

Specifications of Services

Complorer Security Awareness

eBuilder Security Awareness Training is offered through the eBuilder Complorer platform. The Security Awareness Training is provided online through Nano-trainings. A package of basic Security Awareness video-based lessons targeting all employees of the organization with the following features is provided:

- Nano Learnings Short and simple lessons through videos in
 - English
 - Swedish
 - Content can be customized based on customer agreement
- Self-Learning
- Anytime and anywhere - smart mobile, tablet or computer device compatibility
- Engaging – Easy to understand and fun to learn
- Repeatable – Reinforce training as often as you need/want/require
- Measurable – Participation and awareness progress is measurable.
- Role-based Training – Training can be customized to each person's job role

The Security Awareness Training is coupled with up to 6 annual friendly phishing attempts to see if/where you need more training. It will allow you to tailor your training efforts to your specific organization and will allow you to follow up and improve your results over time.

The product is offered as a service "fully managed" i.e., the goal is to minimize the engagement of the customer. eBuilder will manage all:

- user management
- end user notifications such as training assignment, deadline reminders etc...
- followup
- reporting
- phishing and associated refresher training

The product is priced per employee trained during a 12-month period (per employee user license for a 12-month period).

Complorer Data Privacy Training

eBuilder Data Privacy Training is offered through the eBuilder Complorer platform. The Data Privacy Training is provided online through Nano-trainings. A package of basic Data Privacy video-based lessons targeting specific employees of the organization with the following features is provided:

- Nano Learnings Short and simple lessons through videos
- Self-Learning
- Anytime and anywhere - smart mobile, tablet or computer device compatibility
- Engaging – easy to understand and fun to learn
- Repeatable – reinforce training as often as you need/want/require
- Measurable – Participation and awareness progress is measurable.
- Role-based Training – Training can be customized to each person's job role

General Terms and Conditions

These General Terms and Conditions are an inseparable part of this Contract. By accepting the Contract you also agree to the full General Terms and Conditions. This Contract replaces any previous Contracts and their attachments.

1. Scope of Terms

These Terms apply to the provision of the products, information and services available through www.ebuildersecurity.com or otherwise provided by eBuilder Security ("Service" or "Services") to the firm, company, corporation, or other customer ("Customer") and to all Contract(s). The Customer may not be an individual person and the Services are intended for business use only. eBuilder Security and the Customer are also referred to each as a "Party" and together as the "Parties". These Terms form an integral part of the Contract. The Customer's purchase, procurement or other terms shall not apply to the Contract, even if referred in or attached to the Customer's purchase order or other document submitted by Customer. In the event of a conflict between the Terms and other terms of the Contract added by eBuilder Security, the terms elsewhere in the Contract added by eBuilder Security shall prevail. The Customer represents and warrants that each person who takes the Services in use or uses the Services, the Documentation or the Software or clicks the acceptance of the Contract/Terms or otherwise accepts the Contract/Terms (or the modified version thereof) is authorized to conclude a binding agreement on behalf of the Customer and that the Customer is bound by the Contract (including but not limited to the Terms). If the Customer does not accept the terms of the Contract (including but not limited to the Terms), the Customer is not entitled to use the Services, the Documentation or the Software.

2. Definitions

"Affiliates" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by, is under common control with, or controls that party, and here "control" means an ownership, voting, or similar interest representing fifty percent (50%) or more of the total interests then outstanding of that entity.

"Confidential Information" means any and all information of confidential nature supplied by a Party to the other Party, whether in writing, orally, electronically or otherwise, and whether marked as confidential or not.

"Contract" means this document consisting of Specifications of Services, General Terms and Conditions and the Data Processing Agreement.

"Contract Period" is defined in clause 7.

"Customer Data" means data, files, or information, including data, files, or information that include Personal Data, accessed, used, communicated, stored, or submitted by Customer or Customer's Users use of the eBuilder Security Service.

"Documentation" means the operating instructions, user manuals, product specifications, "read-me" files, and other documentation that eBuilder Security makes available to Customer in hard copy or electronic form, are stored by eBuilder Security's Help Desk for the purpose of use of eBuilder Security's customers or are accessible through the Service, but excluding marketing materials.

"eBuilder/eBuilder Security" means eBuilder Sweden AB, a limited liability company registered in Sweden (company registration number 556595-2933).

"GDPR" means EU's General Data Protection Regulation 2016/679.

"Intellectual Property Rights" means all intellectual property rights, including patents, inventions, trademarks, domain names, rights in know-how, trade secrets, copyrights, database rights, rights related to copyrights and any other intellectual and industrial property rights, whether registered or unregistered, and including without limitation the right to amend and further develop the objects of those rights and the right to assign the rights to third parties.

"Personal Data" shall mean any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Services" means security services delivered by eBuilder Security in the form of:

- Security Awareness Training with associated Phishing
- Data Privacy Training

“Service Fee” is defined in clause 6

“Statistical Information” means (i) information on the way the Customer use and access the Services, (ii) Customer Data in an aggregated form so that the Customer’s or the users’ identity cannot be identified directly from the Statistical Information.

“Subscription” means a subscription purchased by Customer to access and use the eBuilder Security Service during the applicable Subscription Term.

“Subscription Term” means the contract term for Customer’s access and use of the eBuilder Security Service as set forth on the applicable Order Form.

“Support” means the standard maintenance or support provided by eBuilder as defined in clause 4.

“Usage Parameters” means the maximum number of permitted web application scan targets using the eBuilder Security Solution as specified on an Order Form and any other parameters specified in the Documentation, Order Form, or other writing by eBuilder Security regarding the scope of use of the eBuilder Security Service by Customer or its Users.

“User(s)” means Customer’s employees, contractors, or agents who are authorized to use the eBuilder Security Services subject to applicable Usage Parameters and the terms of this Agreement and only for Customer’s internal business purposes.

3. Features of Services

The features of the Services provided to the Customer are described in the “Specifications of Services” section in this Contract.

4. Services and Support

Subject to the terms of the Contract, eBuilder Security will use commercially reasonable efforts to provide the Customer with the Services. As part of the registration process, Service Provider will identify an administrative username and (one-timepassword) for the Customer’s company account. eBuilder Security reserves the right to refuse registration and require change of passwords as it deems appropriate.

Subject to the Terms hereof, eBuilder Security will provide the Customer with reasonable technical support services via ITSM (email or login) on reasonable effort basis. As part of the technical support services, eBuilder Security will upgrade tools used for the service without any additional fee.

Noncommercial agreements come with no commitment for services or support. eBuilder Security’s responsibility for the Services and their functionality is limited to the functionalities of eBuilder Security’s own information systems. eBuilder Security cannot guarantee disruption-free access to the Services, or otherwise guarantee the availability or disruption-free use of the Services. eBuilder Security is not responsible for any restrictions on the use of the Service in any country.

5. Terms of Use

Subject to the Customer’s payment of the prices payable for the Services (“Service Fee”), the Customer is granted a nonexclusive, non-transferable and non-sublicensable right to use the licensed features of the Services during the term of the Contract in the Customer’s own operations in accordance with the Documentation.

The Customer may not use the Services to offer services to any third party, otherwise transfer the Services or allow access to the Services to any third party or allow any third party to benefit from the Services. The Customer shall follow the usage limitations set out in the Contract and the Documentation, regarding e.g., the functionalities of the Services provided to the Customer or other limitations. There are no implied licenses. The Customer may use the Documentation to use the Services, as long as the Customer’s right to use the Services is in force.

6. Pricing and Payments

Subscription Services Purchase: The customer fully commits to the subscription purchase upon accepting a quote and offer on AWS Marketplace. Even if subject to fiscal period or budget restrictions, the customer agrees to pay in full either from the current budget or with proper authority to commit future funds. All sales are final and non-refundable.

Subscription Services Pricing: All prices for Subscription Services, with applicable discounts, will be specified by eBuilder Security. Additional services, such as additional hourly work, will be agreed upon separately. Prices for offers made through the AWS Marketplace do not include any taxes, levies, duties, or similar governmental charges of any kind, including, without limitation, value-added, sales, use, or withholding taxes, imposed by any jurisdiction (collectively, 'Taxes'). Customer shall be responsible for all Taxes associated with their purchases.

Unless otherwise stated in this Agreement or an AWS Marketplace offer:

- (a) prices are based on the Subscription Services purchased, not actual usage;
- (b) all payment obligations are non-cancelable, and fees are non-refundable; and
- (c) Subscription Terms and quantities purchased cannot be reduced during the applicable term and agreed duration.

The Customer is also responsible for any unpaid amounts incurred by its Affiliates. Additionally, if the Customer requires eBuilder Security to use a vendor management or compliance portal that charges fees, the Customer will bear those costs.

Late Payments: Unless otherwise agreed by the Customer and the AWS Marketplace, the Customer shall pay each invoice in full, without deduction, within thirty (30) days of receipt. Any amount not received from the Customer by the due date (except with respect to charges under reasonable and good faith dispute) shall accrue interest from such date until paid, at a rate of one and one-half percent (1.5%) per month, or the maximum rate permitted by applicable law in the jurisdiction of the Customer's principal place of business, whichever is higher. The Customer shall be responsible for all reasonable costs of collection incurred by eBuilder Security, including reasonable attorneys' fees. If the Customer's account remains overdue for thirty (30) days or more (except with respect to charges under reasonable and good faith dispute), eBuilder Security may, upon prior written notice and without liability, suspend the Services until all outstanding amounts are paid in full, in addition to any other rights or remedies available to eBuilder Security.

Index adjustments: eBuilder Security may, for any Renewal Period, adjust the Fees without prior written notice in line with changes to the Consumer Price Index (or equivalent index) in the country of the Customer's principal place of business for the same period, plus two percent (2%). Alternatively, eBuilder Security may make other adjustments to the Fees by providing the Customer with written notice no later than four (4) months prior to the commencement of the applicable Renewal Period.

Refunds: eBuilder Security is not obligated to provide a refund for any reason, including but not limited to partial months or years of Services, upgrades or downgrades, unused time or if the Customer did not use the Services, used the Services only partially or deactivated the Services or if the Contract is terminated before the contracted earliest termination date. However, if the Contract is terminated due to eBuilder Security's material breach in accordance with clause 7 of these Terms, eBuilder Security will refund the proportion of the pre-paid Service Fee attributable to the period after the date of termination, as the Customer's sole and exclusive remedy.

eBuilder Security should authorize all subscription downgrade refund requests, and AWS shall be notified to process them.

7. Term and Termination

The Contract will remain in force for:

- twelve months (Initial Contract Period).

Either Party may terminate the Contract with immediate effect by giving the other Party a written notice if the other Party commits a material breach of the Contract and fails to remedy the same within thirty (30) days after receipt of a written demand from the other Party to cure the breach. The Customer shall notify eBuilder Security of eBuilder Security's breach of Contract without delay and latest within time that enables eBuilder Security to remedy the breach to so as to mitigate the adverse effects caused to the Customer by the breach.

eBuilder Security may terminate any Customer agreement that is free of charge, at its own discretion at any time.

8. Customer Data, Use of Services and Statistical Information

The Customer warrants that eBuilder Security and its subcontractors are entitled to store and otherwise process the Customer Data lawfully for the purposes of the Contract. The Customer shall also keep own records of output data (such as reports) as the originals will be deleted once the Contract is terminated.

The Customer may use the Services only in accordance with good business ethics. The Customer may not use Service for any illegal or questionable use.

It is the sole responsibility of the Customer to ensure that the service usage complies with local legislation. The Customer agrees to defend and indemnify eBuilder Security from and against any claim by a third party in connection with the Customer's failure to comply with laws or regulations. No limitations of liability shall apply to such liability of the Customer.

During and after the term of the Contract, eBuilder Security has a perpetual, non-revocable, transferable, sublicensable and free of charge right to use, operate, copy, modify, disclose and publish Statistical Information in any and all means and for any and all purposes. eBuilder Security undertakes not to identify the Customer as the source of the Statistical Information, unless consented to by the Customer. eBuilder Security reserves the right to delete all data for unpaid, unused accounts after 1 month of inactivity.

9. Intellectual Property Rights

Title and any and all Intellectual Property Rights in and to the Services, the Software, the software used by eBuilder Security to provide the Services and the Documentation, and any copies, modifications, translations, amendments and derivatives thereof, are and shall belong to eBuilder Security and/or its licensors.

10. Warranties and Disclaimers

Each party represents and warrants that it has the legal power to enter into the Agreement.

eBuilder Security represents and warrants that the Services do not and will not contain any virus or any other contaminant, or disabling devices including, but not limited to, codes, commands or instructions that may be used to access, alter, delete, remotely access, damage or disable Customer software, Customer Data, the Customer network or other Customer property.

Services, Consulting Services and Support provided by eBuilder shall be performed in a professional and workmanlike manner in accordance with generally accepted practice in the industry and that the Services will perform substantially in accordance with the online eBuilder Security service descriptions and help documentation under normal use and circumstances. Except as specified in this Section, all express or implied conditions, representations and warranties including without limitation any implied warranties or conditions, e.g., regarding merchantability, fitness for a particular purpose, and satisfactory quality are hereby excluded to the extent allowed by applicable laws.

eBuilder Security is not be responsible for defects of the Services that are caused by: (a) faulty use or third parties; (b) failure to follow these Terms or the usage instructions; (c) a modification or repair performed by anyone else than eBuilder Security; (d) any equipment, devices, connections, data transfer services, hardware, software or information security not provided by eBuilder Security, or for any changes in the same or for incompatibility issues with the same; (e) the Customer Data or the Customer's instructions.

11. Confidentiality

Each Party shall keep in confidence all Confidential Information received from the other Party and may not use such Confidential Information for any purposes other than those set forth in the Contract unless required by "**Offentlighets- och sekretesslagen (2009:400)**", the Swedish principle of public access to official records.

eBuilder Security may disclose the Customer's Confidential Information to its subcontractors for the purposes set forth in the Contract provided that the subcontractors are bound by a confidentiality obligation substantially similar as herein. However, Confidential Information does not include information: (a) which is generally available to the public or otherwise public information through no breach of this confidentiality obligation by the receiving Party; (b) which the receiving Party has received from a third party; (c) which was in the possession of the receiving Party prior to receipt of the same from the other Party; (d) which the receiving Party has independently developed without using the Confidential Information of the other Party; or (e) which has to be disclosed in accordance with a mandatory judicial or other governmental order or otherwise under law.

12. Reference Use

eBuilder Security may use the Customer's name and logo in eBuilder Security's marketing websites and promotional materials to identify the Customer as a Service customer of eBuilder Security.

13. Changes to Terms and Notifications

eBuilder reserves the right to modify the terms and conditions of these General Terms or its policies relating to the Services at any time, effective upon the next contract period. eBuilder Security will notify the Customer of any changes of the general terms and conditions.

If the Customer does not accept the amendments of the Terms which are materially unfavorable to the Customer, the Customer may terminate the Contract as the Customer's sole and exclusive remedy, to expire on the date the amended Terms become effective. The Customer shall notify eBuilder Security of the termination by email (support@complorer.com) latest fourteen (14) days before the date the amended Terms become effective. The Customer's continued use of the Services after the next contract period date constitutes the Customer's acceptance of the amended Terms.

The Customer shall notify eBuilder Security of any changes in the Customer's circumstances that may affect the provision of the Services, by email to (support@complorer.com). eBuilder Security may make effective notifications to the Customer by push notifications, to the Customer users' email addresses, phone numbers and other contact addresses, in the user interface of the Services and in other means. The Customer guarantees that each of its users is authorized to receive notifications and to accept changes of these Terms and other terms of the Contract on the Customer's behalf.

14. Mutual Indemnification

Customer shall indemnify and hold eBuilder, its licensors and each such party's parent organizations, subsidiaries, affiliates, officers, directors, employees, attorneys, and agents harmless from and against any and all claims, costs, damages, losses, liabilities, and expenses (including attorneys' fees and costs) arising out of or in connection with: (i) a claim alleging that use of the Customer Data infringes the rights of, or has caused harm to, a third party; (ii) a claim, which if true, would constitute a violation by Customer of Customer's representations and warranties; or (iii) a claim arising from the breach by Customer or Customer Users of this Agreement, provided in any such case that eBuilder (a) gives written notice of the claim promptly to Customer; (b) gives Customer sole control of the defense and settlement of the claim (provided that Customer may not settle or defend any claim unless Customer unconditionally releases eBuilder of all liability and such settlement does not affect eBuilder's business or Service); (c) provides to Customer all available information and assistance; and (d) has not compromised or settled such claim.

eBuilder shall indemnify and hold Customer and Customer's parent organizations, subsidiaries, affiliates, officers, directors, employees, attorneys, and agents harmless from and against any and all claims, costs, damages, loss-es, liabilities, and expenses (including attorneys' fees and costs) arising out of or in connection with: (i) a claim alleging that the Service directly infringes a copyright, a patent issued as of the Delivery Date, or a trademark of a third party; (ii) a claim, which if true, would constitute a violation by eBuilder of its representations or warranties; or (iii) a claim arising from breach of this Agreement by eBuilder; provided that Customer (a) promptly gives written notice of the claim to eBuilder; (b) gives eBuilder sole control of the defense and settlement of the claim (provided that eBuilder may not settle or defend any claim unless it unconditionally releases Customer of all liability); (c) provides to eBuilder all available information and assistance; and (d) has not compromised or settled such claim. eBuilder shall have no indemnification obligation, and Customer shall indemnify eBuilder pursuant to this Agreement, for claims arising from any infringement arising from the combination of the Service with any of Customer products, service, hardware or business process(s).

15. Limitation of Liability

EXCEPT FOR INDEMNIFICATION OBLIGATIONS TO THE MAXIMUM EXTENT PERMITTED BY LAW, UNLESS CAUSED BY INTENT OR GROSS NEGLIGENCE, EITHER PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THE AGREEMENT, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, SHALL BE LIMITED TO 50000 SEK.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, NEITHER PARTY SHALL UNLESS CAUSED BY INTENT OR GROSS NEGLIGENCE, HAVE ANY LIABILITY TO THE OTHER PARTY FOR ANY LOST PROFITS OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES HOWEVER CAUSED, WHETHER

IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SECTION 15 SHALL IN NO EVENT LIMIT THE AMOUNTS THAT MAY BE PAYABLE BY EITHER PARTY UNDER OR BY BREACH OF SECTION 5 (TERMS OF USE), SECTION 9 (INTELLECTUAL PROPERTY OWNERSHIP), SECTION 11 (CONFIDENTIALITY) AND SECTION 14 (MUTUAL INDEMNIFICATION). THE LIMITATIONS OF LIABILITY SHALL NOT APPLY TO DAMAGES CAUSED BY GROSS NEGLIGENCE OR INTENTIONAL ACT.

NO ACTION MAY BE BROUGHT BY THE CUSTOMER AGAINST EBUILDER SECURITY MORE THAN TWO (2) MONTHS AFTER THE CAUSE OF ACTION HAS ARISEN.

16. Personal Data and Privacy

The Customer hereby consents and authorizes eBuilder Security and other service providers listed in the enclosed Data Processing Agreement to process data including Personal Data provided by the Customer to eBuilder Security as contemplated by this Agreement.

When eBuilder Security is a Personal Data processor on behalf of the Customer in the meaning of the GDPR, the terms of the enclosed Data Processing Agreement will apply.

17. Applicable Law and Settlement of Disputes

The Contract shall be construed in accordance with the laws of Sweden, excluding its choice of law provisions and the UN Convention on Contracts for the International Sale of Goods. Any dispute, controversy or claim arising out of or relating to the Contract shall be settled primarily through negotiation. If the Parties cannot find a satisfactory solution through negotiation within sixty (60) days from the start of the negotiation, the dispute, controversy, or claim shall be settled by Swedish Public Courts. The court of first instance shall be the City Court of Stockholm. The language to be used in the proceedings shall be Swedish.

18. Miscellaneous

18.1 Assignment and Subcontractors

Either Party may not assign the Contract to a third party, without the prior written consent of the other Party. However, eBuilder Security may assign the Contract without the consent of the Customer to a transferee, when assigning the ownership of eBuilder Security's business assets or part thereof, or to a eBuilder Security's affiliated company, and, for the avoidance of doubt, in merger or demerger. eBuilder Security may subcontract its duties. eBuilder Security shall be liable for the work of its subcontractors as for work of its own.

18.2 Survival

Upon termination of the Contract, the provisions relating to title and Intellectual Property Rights, confidentiality, limitations of liability, warranty disclaimers and this clause "Miscellaneous" shall survive. Also, any other provisions which by their nature or wording contemplate effectiveness beyond the termination of the Contract, shall survive the termination.

18.3 Entire Contract

The Contract (including but not limited to the Terms) constitutes the complete agreement between the Parties with respect to the subject matter hereof and supersedes all previous proposals, marketing materials and other communications between the Parties with respect to the subject matter hereof.

18.4 Severability

If any provision of the Contract is found to be contrary to law, the other provisions of the Contract will remain in force. The invalid provision shall be amended by the Parties, and the Contract shall be interpreted, so as to best accomplish the objectives of the original provision to the fullest extent allowed by law.

18.5 Amendment

No change of the Contract shall be binding unless made in writing and signed by duly authorized representatives of each Party.

18.6 Force Majeure

eBuilder Security shall not be liable for delays, defects or damages caused by factors due to an impediment beyond eBuilder Security's reasonable control, which eBuilder Security cannot reasonably be deemed to have taken into

account at the time of the conclusion of the Contract, and the consequences of which eBuilder Security could not reasonably have avoided or overcome. Such events of force majeure shall include, without being limited to, natural disasters, breakdown of electricity or networks, security attacks, failures in Internet or other public networks or data traffic, strikes and other labor disputes or acts of government. A labor dispute shall be considered a force majeure event also when eBuilder Security is the target or a party to such an action. The force majeure events suffered by eBuilder Security's subcontractors are also deemed as force majeure events.

Data Processing Agreement

This Data Processing Agreement is an inseparable part of this Contract. By accepting the Contract you also agree to the full Data Processing Agreement.

1. Contract and purpose of this DPA

This DPA has been entered into in connection with the Contract concerning the provision of eBuilder Security's services entered into between the Parties. This DPA sets additional requirements and details regarding the Service Provider's handling of personal information relating to the Customer's employees, contractors, partners or other parties ("Personal Data") on behalf of the Customer in accordance with and as required by the Contract. Subject-matter, nature and purpose of the Processing are defined and agreed under the Contract.

The DPA shall form an integral part of the Contract, meaning that applicable parts of the Contract (including its provisions on governing law and dispute resolution) shall apply also to this DPA. However, in the event of a conflict, the provisions of this DPA shall prevail over the provisions of the Contract.

2. Duration of the process

Personal Data will be processed by the Service Provider for the duration of the Contract unless a longer or shorter period is agreed between the Parties in the Contract or elsewhere in writing. Personal Data of the Customer may be stored up to two months after the termination of the Contract.

3. Types of personal data processed

During the duration of the Contract, Service Provider will store Personal Data. This type of data may include, for example, person's name, required contact information, and as well as other necessary additional information needed for registration, using the service, and payment.

4. Definitions

The capitalized terms used herein shall have the meaning ascribed to them below or in the text of this DPA.

"Affiliate" shall mean any legal entity which is directly or indirectly owned or controlled by a Party or directly or indirectly owning or controlling a Party or under the same direct or indirect ownership or control as a Party for so long as such ownership or control lasts.

"Data Protection Laws" shall mean EU Data Protection Regulation (2016/679) and the data protection laws under the governing law of the Contract applicable to the Processing hereunder from time to time.

"Personal Data" shall mean any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Personal Data Breach" shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed hereunder.

"Processing" shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, of Personal Data.

"Sub-Processor" shall mean a processor contracted by the Data Processor to perform Processing hereunder, in part or in whole, on the Data Processor's behalf.

5. Rights and obligations of the parties

Both Parties shall be responsible to ensure that the Processing is made in accordance with the Data Protection Laws which apply to each Party as well as good data processing practices.

6. The Data Controller shall

1. Give the Data Processor documented and comprehensive instructions on the Processing, which instructions shall comply with the Data Protection Laws;
2. Have the right and obligation to specify the purpose and means of Processing of Personal Data;
3. Represent that all the data subjects of the Personal Data have been provided with all appropriate notices and information and establish and maintain for the relevant term the necessary legal grounds for transferring the Personal Data to the Data Processor and allowing the Data Processor to perform the Processing contemplated hereunder;
4. Represent that if the Data Controller represents its Affiliates or third parties under this DPA, it has the legal grounds to enter into this DPA with the Data Processor and allow the Data Processor to process the Personal Data according to the terms of this DPA and the Contract; and
5. Confirm that the Processing stipulated under this DPA meets the Data Controller's requirements including, but not limited to, with regard to intended security measures, and it has provided the Data Processor with all necessary information in order for the Data Processor to perform the Processing in compliance with the Data Protection Laws.

7. The Data Processor shall

1. Perform the Processing only on and as per the documented, legitimate and reasonable instructions from the Data Controller unless required to do otherwise by Data Protection Laws, in which latter case the Data Processor shall inform the Data Controller of such deviating legal requirement (provided the Data Protection Laws do not prohibit such notification). For the avoidance of doubt, the Data Controller shall at all times be deemed to have instructed the Data Processor to provide the Service as defined and agreed under the Contract;
2. Ensure that persons authorized to perform the Processing hereunder have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality as further stated under this DPA;
3. Take all security measures required to be taken by data processors under the Data Protection Laws as further stated under this DPA;
4. Respect the conditions referred to under Data Protection Laws for engaging any Sub-Processor as further stated under this DPA;
5. Insofar as this is possible and taking into account the nature of the Processing, assist the Data Controller by appropriate technical and organizational measures for the fulfillment of the Data Controller's obligation to respond to requests for exercising the data subject's rights laid down in under the Data Protection Laws;
6. Assist the Data Controller in ensuring compliance with its legal obligations, such as data security, data breach notification, data protection assessment and prior consulting obligations, as required of the Data Processor by the Data Protection Laws, taking into account the nature of Processing and the information available to the Data Processor;
7. Maintain necessary records and make available to the Data Controller all information necessary to demonstrate compliance with the obligations of the Data Processor, as laid down in the Data Protection Laws, and allow for and contribute to audits, including inspections, conducted by the Data Controller or any auditor mandated by the Data Controller as further agreed under this DPA; and
8. At the Data Controller's instructions, delete or return to the Data Controller all the Personal Data after the end of the provision of the Services relating to Processing, and delete existing copies unless applicable laws require storage of the Personal Data. Deletion and return methods may be further agreed between the Parties;

Unless otherwise agreed, the Data Processor shall have the right to invoice any costs resulting from the above assistance under 5) and 6) above in accordance with the Data Processor's prevailing price list.

8. Security processing

Both Parties shall implement and maintain appropriate technical and organizational measures to protect the Personal Data, taking into account:

1. the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and
2. the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Personal Data transmitted, stored or otherwise processed.

Such measures include, inter alia as appropriate:

1. the pseudonymization and encryption of the Personal Data; and
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and
3. the ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident; and
4. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

The Data Controller shall inform Data Processor of all issues (including but not limited to risk assessment and the inclusion of special categories of Personal Data) related to the Personal Data provided by the Data Controller which affect the technical and organizational measures that should be employed under this DPA.

9. Sub-processors

The Data Processor may from time to time use Sub-Processors to process the Personal Data hereunder.

Sub-Processor(s) used in the provision of Services are listed as a part of the agreement. Sub-Processors agreed and used under the existing Services and Contract shall be considered approved Sub-Processors by the Customer.

Such use will be under written contract and the Data Processor will require the Sub-Processor to comply with the data protection obligations applicable to the Data Processor under this DPA or obligations which provide for the same level of data protection.

The Data Controller agrees that the Data Processor has a general consent to use the Data Processor's Affiliates as Sub-Processors when Processing Personal Data.

The Data Processor will inform the Data Controller in advance on any intended changes concerning the addition or replacement of Sub-Processors. Approved Sub-processors at the time of the agreement are:

Name of Sub-Processor	Categories of processing	Third countries data is transferred to	Description and additional safeguards	Agreement
AWS	Storage and processing of customer data	AWS Region in Stockholm	Hosting partner for Security Awareness Training	DPA
eBuilder Technology Center Pvt Ltd	Storage and processing of all customer data	Colombo, Sri Lanka	eBuilder AB wholly owned subsidiary since its incorporation over 20 years ago. Software Development, Technical Support, Security Services.	EU Standard Clauses Agreement.

10. Transfer of personal data

The Data Processor will only transfer Personal Data out of the territory of the member states of the European Union, the European Economic Area, or other countries with the Data Controller's prior written consent or that the Customer has explicitly approved.

If required by applicable legislation, the Data Processor shall enter into relevant contractual arrangements with required parties (including with the Data Controller itself or any of the Data Controller's Affiliates) for the lawful transfer of Personal Data from the Approved Jurisdiction to third countries.

Such contractual arrangements shall be carried out in accordance with the standard data protection clauses adopted or approved by the European Commission ("Standard Contractual Clauses"). As an alternative to entering into the Standard Contractual Clauses, the Data Processor may rely upon an alternative transfer safeguard permitting and providing for the lawful transfer of Personal Data outside of the Approved Jurisdictions, provided that such safeguard is in compliance with applicable legislation.

In case of conflict between the Standard Contractual Clauses or any other alternative transfer safeguard permitting the lawful transfer of Personal Data outside the Approved Jurisdictions and the DPA, the Standard Contractual Clauses or such alternative framework shall always take precedence over the Contract and this DPA.

11. Notification of personal data breach

The Data Processor shall without undue delay (24h) notify the Data Controller if it, or one of its Sub-Processors, becomes aware of a Personal Data Breach. Information shall be provided to the contact person named by the Data Controller, if not otherwise agreed between the Parties.

The Data Processor shall without undue delay inform the Data Controller of the circumstances giving rise to the Personal Data Breach, and any other related information reasonably requested by the Data Controller and available to the Data Processor.

Additionally, to the extent it is available, the Data Processor shall provide to the Data Controller the following information:

1. a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
2. a description of the likely consequences of the personal data breach; and
3. a description of the measures taken or proposed to be taken by the Data Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

12. Auditing

The Data Controller and its customers whose data may be processed hereunder shall be entitled to audit the Data Processor's performance of its Processing obligations under this DPA ("Audit").

The Data Controller shall use external auditors who are not competitors of the Data Processor, to conduct such an Audit. The Parties shall agree well in advance on the time and other details relating to the conduct of such Audits.

The Audit shall be conducted in such a manner that the Data Processor's undertakings towards third parties (including but not limited to the Data Processor's customers, partners and vendors) are in no way jeopardized. All the Data Controller's representatives or external auditors participating in the Audit shall execute customary confidentiality undertakings towards the Data Processor.

The Data Processor shall always allow any relevant regulatory authority supervising the Data Controller's business to conduct Audits of the Data Processor's operations, in which case relevant parts of the Parties' agreement hereunder shall apply.

The Data Controller shall bear all Audit expenses and compensate the Data Processor for any and all costs incurred as a result of the Audit.

13. Confidentiality

The Data Processor shall:

1. keep any Personal Data received from the Data Controller confidential; and
2. ensure that persons authorized to process the Personal Data have committed themselves to confidentiality; and
3. ensure that Personal Data is not disclosed to third parties without the Data Controller's prior written consent, unless the Data Processor is obliged by mandatory law or decree to disclose such information.

In case data subjects or governmental authorities make a request concerning Personal Data, the Data Processor shall, as soon as reasonably possible, inform the Data Controller about such requests before providing any response or taking other action concerning the Personal Data.

In case any applicable authority prescribes an immediate response to a disclosure request, the Data Processor shall inform the Data Controller as soon as reasonably possible, unless the Service Provider is prohibited by mandatory law or authority order to disclose such information.

14. Limitation of liability

The limitations of liability set out under the Contract shall apply also to this DPA.

The Parties agree that the general principle of division of responsibilities between the Parties relating to administrative fines imposed by any relevant supervisory authority or claims by data subjects under this DPA is based on the principle that the respective Party needs to fulfill its own obligations under the Data Protection Laws. Hence, any administrative fines imposed or damages ordered should be paid by the Party that has failed in its performance of its legal obligations under the Data Protection Laws, as decided by the relevant supervisory authority or competent court authorized to impose such fines or damages. Therefore, the limitations of liability set out under the Contract shall not, however, apply such fines.

15. Term and Termination

This DPA shall be in effect as long as the Parties have Contracts between them in force.

All provisions which by nature are intended to survive the termination of this DPA shall remain in full force and effect regardless of the termination of this DPA.