Continuous Penetration Testing Contract Terms
(CPT Terms)
Version 1.0 dated 7 October 2025

These CPT Contract Terms ("**CPT Terms**") apply to the following service provided by Yes We Hack (the "**Company**") on its proprietary online platform, accessible at https://yeswehack.com/auth/login (the "**Platform**"):

- **CPT Service or Service** which consists of the following:
  (i) access to the Platform's Attack Surface Management (ASM) feature enabling:
    (a) automated identification of potential CVEs (Common Vulnerabilities and Exposures), and
    (b) where activated, automated detection of actual security vulnerabilities (the "**Detected Issues**"),
  (ii) setup and management of pentest campaigns, involving Crowdsourced Pentesters,
  (iii) validation of Detected Issues and Vulnerability Reports submitted by Crowdsourced Pentesters, , and
  (iv) delivery of the Pentest Reports within the Pentest Management (PTM) feature of the Platform.

More details about each feature can be found below:

- ASM: https://www.yeswehack.com/product/attack-surface-management
- PTM: https://www.yeswehack.com/product/pentest-management

Access to the Platform and Service is granted to the entity subscribing to the Service (the "**Customer**") subject to the prior and unconditional acceptance of these CPT Terms and the ordering document signed by the Company and the Customer (the "**Purchase Order**" or "**PO**").

Any Customer's terms and conditions, including but not limited to terms of purchase or terms of use are hereby expressly rejected, even if the Company did not reject their validity once the PO has been concluded.

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

1. SERVICES

The Platform. As part of the Service, the Customer is granted access to the ASM and PTM features of the Platform and shall communicate to the Company all Users requiring access. The Customer remains solely and fully responsible and liable for all acts and omissions of its Users as if such acts and omissions were the Customer's own.

Access and Use of the Platform and the Service. The Company undertakes to procure all reasonable efforts to ensure the availability and accessibility of the Platform and Service. 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 Service 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 Service, (ii) a request from a competent administrative or judicial authority, (iii) unlawful or fraudulent use of the Service, 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 CPT Terms. 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 AND TESTS PERFORMANCE

Onboarding. The Customer shall cooperate in good faith and provide the Company with a written detailed list of the technical and organizational information required to define the scope of the Service, including the designation of the Systems to be tested using the ASM feature and/or the Pentest Programs, the type(s) of Tests, any exclusions, and other relevant parameters, requirements and/or instructions.

Pentest Program(s) management. Based on the information and instructions provided by the Customer during the Onboarding, the Company shall draft, manage, and administer the Pentest Program(s). Any substantial modification to the Pentest Program(s) will be discussed between the parties.

Backups during Tests. The Customer expressly acknowledges and agrees that the Tests will be performed by Pentesters during the applicable Pentest Program, without prior notice or real-time coordination. The Customer further acknowledges that it has been duly informed by the Company of the critical importance of preparing for the Tests and implementing all necessary technical and organizational safeguards in advance, including maintaining backups of its Systems.

3. PAYMENT

Fees. Fees consist of a non-refundable lump-sum and flat-rate as detailed in the PO (the "**Fees**").

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 are payable as stated in the PO. Shall the Customer be in arrears with payments, the Company may charge late payment penalties in accordance with the relevant applicable law.

4. TERM - TERMINATION

Term. These CPT Terms are effective as of the date of mutual acceptance of a PO or as otherwise specified therein. They are entered into for an initial period indicated in the initial PO.

Termination for cause. The Company may immediately revoke access to the Platform and use of the Service, 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 Service 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 Service for any reason whatsoever, all information relating to the use of the Service, 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. For the purposes of this article, 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.

The Company hereby grants to Customer a worldwide, non-exclusive, non-transferable, and non-sublicensable right to use the Platform, solely in connection with the use of the Platform, for the duration of the PO and exclusively for providing the Service within the limits of these CPT Terms.

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 CPT Terms, 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.

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 CPT Terms. The Customer grants the Company and the Pentesters the right to use said Systems for the entire duration of the Service 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 Service and carrying out the Tests, subject to the rules and restrictions of the Program.

Ownership of Vulnerability Reports. The Company shall ensure that the Pentesters allow for the transfer of ownership of the Vulnerability Reports from the Pentester to the Customer. For the limited purpose of performing the Service under these CPT Terms, the Customer hereby grants the Company a non-exclusive, worldwide, royalty-free right to access, use, copy, and reproduce the Vulnerability Reports strictly to the extent necessary for the Company to fulfill its obligations hereunder.

Indemnification. The Customer warrants that it owns all IPRs necessary to enable it to perform its obligations under these CPT Terms. 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 Service 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 CPT Terms 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 Service, 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 Service, and
iii. not to use the Confidential Information directly or indirectly, for any purpose other than the performance of the Service.

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 Confidential Information was lawfully known prior to the PO;
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 CPT Terms 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.

8. OBLIGATIONS

The Customer's obligations. The Customer shall:

i. undertake to use the Platform and Service in accordance with these CPT Terms;
ii. be solely responsible for its Users, including the management of User accounts and the means of authentication (such as identifiers, passwords, etc.) associated therewith;
iii. designate a primary point of contact for operational coordination, and establish a clear escalation path for use in the event of emergencies, incidents, or critical issues related to the performance of the Service;
iv. promptly notify the Company of any circumstances that may affect the performance of the Service, including, without limitation, any changes to the Customer's rights or authorizations over the Systems to be tested. The Customer shall regularly review and ensure the validity of such rights and authorizations throughout the term of the CPT Terms;
v. assign to the Company, in the context of Vulnerability reproduction, identifiers dedicated to the reproducibility of Vulnerability Reports if the creation of an account is impossible or the use of personal information is mandatory (e.g., national identity card, passport, driver's license, social security number, etc.). Failing this, the Company shall only be required to perform a theoretical assessment of the Vulnerability Reports;
vi. ensure that the use of the Service complies with its internal, legal and any regulatory requirements.

Subject to the Crowdsourced Pentester's compliance with the rules set by the Pentest Program and the Pentesters Terms, the Customer acknowledges that:

i. any Test conducted by the Pentesters as part of a Pentest Program is authorized and operated with the Customer's express consent and under its sole responsibility;
ii. the acts carried out by the Pentesters 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 Pentester for acts performed in the context of a Pentest Program under criminal or civil law, being specified that the Company cannot be held liable for any breach by the Pentester 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 Pentest Program.

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

i. provide the Customer with the necessary resources (documentation, demonstration, advice and assistance) enabling the Customer to become aware of and understand the characteristics and use of the Service;
ii. exercise all due care and diligence in providing the Service in accordance with these CPT Terms, including having a primary point of contact to ensure operational cooperation with the Customer
iii. draft and manage the Pentest Programs in accordance with the Customer's instructions and restrictions provided during the Onboarding, and to promptly notify the Customer of any difficulties it may encounter in providing the Service.

The Company shall under no circumstance be liable for:

i. Any error, omission, or failure by the Customer to provide complete, accurate, or timely information necessary for the definition and management of the Program;
ii. use or misuse of the Platform or Service nor for any malfunction of the Platform resulting from Customer, User, or a third party's (including Pentester's) actions or omissions;
iii. non-compliance with the Pentesters Terms, violation of the rules of the Program or any other agreement by the Crowdsourced Pentesters;
iv. 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;
v. suspension of access to the Platform and/or the Service under the conditions set out herein; and
vi. incidents due to the use of the Internet (e.g. loss of connectivity…).

As part of the Service, the Company will invite Crowdsourced Pentesters to participate in the Pentest Programs, at its discretion but subject to the Customer's requirements and restrictions communicated during the Onboarding.

Pentesters shall at all-time be considered as the sole editor of the Vulnerability Reports which cannot be edited/tampered with by the Company. Pentesters are the sole responsible for their content, including but not limited to (i) any error or omission, or (ii) any loss or damage of any kind resulting from the use of Vulnerability Reports.

Notwithstanding the foregoing, the Company accesses the information contained in the Detected Issues and Vulnerability Reports to perform a series of actions, including validating their content, communicating with the Pentesters and, if applicable, carrying out actions on the Systems in the context of Vulnerability reproduction.

The results of the aforementioned actions will be documented in a Pentest Report, which will include identified vulnerabilities, their severity, potential impacts, and, where practicable, the mitigation or remediation measures based on current state-of-the-art knowledge. The Pentest Report does not guarantee the complete elimination of Vulnerabilities or immunity from future security incidents.

In consideration of the foregoing, the Company shall therefore not be liable for any damage caused by the Customer or a Crowdsourced Pentester'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 Service or any act or omission arising out of or in relation to the Service, 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 CPT Terms, 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 Service will not in any case exceed twice 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 CPT Terms arising from 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 PO 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 (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 Service for more than thirty (30) calendar days, the Company may terminate as of right the Service 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 Service 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 PO 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 CPT Terms 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 CPT Terms 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 CPT Terms which, by their nature or by virtue of specific provisions, extend beyond the end or expiry of these CPT Terms.

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. For the purposes of this article, an Affiliate means 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.

Governing Law and Jurisdiction. These CPT Terms are governed by the laws of the country where the Company's contracting entity is registered, as specified in the relevant PO. 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 CPT Terms 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 PO, and the parties hereby irrevocably submit to the exclusive jurisdiction of those courts for these purposes.

***

APPENDIX 1: DEFINITIONS

***Crowdsourced Pentester(s) or Pentester(s)**: means an independent IT security researcher acting in a professional capacity and registered on the Platform. Pentesters are subject to the prior and unconditional acceptance of the Crowdsourced Pentesters Terms and conduct Tests and submit Vulnerability Reports under the relevant Pentest Program. For the avoidance of doubt, Pentesters are neither employees nor subcontractors of the Company.*

***Pentest Program(s) or Program(s):** means the testing initiatives aiming at Vulnerability disclosure instructed by the Customer and managed by the Company, subject to the documented scope and criteria mutually defined with the Customer. The Program notably enables selected Pentesters to identify and report Vulnerabilities on designated Systems through the Platform during defined pentest campaigns, in accordance with the Customer's instructions and as conveyed by the Company. When there is a difference between a Pentest*

Program and the Pentesters Terms, the Pentest Program shall prevail.

Pentest Report(s): *means the report made available to the Customer via the Pentest Management feature of the Platform, based on the Detected Issues and the Vulnerability Reports reviewed by the Company. It includes identified Vulnerabilities, severity ratings, potential impact assessments, and, where practicable, the mitigation or remediation measures based on current state-of-the-art knowledge.*

Systems: *means the Customer's designated IT systems and internet-exposed assets (e.g., servers, websites, applications, software, modules, interfaces, connected objects, etc.) on which the Tests are performed by the Pentesters.*

Tests: *means the actions conducted by Pentesters, on a crowdsourced basis, to reach or enter the System as authorized under a Pentest Program. These Tests are technical in nature and aim at analyzing the level of security in place and search for Vulnerabilities.*

User(s)*: means the Customer employee (including those of any of its Affiliates) or any third-party, appointed by and representing the Customer who uses the Pentest Management feature of the Platform on behalf of the Customer. Any action or omission of the User shall be deemed an action or omission of the Customer.*

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(s)*: means the document(s) drafted and issued by Pentesters in connection with a Pentest Program, containing technical data in a standardized format, along with any relevant attachments of a functional nature, describing the identified vulnerabilities and, if applicable, the remediation recommendations.*

***

APPENDIX 2: PROTECTION OF PERSONAL DATA

The Service 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)*** *the Company hosts encrypted Vulnerability Reports (i.e., unreadable by the Company) – **Purpose #1**;*
- ***(B)*** *the Company accesses, consults, copies, and stores information of the Customer's Systems as well as the Detected Issues and the Vulnerability Reports and, consequently, any potential Personal Data contained thereof – **Purpose #2**.*

*The Company acts as a Data Processor of the Customer, having the capacity of Data Controller, under its instructions as defined below and by General Data Protection Regulation (the **"GDPR"**). 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.*

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 Service 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 Service 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 Pentesters.

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 CPT Terms are deemed to have been authorized by the Customer under a general authorization.

Upon acceptance of the CPT Terms, 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 Service covered by the CPT Terms, 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 CPT Terms 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 Pentesters 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 CPT Terms, 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 the information required by Article 33 of the GDPR.

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

Purposes and nature of the processing:

- ***Purpose #1:*** *Hosting of Detected Issues and Vulnerability Reports (Storage of Personal Data contained in Vulnerability Reports)*
- ***Purpose #2:*** *Automated mapping and monitoring of the Customer's Systems, the identification of security vulnerabilities within such Systems, and the management of Detected Issues and Vulnerability Reports (Access to and consultation of any potential Personal Data contained therein)*

Categories of data subjects: *Depending on the scope of the Program or the list of the Systems as instructed by the Customer*

Categories of Personal Data: *Depending on the scope of the Program or the list of the Systems as instructed by the Customer*

Categories of recipients :

- ***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* ***(Purpose #1)****;*
- ***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* ***(Purpose #1)****;*
- ***Sekost S.A.S.****, Maison des Entreprises, Espace Corinne Erhel 4 Rue Louis de Broglie, 22300 Lannion, France: sub-processor is used to enrich the Company's ASM feature* ***(Purpose #2)****;*
- *The Customer acknowledges and agrees that the Company may engage its subsidiaries as Sub-Processors globally as necessary to deliver validation of Detected Issues and Vulnerability Reports submitted by Pentesters* ***(Purpose #2)*** *in accordance with these CPT Terms. 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: *Detected Issues and 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.…) in accordance with Art. 8 of the French Code of Criminal Procedure. Then, the Detected Issues and Vulnerability Reports are deleted at Customer's request* ***(Purpose #1)****. *The Vulnerability Reports are encrypted during their storage.*

Automated access by the Company to the Customer's Systems is required for the duration of the continuous identifications, as instructed by the Customer through the ASM feature ***(Purpose #2)****.*

Access of the Company's personnel to the Detected Issues and Vulnerability Reports is required for the duration of the Service (i.e., upon termination or expiration of the PO) ***(Purpose #2)****.*