Terms and Conditions for the Provision of ESET Professional and Security Services (the "Terms")

Effective date: 04.04.2022

Provider: ESET, spol. s r.o., a company organized and existing under the laws of the Slovak Republic, with its registered seat at Einsteinova 24, 851 01 Bratislava, Slovak Republic, company identification No. (IČO): 31 333 532, registered in the Commercial Register of District Court Bratislava I, Section Sro, Insertion No. 3586/B (the "**ESET**").

Customer: A legal person who orders Services based on a separate Order issued by the person on behalf of whom the Terms are accepted and addressed to the ESET Partner. If the person submitting the Order accepts the Terms on behalf of a company or other legal entity, they represent and warrant that they have the authority to bind the entity to the Terms; in this case, the term "Customer" shall refer to this entity (the "**Customer**").

ESET and the Customer are jointly referred to as the "**Parties**" and individually as the "**Party.**"

BACKGROUND:

A. ESET is a world-renowned company that provides IT security solutions to its clients worldwide and that provides services specified herein to its business customers.

B. The Customer seeks to receive and use such services to assist with cybersecurity-related issues and protect its IT infrastructure.

C. ESET will use its expert knowledge and professional experience to deliver world-class service, as requested by the Customer and in accordance with the following Terms.

AGREED TERMS:

1. Definitions and Interpretation. Unless a particular provision of the Terms implies otherwise, the meaning of all capitalized terms contained herein shall be as defined in this Article or as ascribed to them in the provisions hereof. These capitalized terms, when defined, will be placed into quotation marks.

1.1 *"Assessment Form"* refers to a document created by ESET for the purpose of collecting the information required to perform specific activities included in the Service.

1.2 *"Distributor"* refers to ESET affiliate or partner distributing Services on certain territory, defined as "Distributor" in the applicable Order.

1.3 *"ESET Partner"* refers to a Distributor or its partner (reseller) from whom the Services are ordered by the Customer based on the Order and who supplies them to the Customer in accordance with the Order. ESET Partner is defined as "Supplier" in the applicable Order.

1.4 *"Man-Day"* refers to the time unit set to quantify the extent of the work necessary for the provision of the Services and/or execution of the Service Outcomes. One Man-Day represents eight (8) hours of work per person.

1.5 *"Services"* refers to one or more services specified in the Annexes to the Terms provided by ESET that were ordered by the Customer as per the Order.

1.6 *"Order"* refers to a written order for the provision of any of the Services issued by the Customer and addressed and delivered to the ESET Partner based on a Service Proposal (if applicable) that contains a reference to the Terms and uses a standard form provided to the Customer by ESET or the ESET Partner. No additional provisions stipulated in the Order are binding towards ESET or for provision of Services, unless the Terms expressly state that certain aspects of Services provision have to be or may be defined in the Order. The Terms apply and prevail over any additional or conflicting provisions in the Order, and any such additional or conflicting provisions shall be deemed as refused by ESET.

1.7 *"Product"* refers to a product provided by ESET to which the Services relate.

1.8 *"Representatives"* refers to person's entitlement or authority to act on behalf of ESET or the Customer in matters related to the performance of the Services and handover of the Service Outcome, as defined in the respective Order or other documentation related to the provision of Services.

1.9 *"Service Outcome" or "Output"* refers to any outcome other than a Product and any of its versions that will be delivered to the Customer in connection with the performance of the Services.

1.10 *"Service Proposal"* refers to a written offer for the provision of those Services, where customization is possible and where their scope changes based on the details stated in the Assessment Form and Products used by the Customer. The Service Proposal tailors the Services that shall be provided to the specific Customer beyond their specification in Annexes and is issued and delivered to the Customer by the ESET Partner based on the

assessment of the Customer´s environment. The applicable Annex specifies whether the Service Proposal will be issued in connection with a Service.

1.11 *"Site"* refers to the place where the Service is to be provided and/or where the Service Outcome is to be handed over to the Customer.

1.12 *"Third Party"* refers to any party other than ESET or the Customer.

2. Scope of Terms and their Binding Character.

2.1 The Terms regulate the provision of the Services by ESET and their use by the Customer, as well as the Parties´ rights and obligations in relation thereto.

2.2 The supply and delivery of both the Services and remuneration for their provision is beyond the scope of the Terms and will be agreed separately between the Customer and the ESET Partner based on the Order.

2.3 The Customer accepts the Terms and agrees to be bound by them to the full extent by executing the Order. The sending of the Order by the Customer to the ESET Partner is deemed an offer to conclude a contract between the Customer and ESET for the provision of Services, with its content fully determined by the Terms and the respective Order, to the extent it specifies the Services that shall be provided, the term hereof, and the related remuneration. The confirmation that ESET accepted the Order (not the confirmation that the ESET Partner received the Order) that is sent by ESET to the Customer via email is deemed ESET´s acceptance of the Customer´s offer to conclude a contract. The contract between ESET and the Customer on provision of the Services, with its content fully determined by both the Terms and the Order, to the extent it specifies the Services that shall be provided, the term hereof, and the related remuneration, will be concluded when confirmation that ESET accepted the Order is delivered to the Customer via email (the "**Contract**").

2.4 The Contract is entered into to enable provision of the Services that were ordered by the Customer from the ESET Partner by use of the Order but are provided by ESET. Therefore, the legal relationship between the Customer and the ESET Partner based on the Order shall be interpreted as primarily economic, where the ESET Partner´s main obligation is to procure the delivery of the ordered Services to the Customer, and the Customer´s main obligation is to pay the agreed remuneration for their provision to the ESET Partner.

3. Provision of the Services.

3.1 ESET shall provide the Customer with all the Services stated in the Order, which became binding pursuant to Clause 2.3 of the Terms. The Services and their scope is defined in the respective Annex to the Terms. If applicable, a detailed and customized scope of the Services to be provided to the Customer will be stated in the respective Service Proposal, which forms an annex to the respective Order.

3.2 ESET shall provide the Services on time, with due care, in a professional manner, and in compliance with the Terms and the Order.

3.3 Unless otherwise stated in the respective Order or Annex, ESET shall start to provide the Services at the moment of Contract conclusion. Services may be performed by telephone (hotline), remote access, on Site or by other means specified in the applicable Annex. ESET and the Customer shall comply with the computer security, safety, and access regulations that are provided to them by the other Party.

3.4 Unless agreed otherwise between the Parties, ESET shall have physical and/or remote access to the Site as necessary for the provision of each of the Services.

3.5 Each Service Outcome shall be provided to the Customer as described in the respective Annex.

3.6 ESET may engage subcontractors to perform any of the Services without the consent of the Customer. In such cases, ESET shall: (i) use the same degree of care in selecting the subcontractor as it would if the contractor were being retained to provide similar services to ESET; and (ii) in all cases, remain responsible for all of its obligations with respect to the scope of the Services/Service Outcomes, the standard for Services/Service Outcomes, and the content of the Services/Service Outcomes provided to the Customer.

4. Use of Services and its Restrictions.

4.1 The Customer shall use the Services only for its own business purposes, in a conventional manner, in accordance with the Terms and the applicable Annexes, and only for the purpose for which they are intended, as described in the respective Annex and Services documentation.

4.2 The Customer is forbidden to enable or allow the use of Services by any Third Party, including its affiliated entities, unless stated otherwise in the Order. Noncompliance with this obligation shall be deemed a substantial/material breach of the Terms.

4.3 The Services are only provided in relation to ESET Products, and unless stated otherwise, do not concern any Third-Party products or services. Some Services can only be provided in relation to a specific Product as specified in the Annex; therefore, obtaining a license for this Product is a prerequisite for the provision of such Service.

4.4 To use a Service, the Customer is obliged to send any request for its provision, as well as for the provision of any Service activities, solely in the manner and using means as specified in the applicable Annex.

4.5 The Customer undertakes to use the Services to a reasonable extent and not excessively. ESET reserves the right to refuse or limit the provision of Services or to charge additional fees via the ESET Partner in exceptional cases when it deems that the Customer´s use of the Services is significantly excessive compared to other customers of a similar character or when such use can be considered unreasonable. In the rare case that ESET invokes this fair-use clause, ESET will try to propose an alternative solution that shall help the Customer to accommodate their Service-related needs.

4.6 The Customer acknowledges, understands, and agrees to the following:

a) ESET will always aim for the highest standards when providing Services; however, ESET does not guarantee or warrant that it will find, locate, discover, prevent, warn of or respond to all threats, vulnerabilities, malware, or malicious software that might be present at the Customer´s IT infrastructure and will not hold ESET liable therefore.

b) If ESET provides any recommendations while providing the Services, they only have informative character. It is solely the Customer´s business decision to follow such recommendation.

c) If provision of the Service requires any intervention to the Customer´s IT infrastructure, it might result in malfunctioning or damage. Therefore, the Customer is obliged to notify ESET if any part of the infrastructure, which shall be subject to intervention, is critical for the functioning of the Customer´s infrastructure.

d) The Customer´s IT systems, documents, software, and other data shall be regularly backed up to prevent or minimize the risk of loss or damage.

e) Products and other related software shall be kept available, in operation, and up-to date (by updating and upgrading them regularly). In particular, the Customer shall install the latest version of the Products used no later than six (6) months after its release.

f) If any Customer´s hardware is to be sent to ESET for the purpose of the provision of Services, the Customer is obliged to pack it correctly to avoid any damage, as well as to fulfill other instructions or obligations imposed by the postal service.

ESET, ITS AFFILIATES, ESET PARTNERS, DISTRIBUTORS AND ITS SUPPLIERS CANNOT BE HELD LIABLE FOR ANY LOSSES OR DAMAGES CAUSED BY THE CUSTOMER´S FAILURE TO FULFILL ANY OF THE OBLIGATIONS ABOVE OR FOR THE CUSTOMER´S RELIANCE ON SERVICES OR THEIR OUTPUTS IN CONFLICT WITH ANY OF THE ABOVE ACKNOWLEDGMENTS.

5. Cooperation.

5.1 The Customer shall provide ESET through its Representatives with all the available information, documents, equipment and assistance that are necessary to fulfill the obligations of ESET according to the Terms and the Order or modified Order. Should the Customer fail to provide ESET with such cooperation, ESET shall not be liable for delays to the performed Services. In such cases, all agreed time periods and deadlines shall be extended by a period corresponding to the delay caused by the Customer.

5.2 The Customer shall keep information and documents, on which ESET has based or will base its assumptions for provided Services, accurate and up to date as well as to ensure that Products and related software are in operation, available, and up to date in accordance with Section 4.6e). Otherwise, ESET shall not be responsible for the quality of the provided Services and/or Service Outcomes.

5.3 The Customer may at any time require a change in the provided Services upon submitting a modified Order to ESET via the ESET Partner. Provisions of Section 2.3 shall be applied accordingly to submission and acceptance of the modified Order. ESET will attempt to accommodate the Customer´s new proposal; however, it reserves the right to refuse any modified Order submitted by the Customer without stating any reason. The confirmation of the modified Order will be delivered to the Customer by ESET via email and it shall modify the original Order as of the date thereof.

5.4 ESET, if using or accessing the Customer's premises or facilities, shall be obliged to comply with all reasonable directions and procedures relating to health and safety and security in operation at those premises or facilities, whether specifically drawn to the attention of ESET or as might reasonably be inferred from the circumstances.

5.5 Unless the Terms prescribe otherwise, the Customer undertakes to direct all communication in relation to the provision of the Services, mainly any complaints, requests, or other legal communication related thereto and addressed to ESET exclusively to the ESET´s Representative, if practicable.

6. License.

6.1 Unless otherwise agreed between the Parties, ESET reserves all intellectual property rights related to the Service Outcomes. At the time of delivery of the Service Outcomes, ESET grants the Customer an exclusive and non-transferable right to use the Service Outcomes exclusively for the internal purposes of the Customer. ESET will protect Service Outcomes created for the Customer and will not disclose them to a Third Party.

6.2 The license under the previous sentence is granted for the time of duration of ESET's intellectual property rights to Service Outcomes. The Customer is not entitled to change or modify the Service Outcomes (or any part of them) that are protected by intellectual property rights or distribute or disclose them to Third Parties. To avoid any doubt, the use of Service Outcomes for purposes other than this Article is a substantial/material breach of the Terms. Use of the Service Outcomes for other purposes as set out in this Article may only be based on prior written agreement of the Parties or the prior written consent of ESET. The Parties have agreed that the provisions of this Article will continue to be valid after termination of performance under the Terms.

7. Warranty.

7.1 ESET warrants that it has the necessary personal and material resources to ensure the provision of the Services by itself and/or by the qualified subcontractor.

7.2 ESET hereby warrants that to the best of its knowledge, the Services or Service Outcome do not infringe any copyright, patent, trade secret, or other intellectual property rights of Third Parties.

7.3 ESET provides Services on an “as is” basis and expressly declares that except for the warranty set out in Section 7.1 and 7.2, it provides no further expressed or implied representations or warranties, particularly those on merchantability or suitability for a particular purpose.

8. Limitation of Liability.

8.1 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL ESET, ITS AFFILIATES OR SUPPLIERS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, LOST BUSINESS OPPORTUNITIES, LOST DATA, COSTS OF DATA RESTORATION OR OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, INTERRUPTION OF BUSINESS OR FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, STATUTE, TORT, OR OTHER THEORY OF LIABILITY, EVEN IF THE PROVIDER, ITS SUPPLIERS OR AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES OR THE DAMAGES OR LOSSES WERE REASONABLY FORESEEABLE.

8.2 Either Party´s maximum aggregate liability for damages incurred by the other Party as a result of an action or omission of the liable Party shall be limited to the amount of the value of the respective Order, in direct relation to which the damage arose, unless stated otherwise in the respective Annex.

8.3 Nothing in the Terms excludes or restricts the liability of either Party for death or personal injury resulting from the negligence or liability incurred by one Party for fraud or fraudulent misrepresentation by the other Party.

8.4 The Parties jointly represent that having regard to all facts known to the Parties at the execution hereof, it cannot be foreseen that any damage that the Parties could incur from the Terms would exceed the value of the respective Order, in direct relation to which the damage arose.

9. Force Majeure.

9.1 The Parties shall not be liable for failure to comply with their obligations under the Contract if the performance of their duties is delayed or prevented by the intervention of a public enemy, acts of war, civil unrest, riots, demonstrations, fire, flood, earthquake, strike of the employees causing slowdown or interruption of work, a threat to national security, pandemics, internet outage, the inability to procure equipment, data or material from the respective suppliers even after making reasonable efforts, or by other circumstances beyond the control of the Parties (“**Force Majeure Event**”).

9.2 Exclusion of either Party’s liability for a Force Majeure Event shall be conditioned by the fact that the Force Majeure Event has not been caused by the intention or negligence of the respective Party, and the affected Party notified the other Party without undue delay of the Force Majeure Event in writing. The Party notifying the other Party of the Force Majeure Event is obliged to make a reasonable and customary effort to prevent the Force Majeure Event and minimize its possible consequences and duration. Following the end of the Force Majeure Event, the performance period shall be extended for the duration of the delay or the inability to meet the contracting obligations due to the Force Majeure Event. If the Force Majeure Event lasts longer than three (3) months, either Party shall be entitled to withdraw from the Contract and deliver the withdrawal to the other Party´s Representative.

10. Confidential Information Protection.

10.1 The Parties acknowledge a duty not to disclose any non-public information and data disclosed by the other Party during or after the term of the Contract without the other's prior written permission, whether in written, oral, electronic, website-based, or other form and without the need of their explicit identification as confidential by the disclosing Party (the "**Confidential Information**") and to protect and use them in accordance with the Terms.

10.2 The Terms impose no obligations with respect to Confidential Information that: (i) is already known by the receiving Party at the time of disclosure; (ii) is or becomes publicly available through no fault of the receiving Party; (iii) is independently developed by the receiving Party without the use of Confidential Information of the disclosing Party; or (iv) is lawfully obtained by the receiving Party from a third party who does not have an obligation of confidentiality to the disclosing Party.

10.3 The Parties agree to use Confidential Information only in relation to the provision and use of the Services, and for other purposes only if it was specifically agreed by the disclosing Party in writing (the "**Purpose**").

10.4 The Parties agree to protect Confidential Information disclosed to them with at least the same degree of care, but no less than a reasonable degree of care, as they normally exercise to protect their own Confidential Information of similar character and importance and shall prevent any use of Confidential Information not authorized in the Terms and any disclosure of Confidential Information to any third party or their publication.

10.5 Each Party shall ensure that the Confidential Information is only disclosed to their affiliates, officers, employees, agents, and contractors on a strict "need-to-know" basis to carry out the Purpose and that such affiliates, officers, employees, agents, and contractors are informed of their confidential nature and bound by obligations set out herein. The term "affiliates" refers to entities that are controlled by, controlling, or under common control with the Party. Notwithstanding the provisions of this Article 10, either Party may disclose Confidential Information to the extend it is necessary in accordance with their statutory duty. In such case the disclosing Party shall inform the other Party of the disclosure obligation in advance, at the latest without undue delay after becoming aware of the court or other official order, unless they are obliged to keep such information confidential.

10.6 Upon the disclosing Party's request, the receiving Party shall promptly return or destroy all Confidential Information received, together with all its copies, except for those copies of Confidential Information that have been created by automatic backup systems with limited retention periods if (i) their deletion would involve disproportionate effort and (ii) in case of their recovery, the receiving Party will refrain from any use of such copies and will delete them without undue delay. Additionally, the receiving Party shall certify in writing that all Confidential Information and copies thereof have been destroyed, and if applicable, that some copies of the Confidential Information were stored by its automatic backup systems.

10.7 All Confidential Information provided by the Parties under the Terms shall remain the property of the disclosing Party. Neither Party acquires any intellectual property rights to the Confidential Information of the disclosing Party except the limited rights necessary to carry out the Purpose, as set forth in this Article of the Terms.

10.8 The receiving Party´s duty to protect Confidential Information expires five (5) years from disclosure. In the case of termination or expiry of the Contract, the provisions of this Article of the Terms will survive as to Confidential Information that is disclosed before its termination or expiry.

10.9 Unless expressly provided herein, the Terms impose no obligation for a Party to exchange Confidential Information.

11. Term and Termination of the Contract.

11.1 The Contract shall become effective at the date of its conclusion pursuant to Section 2.3 of the Terms and shall remain effective through the whole term of provision of the Services as indicated in the Order.

11.2 The Contract shall terminate automatically in case of termination of the Order. To avoid any doubt, the termination of the Order means that it will end before being fully performed either by the ESET Partner or the Customer and does not include cases of successful completion of the Order.

11.3 The Parties shall have a right to terminate the Contract in case the other Party commits a substantial/material breach of the Contract and the breach remains unremedied for more than 30 days after a written notice of the breach is delivered to the Party. Notwithstanding the foregoing, if the breaching Party has in good faith commenced to remedy the material breach, and the remedy cannot be reasonably completed within the 30-day period, then the breaching Party will have an additional 30 (thirty) days to complete a remedy. In such cases, the other Party may terminate this Contract only if the failure continues unremedied after passing of the additional 30-day period. Moreover, the Parties are entitled to terminate the Contract with immediate effect if the other Party:

a) becomes (or may become) the object of bankruptcy or liquidation proceedings or if bankruptcy has been declared over a Party´s property,

b) ceases (or threatens to cease) to carry on business, or

c) is object to another similar event or proceeding under the applicable law.

11.4 ESET shall have a right to immediately terminate the Contract, fully or partially, if ESET becomes unable to provide the Services to the Customer or in the case of a substantial/material breach of Terms by the Customer, as specified herein. Moreover, ESET shall have right to cancel the Contract within five (5) business days after its conclusion.

11.5 Unless provided otherwise, both Parties shall direct all communication related to Contract termination to other Party´s Representative.

11.6 The Customer is entitled to terminate the Order before expiration of the subscription term of ordered Services and to claim a refund of paid Service fees under the conditions specified below and in the following cases: (i) if the Customer terminates the Contract due to ESET´s uncured breach or due to a change in the Terms in accordance with Section 12.5, (ii) if the Contract is cancelled in accordance with last sentence of Section 11.3, (iii) if ESET terminates the Contract due to its inability to provide Services or (iv) if the Customer terminates the Data Processing Agreement in Supplement A in accordance with its Art. 5. In such cases, the Customer is entitled to terminate the applicable Order by giving notice to the ESET Partner and to claim from the ESET Partner a refund of paid Service fees for the period from the date termination notice was delivered to the ESET Partner to the end of the Services subscription period specified in the Order. In such cases, the Contract shall terminate automatically with termination of the Order. ESET shall be entitled to the payment of the price for Services (or their part) that have already been provided.

11.7 Any termination of the Contract will not waive or otherwise adversely affect any other rights or remedies the terminating Party may have under the Terms. Upon termination or expiry of this Contract, all rights and duties of the Parties will be terminated, other than the obligations that, by their nature or by express provisions set forth in the Terms, should survive its termination or expiry.

12. Final Provisions.

12.1 The information security requirements and processing of personal data in relation to Services by ESET as a data processor shall be governed by a separate data processing agreement in Supplement A.

12.2 The Terms and the applicable Order (to the extent it specifies the Services which shall be provided, the term hereof, and the related remuneration), constitute the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior and collateral communications and understandings, including any marketing materials, requests for proposal, questionnaires, or reports. No failure or delay in exercising any right under the Terms will operate as a waiver of any term or condition hereunder.

12.3 In the event of any conflict between the Terms, the Annex to the Terms and Order (to the extend it specifies the Services which shall be provided, their term and the related remuneration), the following order of priority will apply: 1. Order, 2. Annex to the Terms, and 3. the Terms.

12.4 The Parties expressly declare that no current or future documents by which the Customer stipulates the purchase terms and conditions shall be applied in relation to the provision of Services. Both Parties hereby explicitly agree that no such documents shall be applied to ESET, even if ESET has not expressly refused or objected to their application either in whole or in part.

12.5 ESET may change the Terms unilaterally from time to time when such change is necessary due to changes to applicable laws, standards, or ESET business strategies, technical, security or organizational changes in ESET systems, or for the purpose of enhancing the quality, security, or accessibility of Services. In such cases, ESET is obliged to send the Customer a notice by sending an email to the Customer´s Representative and publishing it on a dedicated website. If the Customer does not agree with the change, they have a right to terminate the Contract within 30 days of receiving a notice of change. Unless the Customer refuses the proposed change within this time limit, it will be deemed accepted and become effective as of the date stipulated in the new version of the Terms. The Customer is obliged to keep its Representative's contact details up to date and to notify ESET without undue delay about any changes and therefore authorizes ESET to send the updated Terms to the last provided email address(es). ESET will not be liable for Customer's failure to receive the updated Terms due to failure to update the Customer Representative's contact information with ESET.

12.6 The Terms and/or Order (to the extent it specifies the Services which shall be provided, the term hereof and the related remuneration)shall be interpreted and governed under the following laws:

a) If the Order is addressed to ESET SOFTWARE UK LIMITED as a Distributor, then the laws of England and Wales apply without giving effect to the conflicts of law provisions,

b) If the Order is addressed to ESET, LLC. or ESET Canada Inc. as a Distributor, then the laws of State of California, United States of America apply, as if performed wholly within the state and without giving effect to the conflicts of law provisions,

c) If the Order is addressed to ESET Japan Inc. as a Distributor, then the laws of Japan apply without giving effect to the conflicts of law provisions, and

d) If the Order is addresses to any other Distributor than those above, then the laws of Slovak republic apply without giving effect to the conflicts of law provisions.

The laws specified above shall be also applicable to any non-contractual obligations that may arise in connection with the performance of Services. The Parties specifically disclaim the application of the UN Convention on Contracts for International Sale of Goods to the interpretation or enforcement of the Contract.

12.7 Any dispute or disagreement arising out of or in connection with the Contract, including any violation, termination, cancellation or invalidity of the Contract (the "**Dispute**"), shall be finally settled in accordance with this Section. The Parties shall first attempt to settle all Disputes by mutual negotiations in good faith striving to resolve the Dispute by agreement without arbitration. In case of a Dispute, the Party shall be obliged to deliver to the other Party a written notice of the Dispute, in which it shall specify the scope of the Dispute and propose the date and time of negotiations. If the Parties fail to resolve the Dispute without arbitration (including if the noticed Party is inactive in mutual negotiations) within 30 days from delivery of the notice, the Party may initiate arbitration. Any Dispute shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce (the "**ICC**") in the location specified below by one or more arbitrators appointed in accordance with the said Rules. No award or procedural order made in the arbitration shall be published. The Emergency Arbitrator Provisions shall not apply. The Parties agree that the Dispute shall be finally settled by one arbitrator in case its value is 1 million EUR or smaller, and by three arbitrators in case its value is higher. The arbitration shall be held in English, the governing law of arbitration shall be as specified in Section 12.6 of the Terms and the place of arbitration shall be:

a) ICC United Kingdom in London in case the Order is addressed to ESET SOFTWARE UK LIMITED as a Distributor,

b) ICC United States in New York in case the Order is addressed to ESET, LLC. or ESET Canada Inc. as a Distributor,

c) ICC Japan in Tokyo in case the Order is addressed to ESET Japan Inc. as a Distributor, and

d) ICC Austria in Vienna in case the Order is addresses to any other Distributor then those above.

12.8 Except as expressly set forth in the Terms, neither Party has the right to assign, license, or sub-license any of its rights or obligations hereunder without the prior written consent of the other Party, which shall not be unreasonably withheld. Any assignment, license, or sub-license attempted without such consent will be void. Notwithstanding the foregoing, a Party may assign this Agreement as part of a corporate reorganization, consolidation, merger, or sale of substantially all its assets or capital stock.

12.9 If any provision of the Terms shall be held by a court of competent jurisdiction to be illegal, invalid, or unenforceable, the remaining provisions shall remain in full force and effect. The Terms have been executed by the Parties in English. In case any translation of the Terms is prepared for the convenience or any other purpose, the provisions of the English version of the Terms shall prevail.

Date: 28.03.2022

DocuSigned by:
Richard Marko
C177EE0A6254489...

Name: Richard Marko
Title: CEO
ESET spol. s r.o.

Supplemental Terms and Conditions.

Annexes:

Annex no. 1 – Specification of ESET Professional Services.

Annex no. 2 – Specification of ESET Security Services.

Annex no. 1. – Specification of ESET Professional Services

PREAMBLE.

1.1 Professional Services are a set of services aimed at the thorough care of the Customer´s Products.

1.2 Professional Services include the following services:

A. ESET Premium Support Advanced Service.
B. ESET Deployment and Upgrade Service.
C. ESET HealthCheck Service.
D. ESET Premium Support Essential Service.

A. ESET Premium Support Advanced Service.

a. General Provisions.

1. Description of the ESET Premium Support Advanced Service.

1.1 ESET Premium Support Advanced Service is the most robust service from the ESET Professional Services. ESET Premium Support Advanced Service consists of the following Activities:

a. Deployment and Upgrade Activity.
b. HealthCheck Activity.
c. Premium Support Activity.

1.2 Provision of the ESET Premium Support Advanced Service shall be possible under the condition that the Customer has purchased the ESET Premium Support Advanced Service for the adequate number of seats as calculated by the ESET Partner. Provided that the Customer modifies the Product licenses they use, including when they increase the number of seats during the provision of ESET Premium Support Advanced Service, they are also obliged to modify the ESET Premium Support Advanced Service to reflect this change.

2. Terms for Provision of the ESET Premium Support Advanced Service.

1.1 To use the Service, the Customer shall be obliged to submit a Request for its provision in accordance with this Annex. The term "**Request**" shall mean the Customer´s request for provision of any Activity included in the ESET Premium Support Advanced Service submitted in accordance with Request Submission Procedure specified in Art. 13 below.

1.2 The Customer is entitled to request either one Deployment or one Upgrade Activity in each one-year term of provision of ESET Premium Support Advanced Service. The Upgrade Activity would ideally be executed later in the Product license lifecycle. ESET shall provide the Deployment and/or Upgrade Activity anytime during the term of provision of ESET Premium Support Advanced Services and within 30 days from the submission of the Customer´s Request .

a. The Deployment Activity consists of one Deployment Activity delivery. One Deployment Activity delivery accounts for the deployment of 100 units of purchased Products into Customer´s infrastructure on selected endpoints, unless stated otherwise in the Service Proposal. The structure of endpoint selection will be identified and specified by the deployment team in the Deployment Plan, but may be subject to change upon agreement with the Customer. The Customer will then obtain a manual on how to upgrade the rest of Products in its infrastructure as well as required installation packages. If more than one Deployment Activity delivery is suggested by ESET, the Customer will be informed within the Service Proposal. Within one Deployment Activity delivery, the ESET Specialist deploys the corresponding number of Product(s) to the corresponding number of seats and leaves the administrator of the Customer with created installation packages and precise instructions on how to deploy the rest of the Product(s) on the remaining number of seats.

b. The Upgrade Activity consists of one Activity delivery. One Upgrade Activity delivery accounts for upgrade of 100 units of Products in Customer´s infrastructure on selected endpoints, unless stated otherwise in the Service Proposal. The structure of endpoint selection will be identified and specified by the deployment team in the Deployment Plan, but may be subject to change upon agreement with the Customer. The Customer will then obtain a manual on how to upgrade the rest of Products in its infrastructure as well as

required installation packages. If more than one Upgrade Activity delivery is suggested by ESET, the Customer will be informed within the Service Proposal. Within one Upgrade Activity delivery, the ESET Specialist upgrades the corresponding number of Product(s) for the corresponding number of seats and leaves the administrator of the Customer with created installation packages and precise instructions on how to upgrade the rest of the Product(s) on the remaining number of seats.

1.3 A HealthCheck Activity would ideally be executed later in the Product license's lifecycle (e.g., after three months of Product license validity) to verify how effectively the Product was initially set up and how effectively the Customer altered the initial settings. The HealthCheck Activity consists of one Activity delivery. One Activity delivery accounts for a maximum of one Man-Day, and this time includes time spent on preparing an S&R Document. If more than one Activity delivery is suggested by ESET, the Customer will be informed within the Assessment form. The Customer is entitled to request one HealthCheck Activity in each one-year term of provision of ESET Premium Support Advanced Service. The Customer shall send a Request for the provision of the HealthCheck Activity at least 21 days prior to the desired commencement of the provision of the HealthCheck Activity and no later than 21 days before passing of the agreed term of provision of ESET Premium Support Advanced Services. ESET shall provide a HealthCheck Activity during the term of provision of ESET Premium Support Advanced Services and within 21 days from the submission of the Customer´s Request , unless stated otherwise in the Service Proposal.

1.4 The Premium Support Activity shall be provided continuously after the effectiveness of the Contract.

b. Specification of Deployment and Upgrade Activity.

3. Definitions.

Unless a particular provision of this Annex implies otherwise, the meaning of all capitalized terms contained herein shall be as defined in this Article, in the main body of the Terms, or as ascribed to them in the particular provisions herein. Such capitalized terms, when defined, will be placed into quotation marks.

1.1 **"Acceptance Procedure"** refers to the process of verification by the Customer that delivered Activity fully complies with the requirements agreed in the Service Proposal. The standard Acceptance Procedure period is fourteen (14) days from the Activity completion date stated in the Order, unless otherwise agreed between the Parties.

1.2 **"Deployment Plan"** refers to a document created by ESET based upon the Service Proposal. It mainly specifies the scope, dates, and service delivery type (on-site or remote).

1.3 **"Deployment Activity" or "Activity"** refers to the installation and configuration of the Product within the Customer's environment on a scale and to the extent defined within this Annex and the Service Proposal. The Product(s) to be deployed and installation methods to be used are based on the initial assessment of the Customer's environment.

1.4 **"Upgrade Activity" or "Activity"** refers to the update and configuration of the Product within the Customer's environment, on a scale and to the extent defined within this Annex and the Service Proposal. To avoid any doubt, the Upgrade Activity is applicable not only in the case of major version changes, such as going from v5 to v6, but also from v6.1 to v6.2.

1.5 **"Specialist"** refers to an employee of ESET or of its subcontractor providing the Activity.

4. Performance of the Deployment and Upgrade Activity and Acceptance Procedure.

1.1 The Deployment and Upgrade Activity may be done by either remote access or on-site.

1.2 The Customer empowers ESET to express its consent to the terms and conditions of EULA as the Customer´s representative.

1.3 The Acceptance Procedure for the Deployment and Upgrade Activity shall result in the following:

a. If the Deployment and Upgrade Activity stated in the Service Proposal is fully delivered, the Representative of the Customer shall confirm the acceptance protocol with their signature (the "**Acceptance Protocol**").

b. If any part of Deployment and Upgrade Activity stated in the Service Proposal remains undelivered, the Representative of the Customer shall mention this fact in the Acceptance Protocol and agree with the Representative of ESET on an additional period for delivery of undelivered part of Activity. If the Parties do not agree on a period for the elimination of defects, the period for the elimination of defects is 30 days.

c. If the Representative of the Customer unreasonably refuses to confirm the delivery of any Activity stated in the Order or a Service Proposal, such Activity shall be deemed accepted without reservation.

c. Specification of the HealthCheck Activity.

5. Definitions.

Unless a particular provision of this Annex implies otherwise, the meanings of all capitalized terms contained herein shall be as defined in this Article, in the main body of the Terms, or as ascribed to them in the particular provisions herein. Such capitalized terms, when defined, will be placed into quotation marks.

1.1 **"HealthCheck Activity"** or **"Activity"** refers to an activity providing a thorough inspection of the ESET Product(s) specified in the Assessment Form installed in the Customer´s IT environment, with a focus on their integration within the Customer´s IT infrastructure and correctness and effectiveness of their configuration and settings. The Activity outcomes are summarized in the S&R Document.

1.2 **"HealthCheck Plan"** refers to a document created by ESET based on the information recorded in the Assessment Form, which specifies particular areas of Product settings/policies/tasks/reports that will be inspected as part of the Activity execution, the approximate scope of the Activity delivery, and its relevant technical details, such as the date of Activity delivery and delivery type (on-site or remote).

1.3 **"Suggestions & Recommendations Document"** or **"S&R Document"** refers to an Activity Output—a document created by ESET that summarizes the findings and makes recommendations for improvements to ESET Product´s environment (also in the context of the Customer´s IT infrastructure components that are necessary for the operation of ESET Products).

6. Performance of the Activity.

1.1 The Activity may be done by remote access or on Site.

1.2 Provision of the Activity shall be completed when the Customer confirms the acceptance of the S&R Document by their signature and either sends the signed version to the email address of ESET´s Representative or upload it to the original Request submitted via technical support request form. The S&R Document shall be sent by ESET to the email address of the Representative of the Customer after Activity completion. If any part of Activity stated in the HealthCheck Plan remains undelivered , the Representative of the Customer shall mention this fact in the S&R Document and agree with the Representative of ESET on an additional period for the delivery of undelivered part of Activity by harmonizing the S&R Document. If the Parties do not agree on a period for harmonization, this period shall be ten (10) days. After the harmonization of the S&R Document, the Customer shall confirm the acceptance of the harmonized S&R Document with their signature and either send it to the email address of ESET´s Representative or by upload it to the original Request submitted via technical support request form. If the Representative of the Customer unreasonably refuses to confirm the S&R Document, even after the ESET Representative declares that the S&R Document is in full accordance with HealthCheck Plan, the Activity delivery shall be deemed accepted without reservation.

d. Specification of the Premium Support Activity.

7. Definitions.

Unless a particular provision of this Annex implies otherwise, the meaning of all capitalized terms contained herein shall be as defined in this Article, in the main body of the Terms, or as ascribed to them in the particular provisions herein. Such capitalized terms, when defined, will be placed into quotation marks.

1.1 **"Agent"** refers to an employee of ESET or its subcontractor that provides technical support to the Customer.

1.2 **"Error"** refers to such Product functionality that is inconsistent with the description of the Product functionalities contained in the documentation. The definition of an Error shall not include a decreased or restricted Product functionality occasioned by a Third-Party Product inhibiting the use of technologies in the Product. ESET shall not be liable for solving Errors resulting from defects in hardware and software supplied by a third party or from errors made by persons who are neither employed nor contracted by ESET.

1.3 **"Premium Support Activity" or "Activity**" refers to technical support provided by ESET under conditions defined herein in relation to Errors occurring in Products that are installed in the Customer´s IT environment, which goes beyond the scope of end-user support, as defined in the respective Software's End User License Agreement.

1.4 **"Severity Levels"** refers to the fact that Errors are classified into A (critical), B (Serious), and C (Common) Severity Levels. An Error of the "A" Severity Level means that the Product or its main functionality either does not work or is suffering from regular/intermittent problems that significantly affect the ability to use the Product. An Error of the "B" Severity Level means that the Product functionality is defective, missing or causes difficulties that make the Product harder to use, but it is not unusable. An Error of the "C" Severity Level means that the Customer is suffering from a slight performance decrease or minor problems that require modifications to be made to the Product or the documentation.

1.5 **"Temporary Solution"** refers to short-term Product adjustments delivered to the Customer in the form of a hotfix or patch.

1.6 **"Work-Around"** refers to circumventing an Error for a certain time or converting it into an Error of a lower Severity Level. A Work-Around shall be replaced by a Permanent Solution, unless otherwise agreed with the Customer.

1.7 **"Permanent Solution"** refers to a product change (e.g., an update to a Product module) that corrects the Error and puts the Product in line with the documentation.

1.8 **"Reproducible Test Case"** refers to a test code that demonstrates, on a small portion of the code, the portion customarily not exceeding 100 lines, or in a text format, a specific syntax, or case in which an Error occurs. A

Reproducible Test Case must demonstrate inconsistency between a Product and its documentation.

1.9 **"Technical Support Case" or "TSC"** refers to an Error being reported and submitted by the Customer, an Error being solved/ being handled by the Agent, and finally, a confirmation by the Agent that the Error is fixed.

8. **Submitting a Request.**

1.1 When submitting a Request, the Customer is required to proceed in accordance with Article 13 hereto. For avoidance of any doubt, the term "Request" includes reporting any Error and submitting any Technical Support Case by the Customer.

1.2 If, when reporting an Error, the Customer does not follow the procedure laid down in Article 13 hereto, this shall be regarded as failure to provide cooperation under the Article 9. The submission of a Technical Support Case shall be confirmed by the Agent, as described in Article 13 hereto.

9. **Cooperation.**

1.1 When submitting a Request, the Customer shall provide the necessary information as required by the Agent. For the purposes hereof, such necessary information include but are not limited to:

a. Information required under Article 13 hereto.
b. Technical data on computer systems and on installed programs according to the Agent's requirements.
c. Providing remote access and granting the rights required to carry out a remote intervention.
d. The presence and assistance of the Customer's qualified staff in the case of an intervention being carried out on the Customer's premises.

1.2 If the Customer provides no cooperation and assistance, the Agent may close a particular Technical Support Case upon the expiration of 24 hours after sending the second notice demanding cooperation to the contact email address stated in the submitted TSC.

10. **Error Categorization.** The Severity Level of an Error and its category shall be proposed by the Customer and confirmed by the Agent. ESET reserves the right to change the category of the Error based on the outcomes of its initial analysis.

11. **Solution Mode.** A Work-Around, Temporary Solution, or a Permanent Solution, as the case may be, shall be employed to solve an Error. An Error requiring a Temporary Solution shall be deemed solved if the Error replication tests demonstrate that the product functionality accords with the documentation.

12. **Guaranteed Parameters.** The complexity of the Product and specific circumstances, such as the Customer's hardware or third-party software prevent specification of fixed solution times for TSCs, as such times and their lengths depend on the nature and complexity of an Error. ESET, however, shall use its best efforts to solve TSCs as soon as practicable on a "best-effort" basis. However, ESET guarantees the following Premium Support Activity parameters:

Table 1 – Guaranteed SLA Parameters

Guaranteed Parameter	Premium Support
Initial human response time after reporting an Error by the Customer in accordance with Article 13 hereto:	
- Error severity A:	max. 2 hours
- Error severity B:	max. 4 hours
- Error severity C:	max. 1 workday
Technical support availability	24/7/365
Solution time	best effort

13. **Request Submission Procedures.**

1.1 When submitting a Request, the Customer shall provide all information required by the form or the Agent, such as:

a. License data, such as public license ID.
b. Information on the Customer's contact person, such as their name, surname, job position, and contact phone number.
c. Functional email contact address and a detailed description of the Error so that Error replication and/or Reproducible Test Case is possible.

1.2 If, when submitting a Request, the Customer provides inaccurate or incomplete information, the Agent shall demand that the information is completed or corrected; in the meantime, no period or solution time shall be

running under the Terms.

1.3 Requests relating to Errors of the "A" Severity Level shall only be submitted by the Customer to the designated phone number ("HOT PHONE"). The Customer may only call the HOT PHONE using the contact phone numbers they provided to ESET. No CLIR or other similar function restricting the identification of the calling line must be activated on the Customer's contact phone numbers at the time of submitting such Requests relating to an Error of the "A" severity level. If all HOT PHONE lines are busy, the Customer shall leave a message in the voicemail, which is considered as proper Request submission.

1.4 All the other Requests, including Errors of the "B" and "C" Severity Levels shall be submitted by the Customer on either a technical support request form or a HELPDESK phone line. Submission of the Request shall be taken to mean the following:

a. When using a technical support request form: The proper completion of all required data and confirmations in the form, and the subsequent receipt from ESET of an automatically generated email message confirming that the Request was successfully submitted.

b. When using the HELPDESK phone line number: The provision of all information required by the Agent, and the subsequent receipt from ESET of an automatically generated email message confirming that the Request was successfully submitted

c. A confirmation email message shall be sent to the Customer's email contact address stated in the form. If a confirmation email message is not received by the Customer within ten (10) minutes after attempting to submit the Request, the Customer shall proceed according to Section 1.3 hereto.

1.5 Escalation contacts not specified in this Article 14 (e.g., HOT PHONE, HELPDESK phone line) shall be filled in in a separate document (e.g., contact escalation sheet for submission of Requests, technical support request form) provided to the Customer by the ESET Partner before ESET starts to provide the Service.

14. Handling of Requests.

1.1 All Technical Support Cases shall be handled and an Error shall be considered fixed when any of the following occurs:

a. The Customer confirms via email to the Agent that the solution proposed for the given Technical Support Case is efficient.

b. The Customer does not respond to the Agent's email notice demanding a confirmation of the efficiency of the solution proposed for the given Technical Support Case within seven (7) days after receiving the demand notice.

c. Upon the expiration of 24 hours after sending the second notice demanding cooperation pursuant to Article 9 hereof.

1.2 Requests related to provision of HealthCheck or Deployment/Upgrade Activity shall be handled by performance of the related Activity and in accordance with conditions prescribed in Art. 2 of this Annex, Sections 1.2 and 1.3.

15. Number of Technical Support Cases. The Number of Technical Support Cases eligible for the Activity is not limited. To avoid any doubt, Article 4, Section 4.5 of the Terms shall not be affected.

16. **Priority Access to Development Teams.** If an Error arises in the Customer´s environment and Product development teams need to be involved for its investigation/resolution, such Request from the Customer who uses the Service will be handled as a TSC with higher priority and therefore faster. .

17. **Proactive Informative Services.** If either a sudden Product incompatibility with a new operating system update or a similar technical issue occurs, ESET shall immediately start working on resolving the issue and inform the Customer of the issue and mitigation of its effects with regards to the infrastructure of the Customer.

18. **Account Manager.** The account manager shall be dedicated to being attentive to the Customer´s needs during the provision of the Service. The accountmanager shall approach the Customer proactively to check when a particular Activity or individual actions within it need to be executed.

B. ESET Deployment and Upgrade Service.

1.1 The ESET Deployment and Upgrade Service is the same Service as the Deployment and Upgrade Activity described in Annex no. 1, Articles 3. and 4. therein, while the term "Activity" shall be replaced with the term "Service."

1.2 The ESET Deployment and Upgrade Service consists of one Deployment and Upgrade Service Delivery. One Deployment and Upgrade Service delivery accounts for a maximum of one Man-Day, and the Customer is entitled to request either a Deployment Service or an Upgrade Service within one Deployment and Upgrade Service Delivery. This time includes the time spent preparing the Service Proposal. If more than one Deployment and Upgrade Service Delivery is suggested by ESET, the Customer will be informed within the Service Proposal.

1.3 ESET shall provide the Deployment and Upgrade Service within 30 days from the submission of the Customer´s Request unless stated otherwise in the Service Proposal.

C. ESET HealthCheck Service.

1.1 The ESET HealthCheck Service is the same Service as the HealthCheck Activity described in Annex no. 1, Articles 5. and 6. therein, while the term "Activity" shall be replaced with the term "Service."
1.2 The ESET HealthCheck Service consists of one HealthCheck Service Delivery. One HealthCheck Service delivery accounts for a maximum of one Man-Day, and this time includes the time spent preparing an S&R Document. If more than one HealthCheck Service Delivery is suggested by ESET, the Customer will be informed within the HealthCheck Plan.
1.3 ESET shall provide the ESET HealthCheck Service within 21 days from the submission of the Customer´s Request unless stated otherwise in the HealthCheck Plan.

D. ESET Premium Support Essential Service

1.1 ESET Premium Support Essential Service is the same Service as the Premium Support Activity described in Annex no. 1, Articles 7. to 14. therein, and the term "Activity" shall be replaced with the term "Service."
1.2 Provision of the ESET Premium Support Essential Service shall be possible under the condition that the Customer has purchased the ESET Premium Support Essential Service for the adequate number of seats as calculated by ESET Partner. Provided that the Customer modifies the Product licenses they use, including when they increase the number of seats during the provision of ESET Premium Support Essential Service, they are also obliged to modify the ESET Premium Support Essential Service to reflect this change.
1.3 If the resolution of a particular Technical Support Case requires the performance of activities that form the basis of another Service offered by ESET, ESET reserves the right not to resolve such TSCs. The Customer shall be proposed to purchase this additional service; however, it is up to the Customer whether they purchase the offered Service.
1.4 Provision of the ESET Premium Support Essential Service shall be possible under the condition that the Customer has purchased the ESET Premium Support Essential Service for all their Product licenses. Provided that the Customer increases the number of their Product licenses during the provision of ESET Premium Support Essential Service, they are also obliged to enlarge the ESET Premium Support Essential Service to the extent corresponding to the number of increased Product licenses.
1.5 ESET shall start to provide the ESET Premium Support Essential Service after the Contract effective date and for the term stated in the Order.

Annex no. 2 – Specification of ESET Security Services

PREAMBLE.

1.1 ESET Security Service´s purpose is to support the Customer with cybersecurity Issues and anomalies that range from missing detections, file analysis, digital forensic, incident response, and other security-related Issues, Events, or Threats that occur in the Customer´s IT infrastructure in accordance with the conditions defined in this Annex.
1.2 ESET Security Services include the following services:
A. ESET Detection and Response Essential Service.
B. ESET Detection and Response Advanced Service.
C. ESET Detection and Response Ultimate Service.
Each Service consists of several Activities, as described in the following Table:

Included in the Service	Issue/Request type	Issue description	Activity description	Required inputs and resulting Outputs	Dynamic SLA (based on Severity A. / B. /C.) Response times
Detection & Response Essential / Detection & Response Advanced / Detection & Response Ultimate	Malware: missing detection.	Malware is not detected.	Submitted file, URL, domain or IP is analyzed, and if found malicious, detection is added and information about the malware family is provided.	Input: Product version, file/URL/domain/IP, Product version. Output: if the input is found malicious, information about added detection (incl. detection name) is	**A. 2 / B. 4 / C. 24 hours**

				provided; otherwise, a clean status is confirmed.	
	Malware: cleaning problem.	Malware is detected but cannot be cleaned.	Cleaning of the submitted file is tested and improved if found to be problematic. In special cases, a standalone cleaner application might be provided.	Input: Product version, file, logs, information about environment. Output: if cleaning is improved, information about the planned fix is provided; standalone cleaner application/procedure if applicable.	**A. 2 / B. 4 / C. 24 hours**
	Malware: ransomware infection.	System is infected with ransomware.	Ransomware infection is evaluated and if decryption is possible, a decryptor is provided (existing or new). Otherwise, basic mitigation and prevention hints are provided.	Input: Product version, examples of encrypted files, payment info file, logs, malware sample (if indicated in the GPC table). Output: decryptor (if possible); otherwise, basic mitigation and prevention hints.	**A. 2 / B. 4 / C. 24 hours**
	False positive	File, URL, domain, or IP is falsely detected.	Submitted file, URL, domain, or IP is analyzed, and if found falsely detected, detection is removed.	Input: Product version, file/URL/domain/IP, logs, screenshots. Output: if the input is found malicious, information about removed detection is provided.	**A. 2 / B. 4 / C. 24 hours**
	General: Suspicious behavior investigation	Suspicious behavior not linked to any other listed category.	Based on the description of suspicious behavior and other provided data, the behavior is analyzed, and a potential solution is suggested.	Input: Product version, suspicious behavior description, logs, information about environment, additional data on request, incl. remote connection in specific cases. Output: if possible, the problem is resolved, along with basic information.	**A. 2 / B. 4 / C. 24 hours**
	Basic file analysis	Basic info about the file is needed.	Is the submitted file clean or malicious? If clean, basic info is provided. If malicious, reasons for detection, malware family, and basic info about functionality is provided.	Input: file; questions are specified Output: analysis result, along with basic information	**A. 2 / B. 4 / C. 24 hours**
	Detailed file analysis	Detailed info about malware is needed.	Is the submitted file clean or malicious? If clean, basic info is provided. If malicious, reasons for detection, malware family, and detailed info about functionality is provided.	Input: file. Output: analysis result, along with detailed information.	**A. 2 / B. 4 / C. 24 hours**
	Digital forensic analysis	An incident needs to be investigated. All data will be submitted, and no live interaction is needed. It is a post-	Data from the affected environment is analyzed. The requested level of information is provided. Activities are limited to malware/cybersecurity	Input: Data from the environment: disk clone, memory dump, files, …; questions or/and level of detail Is specified. Output: analysis result.	**A. 2 / B. 4 / C. 24 hours**

		incident investigation.	attack-related cases only. The analysis is not a form of expert witnessing suitable for law-enforcement and court case scenarios.		
	Digital forensic incident response assistance / DFIR assistance	An incident needs to be investigated, it's an ongoing incident, interaction is provided (phone call, remote connection). This is not full-blown DFIR, it is DFIR assistance.	The incident is investigated online. A consultation of cybersecurity-related topics from the technical standpoint is provided. This may lead to a file analysis and/or digital forensic. Activities are limited to malware/cybersecurity attack-related cases only and not cases, such as PR issue mitigation and similar areas.	Input: Data from the environment, access to the environment; questions and/or level of detail is specified; info about already investigated/identified facts. Output: any of the following: consultancy, changes in the environment, Report, redirection to another service.	**A. 2 / B. 4 / C. 24 hours**
Detection & Response Advanced / Detection & Response Ultimate	EI: rules support.	Support related to rule creation, modification or disfunction, e.g., to detect specific malware behavior.	Specified rule or behavior is analyzed and consultation is provided.	Input: version of EI, rules, specification of the problem, if it turns out to be a bug—logs, database/database access. Output: consultation and recommendation on how to set up the desired rule.	**A. 2 / B. 4 / C. 24 hours**
	EI: exclusions support.	Support related to exclusion creation, modification, or disfunction is needed.	Specified exclusion or behavior is analyzed and a consultation is provided.	Input: version of EI, exclusion, specification of the problem, if it turns out to be a bug—logs, database/database access. Output: consultation and recommendation on how to set up the desired exclusion.	**A. 2 / B. 4 / C. 24 hours**
	EI: general security related question.	EI security-related question not linked to any other listed category.	Specified behavior is analyzed. Result may be advice for the Customer or bug/improvement for developers.	Input: version of EI, specification of the problem, if it turns out to be a bug—logs, database/database access. Output: consultation and recommendation on how to achieve desired outcome.	**A. 2 / B. 4 / C. 24 hours**
	EI: Initial Optimization	After the installation of EI to a new environment, EI generates large number of false positives (FP).	One-time action. Most frequent FP detections in the EI environment are checked. Exclusions are created. Custom rules may be created, or rules may be modified to reflect expectations.	Input: Assessment form, access to the environment, or exported data. Output: Optimization Report, changes within the EI environment, such as creation/modification of rules and exclusions.	**N/A** (planned activity performed in agreed timeframe)

Detection & Response Advanced	EI: Threat Hunting (on-demand).	The Customer wants to have their environment inspected to see whether there are any Threats present (one-time inspection).	One-time action. Environment is inspected using EI. Information will be provided on any Threats or weaknesses. Advice will be provided. Individual steps will be defined in checklist.	Input: assessment form, access to the environment. Output: Threat Hunting Report.	**A. 2 / B. 4 / C. 24 hours**
Detection & Response Ultimate	EI: Threat Monitoring.	The Customer wants to have their environment monitored by security professionals	Continuous action. The Customer's environment is checked each day (using the EI console). Suspicious EI detections are verified. False positive detections are resolved. Correct detections are reported to the Customer (reports sent at specified intervals). When detection is significant and urgent, the Customer is notified immediately through emergency contact.	Input: assessment form, access to the environment. Output: periodic bi-weekly Reports, periodic sync calls, emergency reports, changes to the EI environment.	**N/A** (continuous activity)
	EI: Threat Hunting (pro-active)	Proactive periodical inspection of the Customer's environment based on ESET's threat intelligence.	Periodic action. Environment is inspected using EI. The Customer will be informed about any found threats or weaknesses. Advice will be provided. Individual steps will be defined in the checklist.	Input: assessment form, access to the environment Output: periodic Reports, periodic sync calls, emergency reports, changes to the EI environment.	**N/A** (planned Activity performed by ESET once within every three (3) months).
	Deployment & Upgrade	Complimentary professional service to perform initial deployment of EI and related products/components required for proper EI operation. Subsequent upgrades to their latest version.	One time action. ESET team will deploy or upgrade the EI console and related ESET Products/components specified in this Annex, Art. 2 C, Section 1.2. (as agreed with the Customer). Deployment & Upgrade will be carried out by ESET by deploying/upgrading of 100 units of Products/components. Manual on how to finish these deployments and upgrades is shared with Customers.	Input: assessment form, Output: acceptance protocol	**N/A** (planned Activity performed by ESET).

1. Definitions.

Unless a particular provision of this Annex implies otherwise, the meanings of all capitalized terms contained in this Annex will be as defined in this Article, in the main body of the Terms, or as ascribed to them in the particular provisions herein. Such capitalized terms, when defined, will be placed into quotation marks.

1.1 **"Availability"** refers to the time during which ESET and its subcontractors are available to provide Services to Customers and respond within the SLA specified for each particular Service.

1.2 **"Critical Event(s)"** refers to Events that are deemed by ESET as requiring further attention, as they might represent a potential Threat.

1.3 **"Deployment and Upgrade Activity"** refers to the meaning as ascribed to it in Annex no. 1, Articles 3. and 4. and Article 2., Section 1.1. with the distinction that the Customer will be contacted by ESET proactively about the timing of its performance and that the Deployment and Upgrade Activity will be performed in relation to Products specified in this Annex, Art. 2 C, Section 1.2.

1.4 **"Detection (in EI v1.4 or newer)" or "Alarm (in EI v1.3 or older)"** refers to information displayed in EI intended to warn of a potential Threat. EI includes the ESET rule-based detection engine for indicators of attack. The Rules written to identify suspicious malicious behavior trigger Alarms with defined severities. Each triggered Alarm is displayed in the Alarm section with a clear identification of where it happened (computer), and which executable and process has triggered it. It is accompanied with the severity information, as defined in the Rules, and a priority can be assigned to each of the Alarms.

1.5 **"Event"** refers to any event that happened at the endpoints in the Customer's infrastructure that are being monitored and recorded by EI. These Events are reported to EI from EI Agents that are deployed on the said endpoints within the Customer's infrastructure. These Events are analyzed by Operators as part of the Threat Hunting and Threat Monitoring activities.

1.6 **"EI"** refers to the ESET Inspect or ESET Inspect Cloud, ESET´s endpoint detection and response product (EDR).

1.7 **"EI Agent"** refers to a small application that acts as a translator/communication interface between installed ESET security Products and the EI server. It extracts all relevant low-level events from ESET security Products and sends them to the EI server. The EI Agent requires the ESET security Product to be installed before deployment. The EI Agent needs its own license to work properly and send Events to the ESET EI server. The EI Agent is crucial for situations when Events from an endpoint cannot be delivered to the EI server; for example, when there is no network connection available. Data is then stored locally on the endpoint and delivered as soon as the device's network connection is restored.

1.8 **"Issue"** refers to a cyber security-related problem occurring in the Customer´s IT infrastructure that the Customer wishes to report and that is defined in the Table.

1.9 **"Operator"** refers to an employee of ESET or of its subcontractor that provides Services to Customers.

1.10 **"Report"** refers to a type of final Service output—a document created by ESET that contains a summary of actions performed by ESET Operators their findings, recommendations, and any other information deemed relevant to the particular Service activity sub-type (e.g., a Threat Hunting Report or a malware analysis Report) and shall be delivered to the Customer via email.

1.11 **"Request"** refers to any request by Customers in relation to the security of their environment and Products deployed within, where the request is not a Product error report. To avoid any doubt, Requests relate (but are not limited) to file and incident analyses, response and mitigation, Threat hunting, EI security-related topics (not product errors), such as Rule and Exclusion, and support and optimization.

1.12 **"Response Times"** are guaranteed for the Initial Human Response. The final Output time cannot be guaranteed and is done on a best-effort basis due to variations in the nature of the reported Issues.

1.13 **"Response Types"** are classified into the following three categories: 1. Automated System Response; 2. Initial Human Response; and 3. Final Output.

1. **"Automated System Response"** refers to an email automatically generated by ESET's ticketing system to confirm that a Ticket has been submitted successfully by the Customer.
2. **"Initial Human Response"** refers to the first reply from an ESET Operator in response to a successfully submitted Ticket. This response type is subject to the guaranteed response times defined in the SLA.
3. **"Final Output"** refers to the final response from the ESET Operator to Issues and/or Requests reported by the Customers. The type of Output varies based on the activities related to different Issue and Request types (e.g., a report, analysis results, or recommendations) and is not labelled as a solution, as finite solutions cannot be guaranteed for all security issue types.

1.14 **"Security Profile"** refers to a document created by ESET as a result of the initial assessment and the information thereby recorded in the Assessment Form. Based on the material stated in the Security Profile, ESET shall create a Service Proposal.

1.15 **"Service Level Agreement"** or **"SLA"** refers to an agreement between ESET and the Customer with a commitment from ESET to the Customer defining the Availability of Security Services and the guaranteed times for the Initial Human Response to correctly reported Tickets.

"Static SLA" refers to the maximum time required for the Initial Human Response to Issues and/or Requests reported by the Customer with the Severity Levels not affecting the time – thus the time in the SLA is static.

"Dynamic SLA" refers to the maximum time required for the Initial Human Response to Issues and/or Requests reported by the Customer with Severity Levels affecting the time – thus the time in the SLA is dynamic.

1.16 **"Severity Levels"** specify the nature and urgency of reported Issues and/or Requests and are applicable to some Issues and/or Requests, as defined in the Table. The Severity Levels also determine the time of the Initial Human Response as defined in the SLA. Severity Levels are classified into the following three different levels: A. Critical; B. Serious; and C. Common. ESET reserves the right to change the Severity Level based on the outcomes of its

initial analysis

A. **"Critical Issues" and "Requests of Critical Nature"** are Issues that have been confirmed to affect business continuity. Common examples of Critical Issues are a live ransomware infection, live incident, false positives that incorrectly block a benign mission or a critical business application, etc. Critical Issues or Requests of critical nature have a guaranteed two-hour SLA for the Initial Human Response.

B. **"Serious Issues" and "Requests of Serious Nature"** are where there is a strong suspicion that business continuity might be affected. Common examples are reporting false positives detected on important files, investigating potentially suspicious behavior, etc. Serious Issues/Requests have a guaranteed three-hour SLA for the Initial Human Response.

C. **"Common Issues" and "Requests of Common Nature"** are of a non-serious nature and do not affect business continuity. Common examples are a retrospective investigation of a historical incident, help with the setup of ESET Enterprise Inspector rules/exclusions, planned detailed malware analysis, etc. This severity includes activities that are planned (e.g., scheduled Threat Hunting) and any Issues and/or Requests that might arise during their delivery. Common Issues and/or Requests of a common nature have a guaranteed four-hour SLA for the Initial Human Response.

1.17 **"Table"** refers to the table set out in Article 1.2 of the Preamble of this Annex No. 2.

1.18 **"Threat Hunting"** refers to the investigation of a certain set of EI Alarms and Events pinpointed by the Customer or a general review of relevant Events and Alarms in case the Customer is suspicious of potential Threats. ESET shall do the following: a) review the highlighted Alarms to determine their root cause; and b) provide actionable advice and compile their findings into Reports. To avoid all doubts, all suggested steps to be conducted outside of EI shall be performed by the Customer.

1.19 **"Threat Monitoring"** refers to a monitoring and advisory service built on top of the EI platform. It guarantees that the Customer's EI console will be checked by ESET once every business day (Monday to Friday). This refers to an overall check of the console—especially triggered Alarms, a further investigation of potential threats, and subsequently, the prioritization of Alarms that require an intervention on the Customer's side. ESET shall do the following: a) compile findings into Reports; and b) reach out to the Customer to alert them of any Critical Events that warrant immediate attention. Any detected anomalies that are pinpointed for further investigation on the Customer's side are addressed by ESET with recommendations on how to proceed in case the anomaly proves to be a real threat. If ESET creates new rules and/or exclusions within EI, they document this in the next Status Report.

1.20 **"Ticket"** refers to an Issue or Request reported by Customers to ESET as part of the ESET Security Services using the reporting procedure prescribed in this Annex.

1.21 **"Threat"** refers to the possibility of a malicious attempt to damage or disrupt the Customer's computer network or system.

2. Description of Security Services.

A. ESET Detection and Response Essential Service.

1.1 The ESET Detection and Response Essential Service is a security support service provided by ESET that consists of the performance of the Activities specified in the Table (for the service hereof) that are performed by the Operator at the Customer´s Request to help resolve the Customer's Issues (covered by the Service hereof in accordance with the Table) by use of Products.

1.2 To use the ESET Detection and Response Essential Service, the Customer has to obtain and have installed in its IT environment at least: (i) ESET end-point Products for its end-point devices and (ii) have those end-point devices managed by the ESET management console product. The service hereof cannot be provided if the Customer has EI installed in its IT environment.

B. ESET Detection and Response Advanced Service.

1.1 The ESET Detection and Response Advanced Service is a security support service provided by ESET that consists of the performance of the Activities specified in the Table (for the service hereof) that are performed by the Operator at the Customer´s Request to help the Customer resolve Issues (covered by the service hereof in accordance with the Table) by use of Products. In addition to all Activities included in ESET Detection and Response Essential Service, this service also includes support in relation to EI and on-demand Threat Hunting.

1.2 To use the ESET Detection and Response Advanced Service, the Customer has to obtain and have installed in its IT environment at least: (i) ESET end-point Products for its end-point devices, (ii) have those end-point devices managed by ESET management console product and (iii) EI.

C. ESET Detection and Response Ultimate Service.

1.1 The ESET Detection and Response Ultimate Service is a security support service provided by ESET that consists of the performance of the Activities specified in the Table (for the service hereof) that are performed by the

Operator at the Customer´s Request to help the Customer resolve the Issues occurring in their IT environment that are defined in the Table (for the service hereof). In addition to all Activities included in the ESET Detection and Response Advanced Service, this service includes pro-active Threat Hunting, Threat Monitoring, and Deployment and Upgrade Activity.

1.2 To use the ESET Detection and Response Ultimate Service, the Customer has to:

- **i.** obtain and have installed in its IT environment at least: (i) EI compatible ESET end-point Products (Endpoint/ File Security/ Mail Security products + Management Agent and EI agents) for its end-point devices, (ii) have those end-point devices managed by ESET management console product ESET PROTECT (Cloud) and (iii) EI. Those Products/components need to be deployed on minimum versions specified by Service professionals. For this purpose, Deployment and Upgrade Activity specified in this Annex shall be performed by ESET, depending on information on Customer´s environment.
- **ii.** As Deployment and Upgrade Activity concerns deployment/upgrade of limited number of Product units by ESET, as specified in the Table above, and as proper deployment of certain Products defined above is a prerequisite to provide the ESET Detection and Response Ultimate Service, Customer is obliged to perform deployment/upgrade of the rest of Products and endpoints within 60 days after ESET´s instruction and provision of deployment/upgrade manual. Failure to perform the required deployment/upgrade by Customer shall be deemed as failure to provide required cooperation and ESET reserved the right to restrict or limit provision of the ESET Detection and Response Ultimate Service until such failure is remedied.
- **iii.** Ensure that hardware and operating system are always in line with hardware requirements and OS requirements of Products/ components;

1.3 When using this ESET Detection and Response Ultimate Service, the Customer shall not change any rules, exclusions, or settings of EI without ESET´s prior approval or knowledge. The breach of this obligation may negatively impact the functioning of the Service and/or EI, and ESET shall not be liable for any damages thereof.

3. Terms for Provision of the Security Services.

1.1 ESET shall start to provide the Security Service from the effectiveness of the Contract.

1.2 The Availability of ESET Security Services shall be 24/7/365 unless specified differently in the applicable Order.

1.3 Response times are based on the SLAs as defined for each Issue/Request type in the Table above.

1.4 Security Services shall be provided for a definite period as stated in the Order.

1.5 To use the Service, the Customer shall be obliged to submit a Request for their provision in accordance with this Annex.

1.6 Critical Issues or Requests of a Critical Nature shall only be reported by the Customer to the designated phone number ("HOT PHONE"). The Customer may only call the HOT PHONE using the contact phone numbers they provided to ESET. No CLIR or other similar function restricting the identification of the calling line may be activated on the Customer's contact phone numbers at the time of reporting Critical Issues or Requests of Critical Nature. If all HOT PHONE lines are busy, the Customer shall leave a message in the voicemail, which is considered a proper way to report Issues or Requests of this Severity Level.

1.7 Serious Issues and Requests of Serious Nature, as well as Common Issues and Issues of Common Nature, shall be reported by the Customer by use of either a dedicated reporting form or a HELPDESK phone line. The reporting of an Issue or a Request with this Severity Level shall be taken to mean the following:

a. When using a dedicated reporting form: The proper completion of all data and confirmations required by the form, and the subsequent receipt from ESET of an automatically generated email message confirming that the Issue or Request was successfully reported.
b. When using the HELPDESK phone line number: The provision of all information required by the Operator, and the subsequent receipt from ESET of an automatically generated email message confirming that the Issue or Request was successfully reported.
c. A confirmation email message shall be sent to the Customer's email contact address stated in the form. If a confirmation email message is not received by the Customer within ten (10) minutes after attempting to report an Issue or a Request, the Customer shall proceed according to Section 1.6 hereto.

1.8 All contact details for reporting any Issues or Requests (e.g., HOT PHONE, HELPDESK phone line, link to a dedicated reporting form) shall be specified in a separate document, which shall be provided to the Customer by the ESET Partner before ESET starts to provide any of the Security Services.

1.9 If, when reporting an Issue or a Request, the Customer provides inaccurate or incomplete information, the Operator shall demand that the information is completed or corrected; in the meantime, no period or solution time shall be running under the Terms.

1.10 An Issue shall be considered resolved when any of the following occurs:

a. ESET provides the Customer with the Output defined in the Table for the respective Issue via email.
b. Upon the expiration of 24 hours after sending the second notice demanding the required cooperation.

1.11 Provision of the Security Services shall be possible under the condition that the Customer has purchased the relevant Security Service for all end-points protected by ESET Products. Provided that the Customer increases the number of end-points protected by ESET Products during the provision of the Security Service, they are also

obliged to enlarge the Security Service to the extent corresponding to the increase in number of end-points protected by ESET Products.

Supplement A – Data Processing Agreement (the "Agreement").

1. According to the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (the "**GDPR**") as well as data protection laws applicable in United Kingdom of Great Britain and Northern Ireland, ESET (the "**Processor**"), and the Customer (the "**Controller**") are entering into a data processing contractual relationship to define the terms and conditions for the processing of personal data, the manner of its protection, and to define other rights and obligations of both parties in relation to the processing of personal data of data subjects on behalf of the Controller during the course of performing the subject matter of the Terms as the main contract.

2. **Personal Data.** To provide the Services in compliance with the Terms, it may be necessary for the Processor to process information relating to an identified or identifiable natural person (the "**Personal Data**") on behalf of the Controller.

3. **Authorization.** The Controller thereby authorizes the Processor to process Personal Data under the following conditions:

   3.1 the "**purpose of processing**" shall mean provision of Services in compliance with the Terms.

   3.2 the "**processing period**" shall mean period from the conclusion of the Contract under the Terms until its termination or expiry.

   3.3 the "**scope and categories of Personal Data**" includes any Personal Data provided or made available by the Controller during the provision of Services, in particular any Personal Data submitted in Service requests or during the process of dealing with any Service requests, or any Personal Data that may be accessible or available to the Processor in case temporary or permanent access was granted by the Controller to their Products or devices over the course of the performance of Services.

   3.4 the "**Data Subject**" refers to any natural persons who are authorized users of the Controller's devices and/or employees or contractors of the Controller, and if applicable, of its affiliated entities, as well as any persons whose data may be provided or made available by the Controller to the Processor over the course of the performance of Services.

   3.5 the "**processing operations**" means every operation necessary for the purpose of processing.

   3.6 the "**documented Instructions**" shall mean instructions described in the Terms, its Annexes, Service documentation, or in requests for provision of the Service.

4. **Obligations of Processor.** The Processor shall be obliged to do the following:

   4.1 Process Personal Data for the purpose of providing the Services in compliance with the Terms and only on the grounds of documented Instructions, including with regard to transfers of Personal Data to a third country, unless required to do so by EU or member state law or UK law; in such cases, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

   4.2 Ensure that persons authorized to process the Personal Data have committed themselves to confidentiality.

   4.3 Take all measures related to the security of processing as required pursuant to Art. 32 of GDPR, taking into account the state of the art, 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, to ensure a level of security when processing of the Controller´s Personal Data that is appropriate to the risk.

   4.4 Taking into account the nature of processing, assist the Controller by appropriate technical and organizational measures, insofar as it is possible, for the fulfilment of the Controller´s obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of GDPR.

   4.5 Upon request, provide reasonable assistance to the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, taking into account the nature of processing and information available to the Processor.

   4.6 At the choice of Controller, delete or return all the Personal Data processed on behalf of the Controller within 30 (thirty) business days after the end of the provision of Services relating to processing, and delete existing copies unless EU law or EU member state law requires storage of those Personal Data.

   4.7 Keep an up-to-date register of all the categories of processing activities that it has carried out on behalf of Controller.

   4.8 Make available to the Controller all information necessary to demonstrate compliance as part of the Terms, its Annexes, and Services documentation, and if strictly necessary, allow for audits conducted by the Controller or

another auditor mandated by the controller in relation to processing conducted within the scope of this Agreement.

5. **Engaging Another Processor.** The Processor is generally entitled to engage another processor (the "**Subprocessor**") to carry out specific processing activities in compliance with the Terms, mainly this agreement and the Services documentation. The Processor shall ensure that any such Subprocessor will be bound by the same obligations as set out in this agreement. Even in this case, the Processor shall remain fully liable to the Controller for the processing of any Personal Data by the Subprocessor. For the purpose of performance of Services, the Processor engages the Distributor as its Subprocessor. The Subprocessor is obliged to inform the Controller of any intended changes concerning the addition or replacement of other Subprocessors, thereby giving the Controller the opportunity to object to such changes. Any objections to a new subprocessor shall be received within seven (7) business days after notification, otherwise the new Subprocessor shall be deemed accepted by the Controller. If the Controller reasonably objects to a new Subprocessor, and the objection cannot be satisfactorily resolved within a reasonable time, the Customer may terminate this Agreement without penalty upon 30 (thirty) days' written notice to the Processor. If the Controller´s objection remains unresolved 30 (thirty) days after it was raised and no notice of termination has been received, the Controller is deemed to accept the new Subprocessor.

6. **Territory of Processing.** The Processor will do its best to ensure that processing takes place in the European Economic Area or a country designated as safe by the decision of the European Commission based on the decision of the Controller. Standard Contractual Clauses (available here: https://www.eset.com/fileadmin/ESET/INT/Docs/no-index/Standard-Contractual-Clauses.pdf) shall apply in the case of transfers and processing of Personal Data located outside of the European Economic Area or a country designated as safe by the decision of the European Commission.

7. **Security.** The Processor is ISO 27001:2013 certified and uses the ISO 27001 framework to implement a layered defense security strategy when applying security controls on the layers of network, operating systems, databases, applications, personnel, and operating processes. Compliance with the regulatory and contractual requirements is regularly assessed and reviewed similarly to other infrastructure and processes of the Processor, and necessary steps are taken to provide compliance on a continuous basis. The Processor has organized the security of the data using ISMS based on ISO 27001. The security documentation mainly includes policy documents for information security, physical security, and the security of equipment, incident management, handling of data leaks, security incidents, etc.

8. **Processor's Contact Information.** All notifications, requests, demands, and other communication concerning personal data protection shall be addressed to ESET, spol. s r.o., attention of: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.