

ESET Smart TV Security

User guide

[Click here to display the online version of this document](#)

Copyright ©2024 by ESET, spol. s r.o.

ESET Smart TV Security was developed by ESET, spol. s r.o.

For more information visit <https://www.eset.com>.

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

Technical Support: <https://support.eset.com>

REV. 4/12/2024

1 ESET Smart TV Security Introduction	1
1.1 What's new in version 3	1
2 Installation	1
3 Start-up wizard	2
4 Product activation	2
4.1 Antivirus	3
4.1 Advanced Settings	4
4.2 Anti-Phishing	5
4.3 Settings	5
4.4 Customer Care	6
4.5 Update Application	6
5 Customer Experience Improvement Program	6
6 End User License Agreement	7
7 Privacy Policy	18

ESET Smart TV Security Introduction

ESET Smart TV Security is part of our security solution for Android devices. With one ESET license or a Google account subscription, you can protect up to 5 Android devices (smartphones, tablets, Android TVs, ...) signed into the same Google account. ESET Smart TV Security is a fast and powerful antivirus and antimalware application that safeguards your smart television and other devices running on the Android TV operating system from emerging threats and phishing websites, protecting your data and your privacy.

Major features include:

- [Antivirus](#)
- [Anti-Phishing](#)
- Ransomware Shield
- Scheduled scan
- Manual malware scan

What's new in version 3

This version comes with:

- Various bug fixes and performance improvements.
- Support for Android 13.

Installation

ESET Smart TV Security is available for downloading on this distribution channel:



[Google Play](#) – this application receives regular updates via Google Play

To protect your personal information and your Android device's resources, ESET Smart TV Security will need to have access to your device's functions and in some cases have control over them.

Minimum system requirements

Operating system: Android TV OS with Android 6.0 (API level 23) and higher.

i If you have Google Play Store on your TV or console, your OS is Android.

Start-up wizard

Once the application is installed, follow the on-screen prompts in the start-up wizard:

1. Click **Accept** to agree to the terms in the End User License Agreement, User Consent and Privacy Policy.
2. Select the option to either **Allow** or **Decline** your participation in the **ESET Live Grid feedback system**. This can be changed later in the program's settings. To read more, [see this section](#).
3. Select either **Enable** or **Disable** to determine if ESET Smart TV Security will detect Potentially unwanted applications (PUA's). This can be changed later in the program's settings. For more details about PUA's, [see this section](#).
4. Review the permissions for ESET Smart TV Security and click **Continue**. Click **Allow** to allow access for ESET Smart TV Security. If you click **Deny**, ESET Smart TV Security will not be installed successfully.
5. In the **Select your email address** screen, select the email account that will receive emails about ESET license registration, security password reset and Technical Support. Click **Choose e-mail** to display the list of available email accounts. Select the email from the list of accounts or click **Add account** to add a new email account to your device. Click **OK** to confirm the account. Click **Next** to continue.

Note



If you already have a license associated with a Google account, you must enter the associated email address to use your existing license.

6. ESET Smart TV Security is now set up on your device. Click **Start first scan** to scan your device for potential threats.

Product activation

ESET Smart TV Security has three available versions:

- Free – a lifetime license for the Free product; it includes basic features.
- Trial – a 30-day trial license for the Premium product; premium features are activated for the duration of the trial. The trial license is automatically activated the first time ESET Smart TV Security is installed per Google account.
- Premium – a license for the Premium product; premium features are activated for the duration of your premium license.

This table indicates which features are available in the Free, Trial and Premium versions:

	Free	Trial and Premium
Antivirus	✓	✓
Antivirus – automatic scans	✓	✓
Automatic updates of detection modules	✓	✓

	Free	Trial and Premium
Real-Time protection	✓	✓
USB On-The-Go Scan	✓	✓
Ransomware Shield	✓	✓
Anti-Phishing		✓
Scheduled scan		✓

To activate ESET Smart TV Security directly on your Android TV device, navigate to **Settings** on the ESET Smart TV Security main screen and click **License**.

There are multiple ways to activate ESET Smart TV Security.

- If you have already purchased an ESET Premium license with your Google account, ESET Smart TV Security will be automatically activated. You can activate up to 5 products with one ESET license on your Google account. To do so, your Google account has to be active on the devices with ESET products you want to activate.
- You can subscribe to a premium features in the **Yearly** or **Monthly** period. Select this option if you do not have a license and would like to buy one through Google Play. Subscription license is automatically renewed at selected intervals.
- **I have a License Key** – select this option if you already have a license key. A license key is a unique string formatted: XXXX-XXXX-XXXX-XXXX-XXXX which is used to identify the license owner. You can find it in the email received from ESET or on the license card included in the purchased box.

Antivirus

The Antivirus module safeguards your device against malicious code by blocking incoming threats and cleaning them. Real-Time protection scans every newly installed application to provide you with proactive security.

Threats

Allows you to manage threats discovered by ESET Smart TV Security. You can delete all the threats at once by clicking **Remove all** or manage single threats by clicking **Threat detail**. You can also choose to ignore a threat; this will place the threat on a whitelist.

Scan now

This option will perform an immediate scan of your device. Certain predefined file types are scanned by default. A device scan checks the memory, running processes and their dependent dynamic link libraries as well as the files that are part of internal and removable storage. ESET Smart TV Security will start a scan after every start-up of your device.

Update modules

By default, ESET Smart TV Security includes an update task to ensure that the program is regularly updated. To run the update manually, click **Update modules**.

- [Advanced settings](#)

Advanced Settings

Schedule scan

You can schedule a scan on specific days of the week. The scan will be repeated every week on days you selected. To schedule a weekly scan:

1. Click **Schedule scan** in the **Advanced settings** option
2. Click **Enable**
3. Select your scan interval by clicking the days you want to perform the scan on and selecting the time when the scan should be performed.
4. Click **Update**

The scheduled scan will run even when the device is in stand-by mode.

Real-time protection

Real-time scanner launches automatically at system startup and scans the files that you interact with. It automatically scans the *Download* folder and installed or updated applications.

ESET LiveGrid reputation system

ESET LiveGrid is a preventative system designed to provide your device with an additional level of security. It constantly monitors your system's running programs and processes against the latest intelligence collected from millions of ESET users worldwide. This allows us to offer better and more precise proactive protection and scanning speeds to all ESET users. We recommend that you enable this feature.

ESET LiveGrid feedback system

Allows us to collect anonymous statistics, crash reports and diagnostics data about suspicious objects, which we process automatically to create the detection mechanism in our cloud system.

Detect potentially unwanted applications

A potentially unwanted application is a program that contains adware, installs toolbars, traces your search results or has other unclear objectives. There are some situations where you may feel that the benefits of the potentially unwanted application outweigh the risks. For this reason, ESET assigns such applications a lower-risk category compared to other types of malicious software.

Detect potentially unsafe applications

There are many legitimate applications that are designed to simplify the administration of networked devices. However, in the wrong hands, they may be misused for malicious purposes. Enable the **Detect potentially unsafe applications** option to monitor these types of applications and block them if you prefer. Potentially unsafe applications is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers.

Scan level

There are two scan levels to choose from:

- **Smart** — Smart Scan will scan installed applications, DEX files (executable files for Android OS), SO files (libraries), archives with a maximum scanning depth of 3 nested archives and SD card content.
- **In-depth** — In-depth scan will scan all file types regardless of their extension in both internal memory and SD card.

Anti-Phishing

The term *phishing* defines a criminal activity that uses social engineering (the manipulation of users to obtain their confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, credit card numbers, PIN numbers or usernames, and passwords.

We recommend that you keep **Anti-Phishing** enabled. All potential phishing attacks coming from websites or domains will be displayed in a notification informing you of the attempted attack.

Anti-Phishing integrates with the most common web browsers available on Android OS including Chrome and stock browsers that come pre-installed on Android devices (usually labeled *Internet* or *Browser*). Other browsers may be listed as Unprotected since they do not provide sufficient integration for Anti-Phishing. To fully utilize the Anti-Phishing functionality, we recommend that you do not use unsupported web browsers.

Improve functionality – ESET Smart TV Security warns you if Anti-Phishing protection requires you to allow additional permissions in the Android OS. Tap **Allow** to open the system's Accessibility settings and consider the available options to provide support for more browsers and enable protection when browsing in private (incognito) mode. If you do not want this issue to be reported as a problem, tap **Ignore this issue (not recommended)**.

Settings

Language

By default, ESET Smart TV Security is installed in the same language that your device has set as system default (in Android OS Language and keyboard settings). To change the language of the application user interface, click Language and select the language of your choice.

Anonymous Usage Statistics

ESET Smart TV Security will send anonymous application information (performance, operational statistics) that will help us improve our application and services.

Customer Care

ESET Customer Care specialists are available to provide administrative assistance or technical support related to ESET Smart TV Security or any other ESET product.

To contact ESET Customer Care, [follow this link](#).

To send a support request directly from your device, navigate to Settings from the ESET Smart TV Security main screen, click **Customer Care** > **Customer Care form** and fill in all required fields. ESET Smart TV Security includes advanced logging functionality to help diagnose potential technical issues. Click **Send** to send your request. An ESET Customer Care specialist will contact you at the email address you provided.

Update Application

For maximum protection, it is important to use the latest version of ESET Smart TV Security. Click **Update** to see if there is an updated version available for download from the ESET website. This option is not available if you downloaded ESET Smart TV Security from Google Play – in this case, the product is automatically updated from Google Play.

Customer Experience Improvement Program

By joining the Customer Experience Improvement Program you provide ESET with anonymous information relating to the use of our products. More information on data processing is available in our [Privacy Policy](#).

Your consent

Participation in the Program is voluntary and based on your consent. After joining in, the participation is passive, which means you don't need to take any further action. You may revoke your consent by changing the product settings at any time. Doing so will bar us from further processing of your anonymous data.

What types of information do we collect?

Data about interaction with the product

This information tells us more about how our products are used. Thanks to this we know, for example, which functionalities are used often, what settings users modify or how much time they spend using the product.

Data about devices

We collect this information to understand where and what devices our products are used on. Typical examples are device model, country, version and name of the operating system.

Error diagnostics data

Information about error and crash situations is also collected. For example, what error has occurred and which actions led to it.

Why do we collect this information?

This anonymous information lets us improve our products for you, our user. It helps us to make them the most relevant, easy-to-use and faultless as possible.

Who controls this information?

ESET, spol. s r.o. is the sole controller of data collected in the Program. This information is not shared with third parties.

End User License Agreement

Effective as of October 19, 2021.

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE [PRIVACY POLICY](#).**

End User License Agreement

Under the terms of this End User License Agreement ("Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 ("ESET" or "Provider") and you, a physical person or legal entity ("You" or "End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on "I Accept" or "I Accept..." while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement and acknowledge the Privacy Policy. If You do not agree to all of the terms and conditions of this Agreement and/or Privacy Policy, immediately click on the canceling option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to the Provider or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. Software. As used in this Agreement the term "Software" means: (i) computer program accompanied by this Agreement and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software ("Documentation"); (iv) copies of the Software, patches

for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. Installation, Computer and a License key. Software supplied on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured Computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the Computer on which You install the Software. Computer means hardware, including but not limited to personal computers, laptops, workstations, palmtop computers, smartphones, hand-held electronic devices, or other electronic devices for which the Software is designed, on which it will be installed and/or used. License key means the unique sequence of symbols, letters, numbers or special signs provided to the End User in order to allow the legal use of the Software, its specific version or extension of the term of the License in compliance with this Agreement.

3. License. Subject to the condition that You have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights ("License"):

a) **Installation and use.** You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a Computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) **Stipulation of the number of licenses.** The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one Computer; or (ii) if the extent of a license is bound to the number of mailboxes, then one End User shall be taken to refer to a Computer user who accepts electronic mail via a Mail User Agent ("MUA"). If MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one user (e.g., through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one Computer. The End User is entitled to enter the License key to the Software only to the extent to which the End User has the right to use the Software in accordance with the limitation arising from the number of Licenses granted by Provider. The License key is deemed confidential, You must not share the License with third parties or allow third parties to use the License key unless permitted by this Agreement or Provider. If your License key is compromised, notify Provider immediately.

c) **Home/Business Edition.** A Home Edition version of the Software shall be used exclusively in private and/or non-commercial environments for home and family use only. A Business Edition version of the Software must be obtained for use in a commercial environment as well as to use the Software on mail servers, mail relays, mail gateways, or Internet gateways.

d) **Term of the License.** Your right to use the Software shall be time-limited.

e) **OEM Software.** Software classified as "OEM" shall be limited to the Computer You obtained it with. It cannot be transferred to a different Computer.

f) **NFR, TRIAL Software.** Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) Termination of the License. The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software. Upon termination of the License, the Provider shall also be entitled to cancel the End User's entitlement to use the functions of the Software, which require connection to the Provider's servers or third-party servers.

4. Functions with data collection and internet connection requirements. To operate correctly, the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers and applicable data collection in compliance with Privacy Policy. Connection to the Internet and applicable data collection is necessary for the following functions of the Software:

a) Updates to the Software. The Provider shall be entitled from time to time to issue updates or upgrades to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled the automatic installation of Updates. For provisioning of Updates, License authenticity verification is required, including information about Computer and/or the platform on which the Software is installed in compliance with Privacy Policy.

Provision of any Updates may be subject to End of Life Policy ("EOL Policy"), which is available on https://go.eset.com/eol_home. No Updates will be provided after the Software or any of its features reaches the End of Life date as defined in the EOL Policy.

b) Forwarding of infiltrations and information to the Provider. The Software contains functions which collect samples of computer viruses and other malicious computer programs and suspicious, problematic, potentially unwanted or potentially unsafe objects such as files, URLs, IP packets and ethernet frames ("Infiltrations") and then send them to the Provider, including but not limited to information about the installation process, the Computer and/or the platform on which the Software is installed and, information about the operations and functionality of the Software ("Information"). The Information and Infiltrations may contain data (including randomly or accidentally obtained personal data) about the End User or other users of the Computer on which the Software is installed, and files affected by Infiltrations with associated metadata.

Information and Infiltrations may be collected by following functions of Software:

i. LiveGrid Reputation System function includes collection and sending of one-way hashes related to Infiltrations to Provider. This function is enabled under the Software's standard settings.

ii. LiveGrid Feedback System function includes collection and sending of Infiltrations with associated metadata and Information to Provider. This function may be activated by End User during the process of installation of the Software.

The Provider shall only use Information and Infiltrations received for the purpose of analysis and research of Infiltrations, improvement of Software and License authenticity verification and shall take appropriate measures to ensure that Infiltrations and Information received remain secure. By activating this function of the Software, Infiltrations and Information may be collected and processed by the Provider as specified in Privacy Policy and in compliance with relevant legal regulations. You can deactivate these functions at any time.

For the purpose of this Agreement, it is necessary to collect, process and store data enabling the Provider to identify You in compliance with Privacy Policy. You hereby acknowledge that the Provider checks using its own means whether You are using the Software in accordance with the provisions of this Agreement. You hereby acknowledge that for the purpose of this Agreement it is necessary for your data to be transferred, during communication between the Software and the Provider's computer systems or those of its business partners as

part of Provider's distribution and support network to ensure functionality of Software and authorization to use the Software and to protection of the Provider's rights.

Following conclusion of this Agreement, the Provider or any of its business partners as part of Provider's distribution and support network shall be entitled to transfer, process and store essential data identifying You for billing purposes, performance of this Agreement and transmitting notifications on your Computer.

Details about privacy, personal data protection and Your rights as a data subject can be found in Privacy Policy which is available on Provider's website and accessible directly from the installation process. You can also visit it from Software's help section.

5. Exercising End User rights. You must exercise End User rights in person or via your employees. You are only entitled to use the Software to safeguard your operations and protect those Computers or computers systems for which You have obtained a License.

6. Restrictions to rights. You may not copy, distribute, extract components or make derivative works of the Software. When using the Software, You are required to comply with the following restrictions:

a) You may make one copy of the Software on a permanent storage medium as an archival backup copy, provided your archival back-up copy is not installed or used on any Computer. Any other copies You make of the Software shall constitute a breach of this Agreement.

b) You may not use, modify, translate or reproduce the Software or transfer rights to use the Software or copies of the Software in any manner other than as provided for in this Agreement.

c) You may not sell, sub-license, lease or rent or borrow the Software or use the Software for the provision of commercial services.

d) You may not reverse engineer, reverse compile or disassemble the Software or otherwise attempt to discover the source code of the Software, except to the extent that this restriction is expressly prohibited by law.

e) You agree that You will only use the Software in a manner that complies with all applicable laws in the jurisdiction in which You use the Software, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

f) You agree that You will only use the Software and its functions in a way which does not limit the possibilities of other End Users to access these services. The Provider reserves the right to limit the scope of services provided to individual End Users, to enable use of the services by the highest possible number of End Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Software and deletion of Data and information on the Provider's servers or third-party servers relating to a specific function of the Software.

g) You agree not to exercise any activities involving use the License key, contrary to the terms of this Agreement or leading to provide License key to any person who is not entitled to use the Software, such as the transfer of used or unused License key in any form, as well as the unauthorized reproduction, or distribution of duplicated or generated License keys or using the Software as a result of the use of a License key obtained from the source other than the Provider.

7. Copyright. The Software and all rights, without limitation including proprietary rights and intellectual property rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 6(a). Any copies which You are

permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

8. Reservation of rights. The Provider hereby reserves all rights to the Software, with the exception of rights expressly granted under the terms of this Agreement to You as the End User of the Software.

9. Multiple language versions, dual media software, multiple copies. In the event that the Software supports multiple platforms or languages, or if You receive multiple copies of the Software, You may only use the Software for the number of computer systems and for the versions for which You obtained a License. You may not sell, rent, lease, sub-license, lend or transfer versions or copies of the Software which You do not use.

10. Commencement and termination of the Agreement. This Agreement shall be effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own cost, the Software, all backup copies and all related materials provided by the Provider or its business partners. Your right to use Software and any of its features may be subject to EOL Policy. After the Software or any of its features reaches the End of Life date defined in the EOL Policy, your right to use the Software will terminate. Irrespective of the manner of termination of this Agreement, the provisions of Articles 7, 8, 11, 13, 19 and 21 shall continue to apply for an unlimited time.

11. END USER DECLARATIONS. AS THE END USER YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION OF THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM IT.

12. No other obligations. This Agreement creates no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

13. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE INSTALLATION, THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

14. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer if running contrary thereto.

15. Technical support. ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. No technical support will be provided after the Software or any of its features reaches the End of Life date defined in the EOL Policy. The End User shall be required to back up all existing data, software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the right to refuse, suspend or terminate the provision of technical support at its own discretion. License information, Information and other data in compliance with Privacy Policy may be required for the purpose of technical support provision.

16. Transfer of the License. The Software can be transferred from one Computer to another, unless contrary to the terms of the Agreement. If not contrary to the terms of the Agreement, the End User shall only be entitled to permanently transfer the License and all rights ensuing from this Agreement to another End User with the Provider's consent, subject to the condition that (i) the original End User does not retain any copies of the Software; (ii) the transfer of rights must be direct, i.e. from the original End User to the new End User; (iii) the new End User must assume all the rights and obligations incumbent on the original End User under the terms of this Agreement; (iv) the original End User has to provide the new End User with documentation enabling verification of the genuineness of the Software as specified under Article 17.

17. Verification of the genuineness of the Software. The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii) through the submission of an e-mail sent by the Provider containing licensing details (user name and password). License information and End User identification data in compliance with Privacy Policy may be required for the purpose of Software genuineness verification.

18. Licensing for public authorities and the US Government. The Software shall be provided to public authorities, including the United States Government, with the license rights and restrictions described in this Agreement.

19. Trade control compliance.

a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any person, or use it in any manner, or be involved in any activity, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies ("Affiliates") being in violation of, or being subject to, negative consequences under trade control laws which include:

i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate, and

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate.

(legal acts referred to in points i, and ii. above together as "Trade Control Laws").

b) ESET shall have the right to suspend its obligations under, or terminate, these Terms with immediate effect in

the event that:

- i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of Article 19 a) of the Agreement; or
- ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under the Agreement could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.
- c) Nothing in the Agreement is intended, and nothing should be interpreted or construed, to induce or require either party to act or refrain from acting (or to agree to act or refrain from acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

20. Notices. All notices and returns of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, without prejudice to ESET's right to communicate to You any changes to this Agreement, Privacy Policies, EOL Policy and Documentation in accordance with art. 22 of the Agreement. ESET may send You emails, in-app notifications via Software or post the communication on our website. You agree to receive legal communications from ESET in electronic form, including any communications on change in Terms, Special Terms or Privacy Policies, any contract proposal/acceptance or invitations to treat, notices or other legal communications. Such electronic communication shall be deemed as received in writing, unless applicable laws specifically require a different form of communication.

21. Applicable law. This Agreement shall be governed by and construed in accordance with the laws of the Slovak Republic. The End User and the Provider hereby agree that the principles of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that any disputes or claims ensuing from this Agreement with respect to the Provider or any disputes or claims relating to use of the Software shall be settled by Bratislava I District Court and You expressly agree to the said court exercising jurisdiction.

22. General provisions. Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable under the conditions stipulated therein. This Agreement has been executed in English. In case any translation of the Agreement is prepared for the convenience or any other purpose or in any case of a discrepancy between language versions of this Agreement, the English version shall prevail.

ESET reserves the right to make changes to the Software as well as to revise terms of this Agreement, its Annexes, Addendums, Privacy Policy, EOL Policy and Documentation or any part thereof at any time by updating the relevant document (i) to reflect changes to the Software or to how ESET does business, (ii) for legal, regulatory or security reasons, or (iii) to prevent abuse or harm. You will be notified about any revision of the Agreement by email, in-app notification or by other electronic means. If You disagree with the proposed changes to the Agreement, You may terminate it in accordance with Art. 10 within 30 days after receiving a notice of the change. Unless You terminate the Agreement within this time limit, the proposed changes will be deemed accepted and become effective towards You as of the date You received a notice of the change.

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.

ADDENDUM TO THE AGREEMENT

Network Connected Devices Security Assessment. Additional provisions apply to the Network Connected Devices Security Assessment as follows:

The Software contains a function for checking the security of End User's local network and security of devices in

local network which requires local network name and information about devices in local network such as presence, type, name, IP address and MAC address of device in local network in connection with license information. The information also includes wireless security type and wireless encryption type for router devices. This function may also provide information concerning availability of security software solution to secure devices in local network.

Protection Against Misuse of Data. Additional provisions apply to the Protection Against Misuse of Data as follows:

The Software contains a function that prevents loss or misuse of critical data in direct connection with theft of a Computer. This function is switched off under the default settings of the Software. The ESET HOME Account needs to be created for it to be activated, through which the function activates data collection in the event of computer theft. If you chose to activate this function of the Software, data about the stolen Computer will be collected and sent to the Provider, which can include data about the Computer's network location, data about the content displayed on the Computer screen, data about the configuration of the Computer and/or data recorded by a camera connected to the Computer (hereinafter referred to as "Data"). The End User shall be entitled to use Data obtained by this function and provided via ESET HOME Account exclusively for rectifying an adverse situation caused by theft of a Computer. For the sole purpose of this function, Provider process Data as specified in Privacy Policy and in compliance with relevant legal regulations. The Provider shall allow End User to access the Data for the period required to achieve the purpose for which the data was obtained which shall not exceed retention period specified in Privacy Policy. Protection against misuse of data shall be used exclusively with Computers and accounts End User have legitimate access to. Any illegal use will be reported to competent authority. Provider will comply with relevant laws and assist law enforcement authorities in case of the misuse. You agree and acknowledge that You are responsible for safeguarding the password to access ESET HOME Account and you agree that You shall not disclose your password to any third party. End User is responsible for any activity using Protection Against Misuse of Data function and ESET HOME Account, authorized or not. If ESET HOME Account is compromised, notify Provider immediately. Additional provisions for the Protection Against Misuse of Data shall be applicable exclusively to ESET Internet Security and ESET Smart Security Premium End Users.

ESET Secure Data. Additional provisions apply to the ESET Secure Data as follows:

1. Definitions. In these additional provisions to the ESET Secure Data the following words have the corresponding meanings:

- a) "Information" any information or data encrypted or decrypted using the software;
- b) "Products" the ESET Secure Data software and the documentation;
- c) "ESET Secure Data" the software(s) used for the encryption and decryption of electronic data;

All references to the plural shall include the singular and all references to the masculine shall include the feminine and neuter and vice versa. Words without specific definition shall be used in compliance with definitions stipulated by the Agreement.

2. Additional End User declaration. You acknowledge and accept that:

- a) It is Your responsibility to protect, maintain and backup Information;
- b) You should fully back-up all information and data (including without limit any critical information and data) on Your Computer before installation of the ESET Secure Data;
- c) You must keep a safe record of any passwords or other information used for setting up and using ESET Secure Data, you must also make backup copies of all encryption keys, license codes, key-files and other data generated

to separate storage media;

d) You are responsible for the use of Products. The Provider shall not be liable for any loss, claim or damage suffered as a consequence of any unauthorized or mistaken encryption or decryption of Information or other data wherever and however that Information or other data is stored;

e) Whilst Provider has taken all reasonable steps to ensure the integrity and security of the ESET Secure Data, the Products (or any of them) must not be used in any area which is dependent on a fail-safe level of security or is potentially hazardous or dangerous, including but not limited to nuclear facilities, aircraft navigation, control or communication systems, weapon and defense systems and life support or life monitoring systems;

f) It is End User's responsibility to ensure that the level of security and encryption provided by the products is adequate for Your requirements;

g) You are responsible for Your use of the Products or any of them, including but not limited to ensure that such use complies with all applicable laws and regulations of the Slovak Republic or such other country, region or state where the Products are used. You must ensure that prior to any use of the Products you have ensured that it is not in contravention of any government (in the Slovak Republic or otherwise) embargo;

h) ESET Secure Data may contact the Provider servers from time to time in order to check for the license information, available patches, service packs and other updates that may improve, maintain, modify or enhance the operation of ESET Secure Data and may send general system information related to the its functioning in compliance with Privacy Policy.

i) Provider shall not be responsible for any loss, damage, expense or claim arising from the loss, theft, misuse, corruption, damage or destruction of passwords, set up information, encryption keys, license activation codes and other data generated or stored during use of the software.

Additional provisions for the ESET Secure Data shall be applicable exclusively to ESET Smart Security Premium End Users.

Password Manager Software. Additional provisions apply to the Password Manager Software as follows:

1. Additional End User declaration. You acknowledge and accept that You may not:

a) use Password Manager Software to operate any mission-critical application where human life or property may be at stake. You understand that the Password Manager Software is not designed for such purposes and that its failure in such cases could lead to death, personal injury, or severe property or environmental damage for which Provider is not responsible.

PASSWORD MANAGER SOFTWARE IS NOT DESIGNED, INTENDED OR LICENSED FOR USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE CONTROLS INCLUDING, WITHOUT LIMITATION, THE DESIGN, CONSTRUCTION, MAINTENANCE OR OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, AND LIFE SUPPORT OR WEAPONS SYSTEMS. PROVIDER SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR SUCH PURPOSES.

b) use Password Manager Software in a manner that breaches this agreement or the laws of the Slovak Republic or your jurisdiction. Specifically you may not use Password Manager Software to conduct or promote any illegal activities including uploading data of harmful content or content that might be used for any illegal activities or that in any way violates the law or the rights of any third party (including any intellectual property rights), including but not limited to any attempts to gain access to accounts in Storage (For the purposes of these additional terms to the Password Manager Software "Storage" refers to the data storage space managed by Provider or a third party other than Provider and the user for the purpose of enabling synchronization and backup

of user data) or any accounts and data of other Password Manager Software or Storage users. If you violate any of these provisions, Provider is entitled to immediately terminate this agreement and pass on to you the cost of any necessary remedy, as well as take any necessary steps to prevent you from further use of Password Manager Software without the possibility of refund.

2. LIMITATION OF LIABILITY. PASSWORD MANAGER SOFTWARE IS PROVIDED "AS IS". NO WARRANTY OF ANY KIND IS EXPRESSED OR IMPLIED. YOU USE THE SOFTWARE AT YOUR OWN RISK. THE PRODUCER IS NOT LIABLE FOR DATA LOSS, DAMAGES, LIMITATION OF SERVICE AVAILABILITY INCLUDING ANY DATA SENT BY PASSWORD MANAGER SOFTWARE TO EXTERNAL STORAGE FOR THE PURPOSE OF DATA SYNCHRONIZATION AND BACKUP. ENCRYPTING THE DATA USING PASSWORD MANAGER SOFTWARE DOES NOT IMPLY ANY LIABILITY OF THE PROVIDER REGARDING THE SECURITY OF THAT DATA. YOU EXPRESSLY AGREE THAT THE DATA ACQUIRED, USED, ENCRYPTED, STORED, SYNCHRONIZED OR SENT USING PASSWORD MANAGER SOFTWARE CAN ALSO BE STORED ON THIRD-PARTY SERVERS (APPLIES ONLY TO THE USE OF PASSWORD MANAGER SOFTWARE WHERE SYNCHRONIZATION AND BACKUP SERVICES HAVE BEEN ENABLED). IF PROVIDER IN ITS SOLE DISCRETION SELECTS TO USE SUCH A THIRD-PARTY STORAGE, WEBSITE, WEB PORTAL, SERVER OR SERVICE, PROVIDER IS NOT LIABLE FOR THE QUALITY, SECURITY, OR AVAILABILITY OF SUCH A THIRD-PARTY SERVICE AND TO NO EXTENT IS PROVIDER LIABLE TO YOU FOR ANY BREACH OF CONTRACTUAL OR LEGAL OBLIGATIONS BY THE THIRD PARTY NOR FOR DAMAGES, LOSS OF PROFITS, FINANCIAL OR NON-FINANCIAL DAMAGES, OR ANY OTHER KIND OF LOSS WHILE USING THIS SOFTWARE. PROVIDER IS NOT LIABLE FOR THE CONTENT OF ANY DATA ACQUIRED, USED, ENCRYPTED, STORED, SYNCHRONIZED, OR SENT USING PASSWORD MANAGER SOFTWARE OR IN STORAGE. YOU ACKNOWLEDGE THAT PROVIDER DOES NOT HAVE ACCESS TO THE CONTENT OF THE STORED DATA AND IS NOT ABLE TO MONITOR IT OR REMOVE LEGALLY HARMFUL CONTENT.

Provider owns all rights to improvements, upgrades and fixes related to Password Manager Software ("Improvements") even in the event that any such Improvements have been created based on feedback, ideas or suggestions submitted by you in any form. You will not be entitled to any compensation, including any royalties related to such Improvements.

PROVIDER ENTITIES AND LICENSORS WILL NOT BE LIABLE TO YOU FOR CLAIMS AND LIABILITIES OF ANY KIND ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF PASSWORD MANAGER SOFTWARE BY YOU OR BY THIRD PARTIES, TO THE USE OR NON-USE OF ANY BROKERAGE FIRM OR DEALER, OR TO THE SALE OR PURCHASE OF ANY SECURITY, WHETHER SUCH CLAIMS AND LIABILITIES ARE BASED ON ANY LEGAL OR EQUITABLE THEORY.

PROVIDER ENTITIES AND LICENSORS ARE NOT LIABLE TO YOU FOR ANY AND ALL DIRECT, INCIDENTAL, SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATED TO ANY THIRD-PARTY SOFTWARE, ANY DATA ACCESSED THROUGH PASSWORD MANAGER SOFTWARE, YOUR USE OR INABILITY TO USE OR ACCESS PASSWORD MANAGER SOFTWARE, OR ANY DATA PROVIDED THROUGH PASSWORD MANAGER SOFTWARE, WHETHER SUCH DAMAGE CLAIMS ARE BROUGHT UNDER ANY THEORY OF LAW OR EQUITY. DAMAGES EXCLUDED BY THIS CLAUSE INCLUDE, WITHOUT LIMITATION, THOSE FOR LOSS OF BUSINESS PROFITS, INJURY TO PERSON OR PROPERTY, BUSINESS INTERRUPTION, LOSS OF BUSINESS OR PERSONAL INFORMATION. SOME JURISDICTIONS DO NOT ALLOW LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THIS RESTRICTION MAY NOT APPLY TO YOU. IN SUCH CASE THE EXTENT OF PROVIDER LIABILITY WILL BE THE MINIMUM PERMITTED UNDER APPLICABLE LAW.

INFORMATION PROVIDED THROUGH PASSWORD MANAGER SOFTWARE, INCLUDING STOCK QUOTES, ANALYSIS, MARKET INFORMATION, NEWS, AND FINANCIAL DATA, MAY BE DELAYED, INACCURATE, OR CONTAIN ERRORS OR OMISSIONS, AND PROVIDER ENTITIES AND LICENSORS WILL HAVE NO LIABILITY WITH RESPECT THERETO. PROVIDER MAY CHANGE OR DISCONTINUE ANY ASPECT OR FEATURE OF PASSWORD MANAGER SOFTWARE OR THE USE OF ALL OR ANY FEATURES OR TECHNOLOGY IN PASSWORD MANAGER SOFTWARE AT ANY TIME WITHOUT PRIOR NOTICE TO YOU.

IF THE PROVISIONS IN THIS ARTICLE ARE VOID FOR ANY REASON OR PROVIDER IS DEEMED LIABLE FOR LOSSES, DAMAGES ETC UNDER APPLICABLE LAWS, THE PARTIES AGREE THAT PROVIDER'S LIABILITY TO YOU WILL BE

LIMITED TO THE TOTAL AMOUNT OF LICENSE FEES PAID BY YOU.

YOU AGREE TO INDEMNIFY, DEFEND AND HOLD HARMLESS PROVIDER AND ITS EMPLOYEES, SUBSIDIARIES, AFFILIATES, REBRANDING AND OTHER PARTNERS FROM AND AGAINST ANY AND ALL THIRD PARTY (INCLUDING OWNERS OF THE DEVICE OR PARTIES WHOSE RIGHTS WERE AFFECTED BY THE DATA USED IN PASSWORD MANAGER SOFTWARE OR IN STORAGE) CLAIMS, LIABILITIES, DAMAGES, LOSSES, COSTS, EXPENSES, FEES THAT SUCH PARTIES MAY INCUR AS A RESULT OF YOUR USE OF THE PASSWORD MANAGER SOFTWARE.

3. Data in Password Manager Software. Unless otherwise, and explicitly, selected by you, all data entered by you that is saved into a Password Manager Software database is stored in encrypted format on your computer, or other storage device as defined by you. You understand that in the case of deletion of, or damage to, any Password Manager Software database or other files, all the data contained therein will be irreversibly lost and you understand and accept the risk of such loss. The fact that your personal data is stored in encrypted format on the computer does not mean that the information cannot be stolen or misused by someone who discovers the Master Password or gains access to the customer-defined activation device for opening the database. You are responsible for maintaining the security of all access methods.

4. Transmission of Personal Data to Provider or Storage. If You select so and solely for the purpose of ensuring timely data synchronization and backup, Password Manager Software transmits or sends personal data from the Password Manager Software database - namely passwords, login information, Accounts and Identities to Storage over the Internet. Data is transmitted exclusively in encrypted form. The use of Password Manager Software for filling in online forms with passwords, logins or other data may require that information being sent over the Internet to the website identified by You. This transmission of data is not initiated by Password Manager Software and therefore Provider cannot be held responsible for the security of such interactions with any website operated by various providers. Any transactions over the Internet whether or not in conjunction with Password Manager Software is done at Your own discretion and risk, and You will be solely responsible for any damage to Your Computer or loss of data resulting from the download and/or use of any such material or service. To minimize the risk of losing valuable data, Provider recommends that End User perform periodic backup of the database and other sensitive files to external drives. Provider is not able to provide You with any assistance in recovering lost or damaged data. If Provider provides backup services for End User database files in case of damage or deletion of the files on End User's Computer, such backup service is without any warranty and does not imply any liability of Provider to you whatsoever.

By using Password Manager Software, you agree that the software may contact the Provider servers from time to time in order to check for the license information, available patches, service packs and other updates that may improve, maintain, modify or enhance the operation of Password Manager Software. The software may send general system information related to the functioning of Password Manager Software in compliance with Privacy Policy.

5. Uninstall information and instructions. Any information that you would like to retain from the database must be exported prior to uninstalling Password Manager Software.

Additional provisions for the Password Manager Software shall be applicable exclusively to ESET Smart Security Premium End Users.

ESET LiveGuard. Additional provisions apply to the ESET LiveGuard as follows:

The Software contains a function of additional analysis of files submitted by End User. The Provider shall only use the files submitted by End User and results of analysis in compliance with Privacy Policy and in compliance with relevant legal regulations.

Additional provisions for the ESET LiveGuard shall be applicable exclusively to ESET Smart Security Premium End Users.

Privacy Policy

ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 as a Data Controller ("ESET" or "We") would like to be transparent when it comes to processing of personal data and privacy of our customers. To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") about following topics:

- Processing of Personal Data,
- Data Confidentiality,
- Data Subject's Rights.

Processing of Personal Data

Services provided by ESET implemented in our product are provided under the terms of End User License Agreement ("EULA"), but some of them might require specific attention. We would like to provide You with more details on data collection connected with the provision of our services. We render various services described in the EULA and product documentation such as update/upgrade service, ESET LiveGrid®, protection against misuse of data, support, etc. To make it all work, We need to collect the following information:

- Update and other statistics covering information concerning installation process and your computer including platform on which our product is installed and information about the operations and functionality of our products such as operation system, hardware information, installation IDs, license IDs, IP address, MAC address, configuration settings of product.
- One-way hashes related to infiltrations as part of ESET LiveGrid® Reputation System which improves the efficiency of our anti-malware solutions by comparing scanned files to a database of whitelisted and blacklisted items in the cloud.
- Suspicious samples and metadata from the wild as part of ESET LiveGrid® Feedback System which enables ESET to react immediately to needs of our end users and keep us responsive to the latest threats providing. We are dependent on You sending us

o infiltrations such as potential samples of viruses and other malicious programs and suspicious; problematic, potentially unwanted or potentially unsafe objects such as executable files, email messages reported by You as spam or flagged by our product;

o information about devices in local network such as type, vendor, model and/or name of device;

o information concerning the use of internet such as IP address and geographic information, IP packets, URLs and ethernet frames;

o crash dump files and information contained.

We do not desire to collect your data outside of this scope but sometimes it is impossible to prevent it. Accidentally collected data may be included in malware itself (collected without your knowledge or approval) or as part of filenames or URLs and We do not intend it to form part of our systems or process it for the purpose declared in this Privacy Policy.

- Licensing information such as license ID and personal data such as name, surname, address, email address is

required for billing purposes, license genuineness verification and provision of our services.

- Contact information and data contained in your support requests may be required for service of support. Based on the channel You choose to contact us, We may collect your email address, phone number, license information, product details and description of your support case. You may be asked to provide us with other information to facilitate service of support.

Data Confidentiality

ESET is a company operating worldwide via affiliated entities or partners as part of our distribution, service and support network. Information processed by ESET may be transferred to and from affiliated entities or partners for performance of the EULA such as provision of services or support or billing. Based on your location and service You choose to use, We might be required to transfer your data to a country with absence of adequacy decision by the European Commission. Even in this case, every transfer of information is subject to regulation of data protection legislation and takes place only if required. Standard Contractual Clauses, Binding Corporate Rules or another appropriate safeguard must be established without any exception.

We are doing our best to prevent data from being stored longer than necessary while providing services under the EULA. Our retention period might be longer than the validity of your license just to give You time for easy and comfortable renewal. Minimized and pseudonymized statistics and other data from ESET LiveGrid® may be further processed for statistical purposes.

ESET implements appropriate technical and organizational measures to ensure a level of security which is appropriate to potential risks. We are doing our best to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and Services. However, in case of data breach resulting in a risk to your rights and freedoms, We are ready to notify supervisory authority as well as data subjects. As a data subject, You have a right to lodge a complaint with a supervisory authority.

Data Subject's Rights

ESET is subject to regulation of Slovak laws and We are bound by data protection legislation as part of European Union. Subject to conditions laid down by applicable data protection laws, You are entitled to following rights as a data subject:

- right to request access to your personal data from ESET,
- right to rectification of your personal data if inaccurate (You also have the right to have the incomplete personal data completed),
- right to request erasure of your personal data,
- right to request restriction of processing your personal data,
- right to object to processing,
- right to lodge a complaint as well as,
- right to data portability.

If You would like to exercise your right as a data subject or You have a question or concern, send us a message at:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava

Slovak Republic
dpo@eset.sk