitutes the entire commitments of the Customer and the Company and supersede all written and verbal agreements delivered or exchanged between them. Terms and conditions contained in the Purchase Order will have no force or effect.

Any capitalized terms used herein shall have the meaning given to them in Appendix 1.

1. SERVICES

The Platform. When the Customer subscribes to the Services, the Company grants to the Customer a right to use the Platform as set out in Article 5 (Intellectual Property) and subject to compliance with the terms of these T&Cs.

The Customer's Affiliates may access and use the Services (including top up the Customer's Wallet) under these T&Cs, subject to the Company's prior approval and provided that such access and use is consistent with the scope and terms set out in the relevant Purchase Order. However, the Customer remains solely and fully responsible and liable for all acts and omissions of its Affiliates as if such acts and omissions were the Customer's own. Notwithstanding the foregoing, the Customer shall, in all respects, remain the exclusive counterpart of the Company in relation to the relevant Purchase Order.

Access and Use of the Platform and the Services. The Company undertakes to procure all reasonable efforts and to implement all necessary technical means, per 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) 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 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 Security Researchers 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 Purchase Order (the "**Fees**"). The Fees are not refundable. The Customer shall also make a pre-payment of the mutually agreed estimated amount of Rewards which the Company agrees to process on behalf of the Customer for use within the Platform. If payment is made by the Customer in a local currency which is not available within the Platform, any currency conversion charges shall be borne by the Customer. Any additional use or service shall be subject to a separate and new Purchase Order.

Taxes and other charges. Prices are quoted exclusive of value-added tax (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, bank fees, or any other similar charge at the applicable rate. The Customer shall be responsible for payment of all such taxes or charges, and any related penalties and interest.

Payment Terms. Invoices shall be drawn up according to the price agreed in the Purchase Order, and payable net and without discount upon receipt of the invoice, unless otherwise stated in the 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.

Non-payment. In the event of total or partial 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 and/or Purchase Order.

The Company shall have the right to offset any balance or amounts due from the Customer with the amounts credited in the Customer's Wallet.

The Customer shall not, 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.

Payment of Rewards.. Upon activation of its Subscription on the Platform, the Customer and its Users are able to consult its balance, and any subsequent payments, through its dedicated account on the Platform. To reward a valid Vulnerability Report, the Company shall ensure payments of Rewards to the Security Researchers using the Wallet, after validation by the Customer on its account. Upon termination for cause of the relevant Purchase Order, any amount remaining in the Customer's balance shall be reimbursed by the Company to the Customer to the extent that all Rewards have been fully paid to Security Researchers.

4. TERM - TERMINATION

Term. These T&Cs are effective as of the date of creation of the Customer account by the Customer representative ("**Effective Date**") using the dedicated registration form on the Platform. They are entered into for an initial period indicated in the initial Purchase Order ("**Initial Subscription Term**"). If the initial Purchase Order does not specify a start date, it shall be deemed to be the Effective Date. At the end of this Initial Subscription Term, the Customer may at any time request the renewal of its subscription for another period agreed between the parties and subject to a new Purchase Order. Unless otherwise agreed in writing between the parties, the Company shall continue to perform the existing Purchase Orders until their expiry, and the parties shall remain bound by the obligations herein until the completion of the last Purchase Order in effect at the date of expiration.

Termination for cause. The Company may immediately revoke access to the Platform and use of the Services, upon (i) the Customer's or any of its User's material breach of its obligations hereunder which has not been remedied within fifteen (15) days of the Customer's receipt of written notice describing the breach in reasonable detail, (ii) 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, and (iii) the filing of voluntary or involuntary bankruptcy or insolvency proceedings by the Customer, subject to applicable law. Terminations for cause are 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 for the sole purpose of complying with its applicable legal obligations in accordance with statutory periods. At the expiry of such statutory periods, they will be completely removed, at the Customer's request, from the Company's databases and systems.

5. INTELLECTUAL PROPERTY

IPRs. The Company does and will retain all proprietary and IPRs, title, and interest in and to the Platform and the Materials. For the purpose of this Article, "**Material**" includes any materials made available to the Customer by the Company (including but not limited to all accessible information, text, photos, images, sounds, data, databases, and standard templates of Programs and templates of Vulnerability Reports, including software and other underlying technology) as part of the Services and the performance of the T&Cs.

The Company hereby grants to Customer a worldwide, non-exclusive, non-transferable, and non-sublicensable right to use the Platform and Materials, solely in connection with the use of the Platform, for the duration of the Purchase Order and exclusively for providing the Services within the limits of these T&Cs.

The Customer 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 Affiliate all or part of the Platform.

Company's warranty. The Company warrants 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 Systems are the exclusive property of the Customer or the third parties that have granted the Customer the right to use them under the terms and conditions defined in these T&Cs. The Customer grants to the Company (for the ASM and Triage Services) and the Security Researchers (for performing their Tests under a Program) the right to use said Systems for the entire duration of the Services or Program, on a personal, free, and non-exclusive basis, for the entire world. The rights hereabove are granted exclusively for the purpose of performing the Services and carrying out the Tests, subject to the rules and restrictions of the Program. As part of these T&Cs and the performance of the Bug Bounty and Featured VDP Services, the Customer hereby grants the Company a non-exclusive, non-transferable, global, and royalty-free license (which cannot be sub-licensed) to use, copy, reproduce, display, and transmit copies of the Customer's Program to the Security Researchers.

Indemnification. The Customer warrants that it owns all IPRs necessary to enable it to perform its obligations under these T&Cs. The Customer agrees to indemnify, defend, and hold harmless the Company from and against any and all third-party claims and causes of action, as well as related losses, liabilities, judgments, awards, settlements, damages, expenses, and costs (including reasonable attorney's fees and related court costs and expenses) incurred or suffered by the Company relating to or arising out of the violation or infringement of third-party intellectual property rights caused by the Customer's content, data, materials, or other contributions submitted, uploaded, or otherwise provided in connection with the Services offered through the Platform.

Indemnification procedure. To obtain indemnification, the Company shall: (i) give written notice of any claim promptly to the Customer; (ii) give the Customer, at its option, sole control of the defense and settlement of such claim, provided that Customer may not, without the prior consent of the Company (not to be unreasonably withheld), settle any claim unless it unconditionally releases the Company of all liability; (iii) provide to the Customer all available information and assistance; and (iv) not take any action that might compromise or settle such claim.

Statistical Data. Without limiting the confidentiality rights and Intellectual Property Rights protections outlined in these T&Cs and in compliance with applicable intellectual property laws, the Company has the right to collect and use aggregated and anonymized statistical information (i.e., metadata such as scoring of Vulnerability, resolution time of Vulnerability) ("**Statistical Data**") from Vulnerability Reports and/or derived from the Customer's use of the Platform and Services, and nothing herein shall be construed as prohibiting Company from utilizing the Statistical Data for business and/or operating purposes. Statistical Data does not allow

to identify individuals nor to trace back to the Customer. For the avoidance of doubt, the Company shall not use any of its rights thereof to harm the Customer, or its Systems, or to damage the Customer's image or its activities.

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 (except Statistical 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 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

For the purpose of managing their contractual relationship and meeting their accounting and financial obligations, each party processes the Personal Data of the other party's employees, officers, representatives, or consultants as a data controller. Furthermore, for the purpose of providing access to its Platform, the Company processes the Personal Data of the Users, as a data controller or joint controller with its payment service provider. The details of these processing activities are available in the Platform Privacy Policy at: https://yeswehack.com/auth/register.

In addition, Appendix 2 to these T&Cs details information about the processing of Personal Data carried out by the Company, in its capacity as data processor of the Customer, in accordance with the GDPR. It sets out the purposes of the processing activities being carried out, the data subjects and data concerned, the recipients of the data, the retention period, and the data subjects' rights.

8. OBLIGATIONS

The Customer's obligations. The Customer shall:

i. undertake to use the Platform and Services in accordance with these T&Cs and the applicable GCUs;

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. regularly review its rights and authorizations on the Systems to be monitored under the ASM Service and accordingly maintain the list of the Systems updated in the Platform;
iv. 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 jeopardize 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 Security Researcher's compliance with the rules set by the Bug Bounty Program and the GCUs, the Customer acknowledges that:

i. any Test conducted by the Security Researchers as part of a Bug Bounty Program is authorized and operated with the Customer's express consent and under its sole responsibility;
ii. the acts carried out by the Security Researchers 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 Security Researcher 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 Security Researcher 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 offense committed within the framework of a Bug Bounty Program.

The Company's obligations. The Company shall provide all reasonable efforts to:

i. provide the Customer with the necessary resources (GCUs, 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 the Services in accordance with these T&Cs, including having a team dedicated to supporting the Customer in the drafting of its Programs, and to promptly notify the Customer of any difficulties it may encounter in providing the Services;
iii. ensure that the GCUs allow for the transfer of ownership of the Vulnerability Reports from the Security Researcher to the Customer.

The Company shall under no circumstance be liable for:

i. use or misuse of the Platform or Services, including but not limited to Customer's failure in the definition and management of the Program (i.e., inaccuracy, error, omission), nor for any malfunction of the Platform resulting from Customer, User, or a third party's (including Security Researcher's) actions or omissions;
ii. non-compliance with the GCUs, violation of the rules of the Program or any other agreement by the Security Researchers;
iii. for security incident related to a Vulnerability that has been reported but not dealt with, or to a Vulnerability that has not been identified as part of the Service, or for the disclosure of sensitive data resulting from security negligence on the part of the Customer;
iv. suspension of access to the Platform and/or the Services under the conditions set out herein; and
v. incidents due to the use of the Internet (e.g. loss of connectivity…).

As part of its Bug Bounty Services, the Company acts as an intermediary to introduce Security Researchers to the Customer. Selection and invitations of Security Researchers is done at the Customer's discretion. To help the Customer in its choice, the Company has set up a ranking system for Security Researchers in order to stimulate their commitment and to allow the Customer to select Security Researchers according to certain indicators and criteria (point/ranking/gamification system on the Platform). However, the Customer remains responsible to invite or disinvite any Security Researcher. The Customer may also invite any new Security Researchers to register on the Platform.

As part of the Featured VDP Service, the Company provides the Customer with access to all Security Researchers registered on the Platform. Restrictions for the Feature VDP Program may be defined by the Customer, and any Security Researcher meeting the conditions set out in the Program may participate.

The Company reserves the right to cancel and/or suspend the Security Researcher's access to the Platform in the event of any breach of the GCUs or the rules of the Programs by the Security Researcher.

Security Researchers shall at all-time be considered as the sole editor of the Vulnerability Reports which cannot be edited/tampered with by the Company, including as part of the Triage Service. Security Researchers are the sole responsible 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.

In consideration of the foregoing, the Company shall therefore not be liable for any damage caused by a Customer, a User, a Security Researcher's failure to fulfil its/their obligations partially or totally.

9. 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 arising under the infringement provision of these T&Cs, the Company's willful misconduct or gross negligence, or 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 amount of the Fees 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.

10. GENERAL

Force Majeure. The Company shall not be liable for any delay or non-performance of its obligations under these T&Cs 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 before 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 that occurred before 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 Purchase Order or at any other address notified per 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 or delay in exercising any right, remedy, power or privilege hereunder shall be construed as a waiver hereof; nor shall any single or partial exercise of any right, remedy, power or privilege hereunder be construed as precluding any subsequent exercise of such right or remedy 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 the laws of the country where the Company's contracting entity is registered, as specified in the relevant Purchase Order. 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 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 located at the registered seat of the Company's contracting entity, as indicated in the relevant Purchase Order, and the parties hereby irrevocably submit to the exclusive jurisdiction of those courts for these purposes.

APPENDIX 1: DEFINITIONS

Affiliate(s): any entity which, directly or indirectly, is owned or controlled by the Company or the Customer or is under common ownership or control with the Company or the Customer. For the avoidance of doubt, and subject to applicable law, a legal entity shall be deemed controlling another when it, either directly or indirectly, (i) owns more than 50% of the share capital; or (ii) has the power to appoint or dismiss most of the administrative members of the administrative body, or may hold most of the voting rights by virtue of agreements reached with other shareholders; or (iii) holds the management control as a result of rights, agreements or other means that grant the possibility of exercise a decisive influence on the company activities.

Attack Surface Management (ASM): means the solution allowing the Customer to continuously monitor its Systems for security flaws from an external perspective, enabling the Customer, actively or passively, to (i) discover assets; (ii) identify internet-facing and reachable services; (iii) characterize technologies; (iv) seek potential Vulnerabilities.

Bug Bounty: means the Service enabling the Customer to manage Bug Bounty Programs.

Bug Bounty Program(s): means the program created by the Customer to invite Security Researchers to conduct Tests on its Systems, and which shall contain a comprehensive description of the terms, conditions and requirements to which Security Researchers 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 Security Researchers who are invited to and participate in such Program. The Customer may choose to run the Program in (i) private mode, where only Security Researchers 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 Security Researcher 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.

Featured Vulnerability Disclosure Policies ("Featured VDP") Program: means the program created by the Customer and accessible on the Platform to allow Security Researchers to report security issues and Vulnerabilities to the Customer. As with the VDP Service, no Rewards or other compensation are provided to Security Researchers (e.g., Security Researchers will not receive any ranking points).

Force Majeure: means an event or circumstance beyond the reasonable control of the affected party, which could not be reasonably foreseen at the time of execution of the Purchase Order 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, national and/or multi cross-sector strikes, accidents, riots or civil disturbance, acts of government, lack of power and delays by suppliers or materials shortages of transportation, facilities, fuel, energy, labor, 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.

GCUs: means the General Conditions of Use, including the relevant provisions applicable to the Security Researchers registered on the Platform, which are accessible on the Company's website: https://yeswehack.com/auth/register#create-company.

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 (PTM): means the solution enabling the Customer to manage and optimize the process and reporting of penetration tests campaigns carried out by Security Researchers using a unified management solution provided within the Platform. For the avoidance of doubt, in this context, Security Researchers may be Users of the Platform.

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 GDPR.

PSP: refers to the Company's trusted third-party Payment Service Provider, subject to the EU Directive 2015/2366 known as "PSD2", which is used by the Company to enable the use of the Wallet functionality on the Platform and to facilitate the payment of Rewards.

Program(s): means either the Bug Bounty Program, the VDP Program, and/or the Featured VDP Program, as applicable.

Purchase Order(s): means the ordering document in a format accepted by the parties (including but not limited to the commercial proposal communicated by the Company and accepted by the Customer) setting forth the Services to be provided by the Company and the corresponding financial terms, and which confirms the Customer's subscription to the Services.

Reward(s): means the financial reward to be awarded to the Security Researcher, by the Customer to the Security Researcher in consideration of a valid Vulnerability Report in the context of a Bug Bounty Program. Payment of Rewards is further detailed in Article 3.**Security Researcher(s)**: means an independent individual or legal entity, IT security researcher, who may act in a professional or non-professional capacity depending on the context of the Services. As part of (i) the Bug Bounty Service, the security researcher registers on the Platform and submits Vulnerability Reports in return for a Reward (ii) the VDP Service, the security researcher is allowed to provide information on Vulnerabilities through a secured and publicly accessible online form (iii) the Featured VDP Service, the security researcher registers on the Platform and submits Vulnerability Reports without a claim for Reward or other compensation (iv) the Pentest Management Service, the security researcher (e.g., the penetration testing company) works for the Customer, as part of a separate agreement, and under the latter's responsibility to conduct penetration tests. For the avoidance of doubt, Security Researchers are neither employees nor subcontractors of the Company.

Services: means access to the Platform and any services made available to the Customer by the Company and purchased by the Customer under a Purchase Order.

Systems: means the IT systems and internet-exposed assets (e.g., servers, websites, applications, software, modules, interfaces, connected objects, etc.) designated by the Customer on the Platform. In the context of Bug Bounty, VDP, Featured VDP and PTM Services, the systems are those on which the Tests shall be carried out by the Security Researcher. As part of the ASM Service, the Customer defines a detailed and exhaustive list of the systems to be monitored.

Tests: means, in the context of Bug Bounty, VDP, Featured VDP and PTM Services, the tests that the Customer wishes to have carried out by a Security Researcher. These Tests are technical in nature including any action to reach or enter a Customer's System, analyze the level of security in place and search for Vulnerabilities. In the context of the ASM Service, the tests consist of continuous automated monitoring of the Systems.

User(s): means the Customer employee (including those of any of its Affiliates) or any third-party (including the Security Researchers in the context of the PTM Service), appointed by and representing the Customer who uses the Platform and the Services on behalf of the Customer. Any action or omission of the User shall be deemed an action or omission of the Customer.

Vulnerability Disclosure Policies (VDP) Program: means a secured and structured channel accessible online via the internet and hosted on the Customer's domain enabling Security Researcher (whether or not registered on the Platform) to report Vulnerabilities found on the Customer's Systems.

Vulnerability Report(s): means the document containing technical data in a standardized format, along with any relevant attachments of a functional nature, describing the Vulnerability discovered and issued by a Security Researcher and submitted to the Customer on the Platform.

Vulnerability(ies): 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 Report Management Services (or "Triage"): means the additional service, as set forth in 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 Security Researcher, communicating with these Security Researchers and (if applicable) carrying out actions on the Systems in the context of Vulnerability reproduction. This Service can be added to Bug Bounty or VDP Services only.

Wallet: means the online payment tool available on the Platform to allow the upload, storage and payment of the Rewards as set out in Article 3. The Wallet functionality is enabled through integration with the PSP which is responsible for payment processing and compliance with applicable financial regulations.

APPENDIX 2: PROTECTION OF PERSONAL DATA

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

The Services provided by the Company are not intended to process Personal Data. The assumptions concerning the processing of Personal Data by the Company on behalf of the Customer are detailed below:

(A) as part of the Bug Bounty, VDP, Featured VDP, or Pentest Management Services, the Company hosts encrypted Vulnerability Reports (i.e., unreadable by the Company);
(B) as part of the Triage Service, the Company accesses the Vulnerability Reports and, consequently, any potential Personal Data contained thereof;
(C) as part of the Attack Surface Management Service the Company accesses, consult, copy, and store information of the Customer's Systems, some of which may constitutes Personal Data.

The Company acts as a Data Processor of the Customer, having the capacity of Data Controller, under its instructions as defined below and by GDPR and Law No 78-17 of 6 January 1978 as amended. 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 GDPR, and these T&Cs.

1. Processing of Personal Data

The Customer acknowledges it is its entire responsibility to determine the Systems to be tested. Consequently, access to Personal Data made available on the Customer's Systems in the context of the Tests and the Services is at the sole discretion of the Customer. Accordingly, the Customer shall represent and indemnify the Company that such Personal Data may be processed for the purpose of the Tests and the Services in accordance with GDPR.

Moreover, it is the Customer's responsibility to inform the data subjects of the processing that may be carried out by the Company, and the Security Researchers.

2. 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 authorized to process the Personal Data are subject to a confidentiality obligation.
- Raise awareness among and train such staff on the protection of personal data.
- Provide reasonable assistance required by 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.

To the extent the Customer's instructions go beyond what could reasonably be required of a Data Processor under applicable data protection legislation, the Company shall be entitled to reasonable compensation for such surplus work (e.g., to provide extensive request volumes from Data Subjects or to provide extensive detailed information under Article 7 (Rights of Data Subjects) or Article 8 (Notification of Personal Data Breaches) of the GDPR.

3. Sub-Processor(s)

The Company undertakes to:

- recruit exclusively Sub-Processors who provide sufficient guarantees as to the implementation of physical, technical and organizational 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 Sub-Processors all the requirements of this Appendix.

The Company's Sub-Processors existing at the time of acceptance of these T&Cs are deemed to have been authorized by the Customer under a general authorization.

Upon acceptance of the T&Cs, the Sub-Processors authorized by the Customer are those identified in Article 11 of this Appendix.

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

- inform the Customer as soon as possible. If the Customer raises objections, and if the Sub-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 Sub-Processors up to date;
- subject the Sub-Processor to the same obligations regarding the protection of Personal Data as outlined in this Appendix.
- ensure that the Sub-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 Sub-Processor (s) and any subsequent amendments thereto;
- prohibit its Sub-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 Sub-Processors. The Company shall inform the Customer of any breach by the Sub-Processor of its contractual obligations.

For the avoidance of doubt, the Security Researchers shall in no circumstances be considered as the Company's Sub-Processors.

4. Transfer of Personal Data to third countries

The Company undertakes not to transfer Personal Data to third countries or an international organization 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 organization by the Company shall be performed solely based on documented instructions from the Customer.

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

If the Company is required to transfer Personal Data to a third country or an international organization, 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.

5. Security of processing

The Company is ISO 27001 and ISO 27017certified and, to this extent, undertakes to take all appropriate technical and organizational measures to ensure the security, integrity, availability and confidentiality of the Personal Data it processes, including the use of pseudonymization and encryption of Personal Data where necessary. Such measures shall at least result in a level of security that takes into consideration (i) existing technical means; (ii) the costs for carrying out these measures; (iii) the particular risks associated with the processing of Personal Data; and (iv) the sensitivity of the Personal Data that are processed. The implemented security measures are available in the ISSP and the Platform Information Security.

When the Company is authorized to access to Personal Data subject to these T&Cs, such Processing operations shall be granted to the members of its personnel only to the extent strictly necessary for the performance, management and monitoring of the agreement between the Company and the Customer. The Company shall ensure that such personnel is bound by a confidentiality obligation of confidentiality.

The Company shall communicate to the Customer, at the latter's request, any useful documentation relating to the security of Personal Data (ISSP, SAP, etc.).

6. Sensitive data

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

7. 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 respond to these requests unless the Customer has expressly authorized 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, considering the nature of the Processing.

8. 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 seventy-two (72) 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.

9. Processor's Register/Data Protection Officer

By 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.

The Company has appointed an external Data Protection Officer who can be reached at: privacy@yeswehack.com.

10. 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, and may not unreasonably interfere with the Company's business activities. When deciding on an audit, the Customer may consider the relevant certifications held by the Company. The Customer shall provide the Company with a copy of the audit report.

11. Customer's data processing instructions

Hosting of Vulnerability Reports

Categories of data subjects	Depending on the scope of the Program or the scope of the penetration tests defined by the Customer
Categories of Personal Data	Depending on the scope of the Program or the scope of the penetration tests defined by the Customer
Purpose of the processing	Hosting of Vulnerability Reports
Nature of the processing performed by the Company	Storage of Personal Data contained in Vulnerability Reports
Categories of recipients	Sub-Processor: • **OVH S.A.S.**, 2, rue Kellermann, 59100 Roubaix, France: sub-processor is engaged for hosting the Platform (private cloud/dedicated server) in France and for encrypted back-up of dedicated server in Germany–; • **Scaleway S.A.S.**, 8, rue de la ville l'évêque, 75008 Paris, France: sub-processor is engaged for encrypted back-up of dedicated server in France
Retention period	By Article 8 of the French Code of Criminal Procedure, the Vulnerability Reports (including attachments and comments) are retained* for evidentiary purposes for six (6) years following the last interaction (comment on a report, status change, etc.…). Then, the Vulnerability Reports are deleted at Customer's request. * The Vulnerability Reports are encrypted during their storage.

Management of Vulnerability Reports

Categories of data subjects	Depending on the scope of the Program or the scope of the penetration tests defined by the Customer
Categories of Personal Data	Depending on the scope of the Program or the scope of the penetration tests defined by the Customer
Purpose of the processing	Management of Vulnerability Reports
Nature of the processing carried out by the Company	Access to and consultation of Personal Data contained in Vulnerability Reports
Categories of recipients	Sub-Processor: The Customer acknowledges and agrees that the Company may engage its Affiliates as Sub-Processors globally as necessary to deliver the Triage Service in accordance with these T&Cs. The Company warrants that any data transfers involved in such subprocessing will be carried out in full compliance with GDPR and any other applicable data protection laws.

	•
Retention period	Until access of the Company's triage team to Customer's Programs is revoked. The Customer is responsible for inviting and revoking access to its Programs.

Mapping and monitoring of the Customer's Systems

Categories of data subjects	Depending on the list of the Systems defined by the Customer
Categories of Personal Data	Depending on the list of the Systems defined by the Customer
Purpose of the processing	Analyze and assess the external perimeter declared by the Customer
Nature of the processing carried out by the Company	Access, consultation, copying, and storage of Personal Data contained in the Systems
Categories of recipients	Sub-Processor: • **OVH S.A.S.**, 2, rue Kellermann, 59100 Roubaix, France: sub-processor is engaged for hosting the Platform (private cloud/dedicated server) in France and for encrypted back-up of dedicated server in Germany–; • **Scaleway S.A.S.**, 8, rue de la ville l'évêque, 75008 Paris, France: sub-processor is engaged for encrypted back-up of dedicated server in France • **Sekost S.A.S.**, 4, rue Andrée Marie Ampère, 22300 Lannion, France: sub-processor is used to enrich the Company's ASM Service.
Retention period	For the duration needed to perform the ASM Service