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

Effective date: October 20th, 2023

(other language versions can be found at the end of this document)

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 the Municipal Court Bratislava III, Section Sro, Insertion No. 3586/B (the "**ESET**").

Customer: A legal person who accepted these Terms via execution of the Terms & Conditions for the Provision of Professional and Security Services Acceptance Form and is entitled to order the Services through the ESET Partner (the "**Customer**").

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

BACKGROUND:

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.

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

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 *"Acceptance Form"* refers to a document by which the Customer has accepted the Terms for the purpose of Services provision from ESET.

1.2 *"Affiliates"* refers to entities that are controlled by, controlling or under common control with the Party.

1.3 *"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.

1.4 *"Confidential Information"* refers to any non-public information and data, whether disclosed in written, oral, electronic, website-based, or in other form and without the need of their explicit identification as confidential by the disclosing Party.

1.5 *"Distributor"* refers to ESET affiliate or partner distributing the Services on a certain territory, defined as "Distributor" in the Acceptance Form.

1.6 *"ESET Partner"* refers to the Distributor or its partner (reseller) from whom the Services are ordered by the Customer and who supplies them to the Customer.

1.7 *"Force Majeure Event"* refers to an intervention of a public enemy, acts of war, civil unrest, riots, demonstrations, fire, flood, earthquake, a 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.

1.8 *"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.

1.9 *"Order"* refers to an order for the provision of any of the Services placed by the Distributor based on a Service Proposal (if applicable).

1.10 *"Order Acceptance"* refers to the email confirmation sent by ESET to the Customer after ESET has accepted the Order.

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

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

1.13 *"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.

1.14 *"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 specific Service.

1.15 *"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.

1.16 *"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 of 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.

2.3 The Customer has accepted the Terms by executing the Acceptance Form and agreed to be bound by them to the full extent in case of ordering any of the Services via ESET Partner.

2.4 The Services provision shall be ordered by placing the Order into the ESET system by the Distributor. The Order shall contain (i) the ordered Service, (ii) the Customer, (iii) the Service price, (iv) the number of units of purchased Service and (v) the expiration date that will determine the duration of the ordered Service. Any other data or conditions stated in the Order are not binding for ESET, unless they are specifically agreed between the Parties. Once ESET accepts the Order via Order Acceptance, ESET shall be obliged to provide the Services to the Customer pursuant to the Terms.

3. Provision of the Services.

3.1 The Services and their scope are 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.

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

3.3 Unless otherwise stated in the respective Annex, the date of the Order Acceptance shall be deemed as the start date of the Services provision. The specific activities of the Services shall be performed based on the Customer´s request as stipulated in the applicable Annex. The 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 use if the contractor were being selected 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 the 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 agreed otherwise. Noncompliance with this obligation shall be deemed as 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 a 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 be held liable therefor.

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 a 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) The 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 is required to upgrade to the latest available version of the Product if an earlier version of the Product limits proper Services delivery or provides lower level of security protection.

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 fulfil 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 with all the available information, documents, equipment and assistance that are necessary to fulfil the obligations of ESET according to the Terms. 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 placing a modified Order to ESET via ESET Partner. Provisions of Article 2 shall apply accordingly to the 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 Order Acceptance related to the modified Order will be delivered to the Customer 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 shall direct all communication in relation to the provision of the Services, mainly any complaints, requests, refunds etc. to the ESET Partner. Other legal communication related to the Terms, mainly the communication relating to the termination of the Terms shall address to ESET on the e-mail address: services@eset.com.

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 any Third Party.

6.2 The license under the previous sentence is granted for the time of duration of ESET's intellectual property rights to the 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 ESET, 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 Terms if the performance of their duties is delayed or prevented by the 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 about the Force Majeure Event in writing. The Party notifying the other Party about 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 terminate the Services provision. The provisions of the sec. 11.10 shall apply accordingly.

10. Confidential Information Protection.

10.1 The Parties acknowledge a duty not to disclose the Confidential Information provided by one Party during or after the term of the Services provisions under the Terms without the Party's prior written permission.

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.

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, Specialists, and contractors on a strict "need-to-know" basis to carry out the purpose stated in the sec. 10.3 and that such Affiliates, officers, employees, Specialists, and contractors are informed of their confidential nature and bound by obligations set out herein. Notwithstanding the provisions of this Article, either Party may disclose Confidential Information to the extent it is necessary to comply 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 Terms, the provisions of this Article 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.

11.1 **Term.** The Terms shall become effective at the date of the execution of the Acceptance Form by the Customer and shall remain effective through the whole term of the provision of Services. The Terms shall terminate automatically in case:

a) there is no valid Order for Services provision in place AND

b) there has been no Order for Services provision placed for the period of six (6) months following the termination of the last active Services provision.

11.2 **Terms Termination.** Either Party shall have a right to terminate the Terms in case the other Party commits a substantial/material breach of the Terms and the breach remains unremedied for more than thirty (30) days after written notice of the breach is delivered to the other 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 thirty (30) days period, then the breaching Party will have an additional thirty (30) days to

complete a remedy. In such cases, the other Party may terminate the Terms only if the failure continues unremedied after the passing of the additional thirty (30) days period.

11.3 The Customer is entitled to terminate the Terms due to a change in the Terms in accordance with sec. 12.6 of the Terms.

11.4 The Parties are entitled to terminate the Terms 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.

11.5 In case of Termination of Terms notwithstanding the reason, ESET shall cease to provide the Services to the Customer and the Customer will not be entitled for the Services provision as well as to order any other Services via ESET Partner.

11.6 The Customer is entitled (not obliged) to terminate the Terms by using the Termination Form attached to the Terms in the annex no. 3.

11.7 **Termination of the Services provision**. ESET shall have a right to immediately terminate the Services provision, fully or partially, if ESET becomes unable to provide the Services to the Customer. Moreover, ESET shall have the right to cancel the Order placed in accordance with sec. 2.4 of the Terms within five (5) business days after its acceptance; thus the Services provision will not commence.

11.8 In case the Customer terminates the Data Processing Agreement in Supplement A in accordance with its Art. 4, the related Services provision shall be terminated as well.

11.9 The Parties shall have a right to terminate the Services provision in case the other Party commits a substantial/material breach of the Terms relating to the specific Services provision, mainly the conditions stated in the annexes of the Terms and the breach remains unremedied for more than thirty (30) days after a notice of the breach is delivered to the Party via Distributor. 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 thirty (30) days period, then the breaching Party will have an additional thirty (30) days to complete a remedy. In such cases, the other Party may terminate the Services provision only if the failure continues unremedied after the passing of the additional thirty (30) days period.

11.10 In case of the termination of the Services provision,

a) the Customer shall notify the ESET Partner who shall secure the cancellation the applicable Order in the ESET system and

b) ESET shall inform the Distributor by cancelling the applicable Order directly and notify the Customer via email about the termination of the specific Service provision.

11.11 **Refund**. In case of termination of the Services provision due to (i) ESET´s uncured breach; (ii) change of the Terms (iii) cancellation of the Order within five (5) business days after its acceptance; (iv) termination of the Services provision for the inability of ESET to provide Services or (v) termination of the Data Processing Agreement in Supplement A in accordance with its Art. 5, the Customer shall have the right for refund. As the financial matters have been settled via ESET Partner, the Customer shall claim the refund from the ESET Partner as well. This provision shall not affect any other provisions relating to refunds that the Customer has agreed with the ESET Partner separately. The refund shall be in the amount of paid Service fees for the period from the date of the termination email (sec. 11.10b) to the end of the Services subscription period specified in the Order. In case of termination due to the situation described in letter (iii), the refund shall be in the amount of the whole paid Service fees.

11.12 Any termination of the Services provision will not waive or otherwise adversely affect any other rights or remedies the terminating Party may have under the Terms, unless otherwise stated in the Terms. Upon termination or expiry of this Terms, all rights and duties of the Parties will be terminated, with the exception of those 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 **Interim provisions**. The provisions of the Terms shall apply to all active relationships between the Customer and ESET concluded in compliance with the Terms and Conditions for the Provision of Professional and Security Services valid as of 12.04.2023 (the „**Previous Terms**“) and older as well. All services ordered as well as all

conditions stated in the orders according to the Previous Terms shall remain valid. The provisions of the current Terms shall apply to these orders accordingly.

12.2 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.

12.3 The Terms constitutes 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.

12.4 In the event of any conflict between the Terms and the Annexes to the Terms, the respective Annex shall prevail.

12.5 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.

12.6 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 the Services. In such cases, ESET is obliged to notify the Customer by email (sent to the email address stated in the Acceptance Form or announced to ESET later) and publish it on a dedicated website. If the change relates to substantial or material provisions of the Terms (e.g. new obligations or prerequisites for the Customer, change of the conditions to terminate the Terms or Services provision, change of jurisdiction, etc.) the Customer has a right to terminate the Terms within thirty (30) days after receiving of notice of the change. This right shall not apply if the change of the Terms will relate to the description of the services not ordered by the Customer or the amendment of a new service into the annexes. 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 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 the Customer's failure to receive the updated Terms due to failure to update the Customer's contact details with ESET.

12.7 The Terms shall be interpreted and governed under the following laws:

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

b) If the Distributor of the Services is ESET, LLC. or ESET Canada Inc., then the laws of the 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 Distributor of the Services is Canon Marketing Japan, Inc., then the laws of Japan apply without giving effect to the conflicts of law provisions; and

d) If none of the previous points applies, then the laws of the 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 Terms.

12.8 Any dispute or disagreement arising out of or in connection with the Terms, including any violation, termination, cancellation or invalidity of the Terms (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 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 thirty (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 one (1) million EUR or smaller, and by three (3) 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 12.7 of the Terms and the place of arbitration shall be:

a) ICC Japan in Tokyo in case the Distributor of the Services is Canon Marketing Japan, Inc.,

b) ICC United States in New York in case the Distributor of the Services is ESET, LLC. or ESET Canada Inc.,

c) ICC United Kingdom in London in case the Distributor of the Services is ESET SOFTWARE UK LIMITED, and

d) ICC Austria in Vienna in any other case then mentioned above.

12.9 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, each Party may assign the Terms as part of a corporate reorganization, consolidation, merger, or sale of substantially all its assets or capital stock.

12.10 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.

12.11 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.

Annexes:

Annex no. 1 – Specification of ESET Professional Services.

Annex no. 2 – Specification of ESET Security Services.

Annex no. 3 – Termination Form

Annex no. 1. – Specification of ESET Professional Services

PREAMBLE.

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

1. 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 the delivered activity fully complies with the requirements agreed in the Acceptance Protocol or in the S&R Document. The standard Acceptance Procedure period is fourteen (14) days from the activity completion date (date, when the Acceptance Protocol or the S&R Document has been sent to the Customer) unless otherwise agreed between the Parties.

1.2 "**Acceptance Protocol**" shall mean a written protocol confirming the acceptance of the Service Output(s) by the Customer, where applicable.

1.3 **"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).

1.4 **"Deployment 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.

1.5 **"Error"** refers to such Product functionality that is inconsistent with the description of the Product functionalities contained in the documentation related to the Product. 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.

1.6 **"HealthCheck 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.

1.7 **"HealthCheck Plan"** refers to a document created by ESET based on the information recorded in the Assessment Form, which describes specific 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).

1.8 **"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 related to the Product.

1.9 **"Premium Support 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.

1.10 **"Reproducible Test Case"** refers to a test code that demonstrates the portion customarily not exceeding one hundred (100) lines, or in a text format, a specific syntax, on a small portion of the code or case in which an Error occurs. A Reproducible Test Case must demonstrate inconsistency between a Product and its documentation.

1.11 **"Request"** refers to requesting any activity included in the Service or submitting any Services Support Case by the Customer.

1.12 **"Severity Levels"** refers to the fact that Errors are classified into A (critical), B (Serious), and C (Common) Severity Levels.

a) **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.

b) **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.

c) **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.

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

1.14 **"Suggestions & Recommendations Document"** or **"S&R Document"** refers to an activity output. It is a document created by ESET that summarizes the findings and 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).

1.15 **"Services Support Case" or "SSC"** refers to the Error being reported and submitted by the Customer, the Error being solved/ being handled by the Specialist, and finally, a confirmation by the Specialist that the Error is fixed.

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

1.17 **"Upgrade 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.

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

A. ESET Premium Support Advanced Service.

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 The ESET Premium Support Advanced Service shall be provided 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 used Product licenses (excluding a renewal), including when the increasement of the number of seats during the provision of ESET Premium Support Advanced Service, the Customer is also obliged to modify the ESET Premium Support Advanced Service to reflect this change. For the avoidance of any doubts, such modification is subject to an additional fee.

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

2.1 To use the ESET Premium Support Advanced Service, the Customer shall be obliged to submit a Request for its provision in accordance with this Annex.

2.2 The Customer is entitled to request either one Deployment Activity or one Upgrade Activity in each one (1) 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 thirty (30) days from the submission of the Customer´s Request.

a) The Deployment Activity consists of one (1) Deployment Activity delivery. One (1) Deployment Activity delivery accounts for the deployment of one hundred (100) units of purchased Products into the 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 deploy the rest of the Products in its infrastructure as well as the required installation packages. ESET shall inform the Customer in the Service Proposal if more than one (1) Deployment Activity delivery is suggested by ESET. Within one (1) Deployment Activity delivery, the ESET Specialist deploys the corresponding number of Product(s) to the corresponding number of seats

and provides 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 (1) activity delivery. One Upgrade Activity delivery accounts for upgrade of one hundred (100) units of Products in the 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 the Products in its infrastructure as well as the required installation packages. ESET shall inform the Customer in the Service Proposal if more than one (1) Upgrade Activity delivery is suggested by ESET. Within one (1) Upgrade Activity delivery, the ESET Specialist upgrades the corresponding number of Product(s) for the corresponding number of seats and provides 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.

2.3 A HealthCheck Activity would ideally be executed later in the Product license's lifecycle (e.g., after three (3) 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 (1) activity delivery, which accounts for a maximum of one (1) Man-Day, including time spent preparing an S&R Document. If more than one (1) activity delivery is suggested by ESET, the Customer will be informed within the Assessment form. The Customer is entitled to request one (1) HealthCheck Activity in each one (1) 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 twenty-one (21) days prior to the desired commencement of the provision of the HealthCheck Activity and no later than twenty-one (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 twenty-one (21) days from the submission of the Customer´s Request unless stated otherwise in the Service Proposal.

2.4 The Premium Support Activity shall be provided continuously after the Order Acceptance.

3. Performance of the Deployment and Upgrade Activity.

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

3.2 The Customer empowers ESET to express its consent to the terms and conditions of End User License Agreement as the Customer´s representative.

3.3 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 and upload it to the original Request submitted via the services support request form. In case the uploading is not available or will fail, the Customer may send the signed version of the Acceptance Protocol via email to the ESET Partner. If any part of the 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 ESET on an additional period for delivery of the undelivered part of the activity. If the Parties do not agree on a period for the elimination of defects, the period for the elimination of defects is thirty (30) days.

b) If the Customer unreasonably refuses to confirm the delivery of any activity or neither confirms the Acceptance Protocol nor mentions any undelivered part of the Deployment and Upgrade Activity during the Acceptance Procedure period, such activity shall be deemed accepted and delivered without reservation.

4. Performance of the HealthCheck Activity.

4.1 The activity may be done by remote access or on Site.

4.2 Provision of the activity shall be completed when the Customer confirms the acceptance of the S&R Document by its signature and upload it to the original Request submitted via services support request form. In case the uploading is not available or will fail, the Customer may send the signed version of the S&R Document via email to the ESET Partner. If any part of the activity stated in the HealthCheck Plan remains undelivered, the Customer shall mention this fact in the S&R Document and agree with the ESET on an additional period for the delivery of the undelivered part of the 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 its signature and either send it to the email address of ESET or by uploading it to the original Request submitted via the services support request form. If the Customer unreasonably refuses to confirm the S&R Document, even after the ESET declares that the

S&R Document is in full accordance with HealthCheck Plan or neither confirms the S&R Document nor mentions any undelivered part of the activity during the Acceptance Procedure period, the activity delivery shall be deemed accepted and delivered without reservation.

5. Performance of the Premium Support Activity.

5.1 **Request Submission.** When submitting a Request, the Customer shall provide the necessary information as required by the form or the Specialist. For the purposes hereof, such necessary information includes but is not limited to:

a) License data, such as public license ID;

b) Information on the Customer's contact person, such as the name, surname, job position, contact phone number and email address;

c) Detailed description of the Error so that Error replication and/or Reproducible Test Case is possible;

d) Technical data on computer systems and on installed programs according to the Specialist's requirements;

5.2 The Customer shall provide the following cooperation:

a) In order to enable handling the Request, the Customer shall provide remote access, grant the rights required to carry out a remote intervention and secure the presence and assistance of the Customer's qualified staff in the case of an intervention being carried out on the Customer's premises.

b) If the Customer provides inaccurate or incomplete information, the Specialist shall demand that the information to be completed or corrected; in the meantime, no period or solution time shall be running under the Terms.

5.3 If the Customer does not provide the required cooperation and assistance, the Specialist may close a specific Services Support Case upon the expiration of twenty-four (24) hours after sending the second notice demanding cooperation to the contact email address stated in the submitted SSC.

5.4 If, when reporting an Error, the Customer does not follow the procedure laid down herein, this shall be regarded as failure to provide cooperation.

5.5 All Requests shall be submitted by the Customer on either a services support request form or a HELPDESK phone line. 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 Request. If all HELPDESK lines are busy, the Customer shall leave a message in the voicemail, which is considered as proper Request submission.

5.6 The submitted Request shall be taken to be confirmed as follows:

a) When using a Services 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 Specialist, and the subsequent receipt from ESET of an automatically generated email message confirming that the Request was successfully submitted.

If the confirmation email message is not received by the Customer within ten (10) minutes after attempting to submit the Request, the Customer shall call the HELPDESK or use escalation contacts.

5.7 Services support request form, HELPDESK phone line and escalation contacts are specified in the Order Acceptance sent to the Customer.

5.8 **Handling of Requests.** All Services Support Cases shall be handled and the Error shall be considered fixed when any of the following occurs:

a) The Customer confirms via email to the Specialist that the solution proposed for the given Services Support Case is efficient.

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

c) Upon the expiration of twenty-four (24) hours after sending the second notice demanding cooperation pursuant to sec. 5.3 hereof.

5.9 Requests related to the HealthCheck or Deployment/Upgrade Activities shall be handled by the performance of the related activity and in accordance with conditions prescribed in sec. 3 and 4 of this Annex.

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

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

5.12 **Guaranteed Parameters.** The complexity of the Product and specific circumstances, such as the Customer's hardware or third-party software prevents specification of fixed solution times for SSCs, as such times and their lengths depend on the nature and complexity of an Error. ESET, however, shall use its best efforts to solve SSCs 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:	
Error severity A:	max. 2 hours
Error severity B:	max. 4 hours
Error severity C:	max. 24 hours
Technical support availability	24/7/365
Solution time	best effort

5.13 **Number of Services Support Cases.** The Number of Services Support Cases eligible for the Service is not limited. To avoid any doubt sec. 4.5 of the Terms shall not be affected.

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

5.15 **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.

5.16 **Account Manager.** The account manager shall be dedicated to being attentive to the Customer´s needs during the provision of the Service. The account manager 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. Description of the 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 Art. 3 of Annex no. 1, while the term "Activity" shall be replaced with the term "Service."

1.2 The ESET Deployment and Upgrade Service consists of one (1) Deployment and Upgrade Service Delivery. One (1) Deployment and Upgrade Service delivery accounts for a maximum of one (1) Man-Day, and the Customer is entitled to request either a Deployment Service or the Upgrade Service within one (1) Deployment and Upgrade Service Delivery. This time includes the time spent preparing the Service Proposal. ESET shall inform the Customer in the Service Proposal if more than one (1) Deployment and Upgrade Service Delivery is suggested by ESET.

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

C. ESET HealthCheck Service.

1. Description of the ESET HealthCheck Service.

1.1 The ESET HealthCheck Service is the same Service as the HealthCheck Activity described in Art. 4 of Annex no. 1, while the term “Activity” shall be replaced with the term “Service.”

1.2 The ESET HealthCheck Service consists of one (1) HealthCheck Service Delivery. One (1) HealthCheck Service delivery accounts for a maximum of one (1) Man-Day, and this time includes the time spent preparing an S&R Document. ESET shall inform the Customer in the Service Proposal if more than one (1) HealthCheck Service Delivery is suggested by ESET.

1.3 ESET shall provide the ESET HealthCheck Service within twenty one (21) days from the submission of the Customer´s Request unless stated otherwise in the HealthCheck Plan.

D. ESET Premium Support Essential Service

1. Description of the ESET Premium Support Essential Service.

1.1 ESET Premium Support Essential Service is the same Service as the Premium Support Activity described in Art. 5 of Annex no. 1 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 used Product licenses (excluding a renewal), including the increasement of the number of seats during the provision of ESET Premium Support Essential Service, the Customer is also obliged to modify the ESET Premium Support Essential Service to reflect this change. For the avoidance of any doubts, such modification is subject to an additional fee.

1.3 If the resolution of a specific Services 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 SSCs. The Customer shall be proposed to purchase this additional service; however, the final decision has to be made by the Customer.

1.4 ESET shall start to provide the ESET Premium Support Essential Service after the Order Acceptance 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 forensics, 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.

d) ESET MDR Service

1.3 Each ESET Security Service consists of the specific features as described below:

Feature \ Service	ESET Detection and Response Essential	ESET Detection and Response Advanced
Digital forensic incident response (DFIR) assistance	✓	✓
Malware detection support	✓	✓
Malware file expert analysis	✓	✓
Customized Threat Hunting for all current threats	–	✓
Customized rules and exclusions optimization		✓
Automatic rules and exclusions optimization	–	–
Continual expert-led threat hunting	–	–
24/7 expert-led continuous monitoring, hunting triage and response	–	–
Deployment & Upgrade	–	–
Expert assistance for MDR alerts with more context	–	–

Table 1: Overview of specific features for reactive Services (triggered upon Requests)

Feature \ Service	ESET MDR	ESET Detection and Response Ultimate
Automatic rules and exclusions optimization	✓	–
Continual expert-led threat hunting	✓	✓
24/7 expert-led continuous monitoring, hunting triage and response	✓	✓
Customized Threat Hunting for all current threats	–	✓
Customized rules and exclusions optimization	–	✓
Digital forensic incident response (DFIR) assistance	–	✓
Malware detection support	–	✓
Malware file expert analysis	–	✓
Deployment & Upgrade	–	✓
Expert assistance for MDR alerts with more context	–	✓

Table 2: Overview of specific features for proactive Services (managed)

1.4 Table A below contains the description of features that are provided by ESET at Request. For each feature there is stated the description of the Issue/ Request types, activities performed by ESET, required inputs from the Customer and resulting Outputs.

Table A – Features at Request

Feature	Issue / Request type	ESET activity description	Required inputs and resulting Outputs
Digital forensic incident response (DFIR) assistance	Digital forensic incident response assistance / DFIR assistance, i.e. an incident needs to be investigated, it's an ongoing incident, and 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 a 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.
Malware detection support	Malware: missing detection, i.e. Malware is not detected.	The 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 provided; otherwise, a clean status is confirmed.

	Malware: cleaning problem, i.e. 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 the environment. Output: if cleaning is improved, information about the planned fix is provided; standalone cleaner application/procedure if applicable.
	Malware: ransomware infection, i.e. The 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 Output: decryptor (if possible); otherwise, basic mitigation and prevention hints.
	False positive, i.e. 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.
	General: Suspicious behavior investigation	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.
Malware file expert analysis	Basic file analysis, i.e. 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.
	Detailed file analysis, i.e. 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.

Customized Threat Hunting for all current threats	EI: Threat Hunting	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.
Customized rules and exclusions optimization	EI: rules support, i.e. 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
	EI: exclusions support, i.e. 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.
	EI: Initial Optimization	After the installation of EI to a new environment, EI generates a 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
Deployment & Upgrade	Deployment and 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, Section 6.2 (as agreed with the Customer). Deployment & Upgrade will be carried out by ESET by deploying/ upgrading of 100 units of Products/ components. Information on how to finish	Input: Assessment form, access to the environment Output: Product deployed or upgraded.

		these deployments and upgrades is shared with Customers.	
Expert assistance for MDR alerts with more context	EI: general security related question.	Security expert's guidance and all-around help at disposal for the customer	Input: depends on type and content of Request Output: depends on type and content of Request

1.5 Table B below contains the description of features that are provided by ESET proactively. For each feature there is stated the description of the activities performed by ESET, required inputs from the Customer and resulting Outputs.

Table B: Features provided proactively

Feature	ESET activity description	Required inputs and resulting Outputs
Automatic rules and exclusions optimization	Rule sets and exclusions optimization based on signals from customer's environment.	Input: access to the environment Output: optimized environment
Continual expert-led threat hunting	EI: Threat Hunting (pro-active) Constant threat hunting, where security experts evaluate and correlate detection into a structured and mapped incident.	Input: access to the environment Output: Incidents generated in EI (with response where possible)
24/7 expert-led continuous monitoring, hunting triage and response	EI: Threat Monitoring. A 24/7 human-led service, which leverage IoC, IoA, UEBA, AI, comprehensive internal and external TI feeds and similar sophisticated monitoring and detection technics to protect customers' environment. This feature will unveil and unhide malicious activity and perform containment and eradication action to prevent severe damages.	Input: access to the environment Output: Incidents generated in EI (with a response where possible)

2. Definitions.

2.1 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.

2.2 **"Availability"** refers to the time during which ESET and its subcontractors are available to provide Services to Customers and respond within the SLA.

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

2.4 **"Detection (in EI v1.4 or newer)"** 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 are written to identify suspicious malicious behavior triggering Detection with defined severities. Each triggered Detection is displayed in the Detection section with a clear identification of where it happened (computer), and which executable and process

have triggered it. It is accompanied by the severity information, as defined in the rules mentioned above, and a priority can be assigned to each Detection.

2.5 **"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 Connectors that are deployed on the endpoints within the Customer's infrastructure. These Events are analyzed by Specialists as part of the Threat Hunting and Threat Monitoring activities.

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

2.7 **"EI Connector" (EI Agent for v1.6 and earlier)** 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 Connector requires the ESET security Product to be installed before deployment. The EI Connector needs its own license to work properly and send Events to the EI server. The EI Connector 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.

2.8 **"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 A.

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

2.10 **"Request"** refers to any request in relation to the security of their environment and Products deployed within, where the request is not a Product error report, including any Issue reported by the Customer to ESET. To avoid any doubt, Requests relate to (but are not limited to) filling incident analyses, response and mitigation, Threat hunting and EI security-related topics (not product errors), such as rule and exclusion (internal functionalities), and support and optimization.

2.11 **"Response Times"** refer to maximum times that are guaranteed for the Initial Human Response.

2.12 **"Response Types"** refer to the classification of the responses to the Request into the following three categories: 1. Automated System Response; 2. Initial Human Response; and 3. Final Output.

a) **"Automated System Response"** refers to an email automatically generated by ESET's ticketing system to confirm that a Request has been submitted successfully by the Customer.

b) **"Initial Human Response"** refers to the first reply from an ESET Specialist in response to a successfully submitted Request. This response type is subject to the guaranteed response times defined in the SLA.

c) **"Final Output"** refers to the final response from the ESET Specialist to the submitted Request. The type of the Final 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. 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.

2.13 **"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.

2.14 **"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 maximum guaranteed times for the Initial Human Response to correctly submitted Request.

2.15 **"Severity Levels"** refer to the specification of the nature and urgency of submitted Request . 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) **"Requests of Critical Nature"** refer to the Requests that have been confirmed to affect business continuity. Common examples of Requests of Critical Nature are a live ransomware infection, live incident, false positives that incorrectly block a benign mission or a critical business application, etc.

b) **"Requests of Serious Nature"** refer to Requests with a strong suspicion that business continuity might be affected. Common examples are reporting false positives detected on important files, investigating potentially suspicious behavior, etc.

c) **"Requests of Common Nature"** refer to Requests 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

Level includes activities that are planned (e.g., scheduled Threat Hunting) and any Requests that might arise during their delivery.

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

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

3. Terms for Provision of the Security Services.

3.1 ESET shall start to provide the Security Service after the Order Acceptance and for a definite period as stated in the Order Acceptance.

3.2 The Services described in the table A shall be provided based on the Request of the Customer. When submitting the Request, the Customer shall provide all information required by the form or the Specialist, such as:

a) License data, such as public license ID;

b) Information on the Customer's contact person(s), such as their name, surname, job position, contact phone number and Functional email contact address;

c) detailed description of the Issue so that Issue replication is possible.

3.3 If, when submitting a Request, the Customer provides inaccurate or incomplete information, the Specialist shall demand the information to be completed or corrected; in the meantime, no period or solution time shall be running under the Terms.

3.4 All Requests shall be submitted by the Customer on either a services support request form or a HELPDESK phone line. 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 Request. If all HELPDESK lines are busy, the Customer shall leave a message in the voicemail, which is considered as a proper Request submission.

3.5 Submission of the Request shall be taken to mean the following:

a) When using a dedicated 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 Specialist, and the subsequent receipt from ESET of an automatically generated email message confirming that the Request was successfully submitted.

3.6 If a confirmation email message is not received by the Customer within ten (10) minutes after attempting to submit the Request, the Customer shall call the HELPDESK or use escalation contacts.

3.7 Services support request form, HELPDESK phone line and escalation contacts are specified in the Order Acceptance sent to the Customer.

3.8 The Request shall be considered resolved when any of the following occurs:

a) ESET provides the Customer with the Output defined in the Table A for the respective Issue / Request type via email.

b) Upon the expiration of twenty-four (24) hours after sending the second notice demanding the required cooperation.

3.9 Provision of the Security Services shall be possible under the condition that the Customer has purchased the relevant Security Service for an adequate number of seats as calculated by the ESET Partner. Provided that the Customer modifies the Product licenses they use (excluding a renewal), including when they increase the number of seats during the provision of the Security Service, they are also obliged to modify the Security Service to reflect this change. For the avoidance of any doubts, such modification is subject to an additional fee.

4. SLA

4.1 The Availability of ESET Security Services shall be 24/7/365 .

4.2 Response times for the Initial Human Response to correctly submitted Request depend on the type of Severity level as follows:

a) Requests of Critical Nature have a guaranteed two-hour (2h) SLA for the Initial Human Response.

b) Requests of Serious Nature have a guaranteed four-hour (4h) SLA for the Initial Human Response.

c) Requests of a Common Nature have a guaranteed twenty-four-hour (24h) SLA for the Initial Human Response.

4.3 The Response times as stated above shall not apply

a) to the features described in the Table B because the ESET activity is continuous and

b) to the specific features from the Table A because the ESET activity is planned and performed in the agreed timeframe. The features from the table A are the following: EI: Initial Optimization and Deployment and Upgrade.

5. Description of ESET Detection and Response Essential Service.

5.1 The ESET Detection and Response Essential Service is a security support service provided by ESET that consists of the features as defined in the sec. 1.3 of annex no. 2. Table A contains for each feature the description of the Issue/ Request types, the activities performed by ESET, the inputs required from the Customer and the resulting Outputs.

5.2 The activities relating to the specific Issue/ Request type are performed by the Specialist at the Customer´s Request to help the Customer.

5.3 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 Customer hereby acknowledges that in case of non-compliance with the prerequisites mentioned in the previous sentence, the ESET Detection and Response Essential Service will not be available and functional to the full extent. In such cases, ESET shall bear no liability for undelivered and undeliverable parts of the ESET Detection and Response Essential Service.

6. Description of ESET Detection and Response Advanced Service.

6.1 The ESET Detection and Response Advanced Service is a security support service provided by ESET that consists of the features as defined in the sec. 1.3 of annex no. 2. Table A contains for each feature the description of the Issue/Request types, the activities performed by ESET, the inputs required from the Customer and the resulting Outputs.

6.2 To use the ESET Detection and Response Advanced Service, the Customer has to obtain and have installed in its IT environment at least:

a) ESET end-point Products for its end-point Products (Endpoint/ File Security/ Mail Security products + Management Agent and EI Connectors) for its end-point devices,

b) have those end-point devices managed by ESET management console product ESET PROTECT / ESET PROTECT Cloud and

c) EI.

7. Description of ESET Detection and Response Ultimate Service.

7.1 The ESET Detection and Response Ultimate Service is a security support service provided by ESET that consists of the features as defined in the sec. 1.3 of annex no. 2. Table A and Table B contain for each feature the description of the Issue/ Request types (if applicable), the activities performed by ESET, the inputs required from the Customer and the resulting Outputs.

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

a) 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 Connectors) for its end-point devices,

ii. have those end-point devices managed by ESET management console product ESET PROTECT / ESET PROTECT Cloud and

iii. EI.

Those Products/components need to be deployed on minimum versions specified by the Specialists. For this purpose, Deployment and Upgrade activity specified in this Annex shall be performed by ESET, depending on the information on the Customer´s environment.

b) As Deployment and Upgrade activity concerns deployment/upgrade of a limited number of Product units by ESET, as specified in the Table above, and as the proper deployment of certain Products defined above is a prerequisite to provide the ESET Detection and Response Ultimate Service, the Customer is obliged to perform deployment/upgrade of the rest of Products and endpoints within sixty (60) days after ESET´s instruction and provision of deployment/upgrade manual. Failure to perform the required deployment/upgrade by the Customer shall be deemed as failure to provide required cooperation, and ESET reserved the right to restrict or limit the provision of the ESET Detection and Response Ultimate Service until such failure is remedied.

c) Ensure that hardware and operating system are always in line with hardware requirements and OS requirements of Products/ components;

7.3 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.

8. Description of ESET MDR Service.

8.1 The ESET MDR Service is a security support service provided by ESET that consists of the features as defined in the sec. 1.3 of annex no. 2. Table B contains for each feature the description of the activities performed by ESET, the inputs required from the Customer and the resulting Outputs.

8.2 To use the ESET MDR Service, the Customer has to obtain and have installed in its IT environment at least:

a) EI-compatible ESET end-point Products (Endpoint/ File Security/ Mail Security products + Management Agent and EI Connectors) for its end-point devices,

b) have those end-point devices managed by ESET management console product ESET PROTECT Cloud and

c) ESET Inspect Cloud.

8.3 ESET end-points Products need to be deployed on the compatible version with ESET Inspect Cloud.

8.4 When using this ESET MDR 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 incurred thereof.

Annex no. 3.

Termination Form

Customer:	**Service provider:**
BUSINESS NAME	**ESET, spol. s r.o.**
ADDRESS	Einsteinova 24, 851 01 Bratislava, Slovak Republic
Company Reg. no.: INSERT	Company Reg. no.: 31 333 532 registered in the Commercial Register of the Municipal Court Bratislava III, Section Sro, Insertion No. 3586/B
VAT no.: INSERT	VAT no.: SK2020317068
E-mail: INSERT	E-mail: services@eset.com
	(the "**ESET**")

The Customer hereby terminates the **Terms & Conditions for the Provision of Professional and Security Services** (the "**Terms**") executed on DATE in accordance with the Art. 11 of the Terms due to:

☐ ESET´s unremedied substantial/material breach of the Terms (art. 11.2 of the Terms)
☐ a substantial or material change in the Terms (art. 11.3 of the Terms)
☐ bankruptcy or liquidation proceedings, ceasing to carry on business or another similar event or proceeding under the applicable law relating to ESET (art. 11.4 of the Terms)
(please mark the termination ground)

The termination of the Terms shall be valid upon the delivery of this termination form to ESET. ESET shall confirm the termination via e-mail.

Signature date :
Name and position of the Customer´s representative(s):
Signature:

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

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.

1. **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.
2. **Authorization.** The Controller hereby authorizes the Processor to process Personal Data under the following conditions:
   - 2.1 the "purpose of processing" shall mean provision of ordered Services as defined in the Annexes in compliance with the Terms.
   - 2.2 the "processing period" shall mean period during which the Services shall be provided.
   - 2.3 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.
   - 2.4 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.
   - 2.5 the "processing operations" means every operation necessary for the purpose of processing.
   - 2.6 the "documented Instructions" shall mean instructions for Personal Data processing described in the Terms, its Annexes, Service documentation, or in requests for provision of the Service.
3. **Obligations of Processor**. The Processor shall be obliged to do the following:
   - 3.1 to 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.
   - 3.2 to instruct the persons authorized to process the Personal Data (hereinafter referred to as the "Authorized Persons") about their rights and duties according to the GDPR, on their liability in case of breach of the duties and ensure that Authorized Persons authorized to process the Personal Data have committed them-selves to confidentiality and to follow the Documented instructions.
   - 3.3 To 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.
   - 3.4 Taking into account the nature of processing, to 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.
   - 3.5 Upon request, to 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. The Processor shall notify the Controller of any breach of personal data processing or personal data security immediately after the discovery. The Processor shall cooperate to a reasonable extent in an

investigation and remediation of such breach, and take reasonable measures to limit further negative implications.

3.6 At the choice of Controller, to 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. The Controller undertakes to inform the Processor about its decision within ten (10) days upon the end of Processing Period. This provision shall not affect the Processor´s right to keep the Personal Data in the necessary extent for the archival purposes in terms of the special legislation or for the purpose of establishment, exercise or defence of legal claims.

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

3.8 To 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. In case of the audit or control of the Personal Data processing from the Controller´ side, the Controller shall be obliged to inform the Processor in writing at least ten (10) days before the planned audit or control.

4. **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 Processor 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 Controller 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. The Processor hereby undertakes to inform the Controller about any addition or replacement of another processor for purposes of possibility to object such change.

5. **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.

6. **Security**. The Processor is ISO 27001 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.

7. **Technical and Organizational measures**. The Processor shall protect the Personal Data against casual and unlawful damage and destruction, casual loss**,** change, unauthorised access and disclosure. For this purpose, the Processor shall adopt adequate technical, and organizational measures corresponding to the mode of processing and to the risk that is presented by processing for the rights of the Data Subjects in compliance with the requirements of the GDPR. A detailed description of the technical and organizational measures is stated in the security documentation related to the specific Product.

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.

Other language versions can be found here:

Terms_ESET_Services_cze.pdf	https://www.eset.com/fileadmin/ESET/INT/Docs/no-index/Terms_ESET_Services_cze.pdf
Terms_ESET_Services_dut-NL.pdf	https://www.eset.com/fileadmin/ESET/INT/Docs/no-index/Terms_ESET_Services_dut-NL.pdf
Terms_ESET_Services_fre-FR.pdf	https://www.eset.com/fileadmin/ESET/INT/Docs/no-index/Terms_ESET_Services_fre-FR.pdf
Terms_ESET_Services_ger-DE.pdf	https://www.eset.com/fileadmin/ESET/INT/Docs/no-index/Terms_ESET_Services_ger-DE.pdf
Terms_ESET_Services_ita-IT.pdf	https://www.eset.com/fileadmin/ESET/INT/Docs/no-index/Terms_ESET_Services_ita-IT.pdf
Terms_ESET_Services_por-BR.pdf	https://www.eset.com/fileadmin/ESET/INT/Docs/no-index/Terms_ESET_Services_por-BR.pdf
Terms_ESET_Services_spa-CL.pdf	https://www.eset.com/fileadmin/ESET/INT/Docs/no-index/Terms_ESET_Services_spa-CL.pdf
Terms_ESET_Services_ukr.pdf	https://www.eset.com/fileadmin/ESET/INT/Docs/no-index/Terms_ESET_Services_ukr.pdf
Terms_ESET_Services_jpn.pdf	https://www.eset.com/fileadmin/ESET/INT/Docs/no-index/Terms_ESET_Services_jpn.pdf