

Kaspersky Security Center 11 END USER LICENSE AGREEMENT; AND  
Products and Services PRIVACY POLICY

KASPERSKY LAB END USER LICENSE AGREEMENT ("LICENSE AGREEMENT")

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE  
YOU START USING THE SOFTWARE.

CLICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE WINDOW CONTAINING THE LICENSE  
AGREEMENT, OR BY ENTERING CORRESPONDING SYMBOL(-S), YOU CONFIRM IN A LEGALLY BINDING WAY  
THAT YOU AS THE ORGANIZATION FOR WHICH THE SOFTWARE IS DOWNLOADED OR ACQUIRED HAVE  
AUTHORIZED THE NATURAL PERSON ACCEPTING THIS LICENSE AGREEMENT TO ENTER INTO THIS LICENSE  
AGREEMENT FOR AND ON BEHALF OF YOU. FURTHERMORE, YOU CONSENT TO BE BOUND BY THE TERMS AND  
CONDITIONS OF THIS LICENSE AGREEMENT. SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU  
ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS LICENSE AGREEMENT AND AGREE  
THAT THIS LICENSE AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY  
YOU. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT,  
CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

IF LICENSE CONTRACT OR SIMILAR DOCUMENT ACCOMPANIES SOFTWARE, TERMS OF THE SOFTWARE USE  
DEFINED IN SUCH DOCUMENT PREVAIL OVER THE CURRENT LICENSE AGREEMENT.

AFTER CLICKING THE ACCEPT BUTTON IN THE WINDOW CONTAINING THE LICENSE AGREEMENT OR AFTER  
ENTERING CORRESPONDING SYMBOL(-S), YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE  
WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

If You are an individual, you must have achieved legal capacity to contract in the state,  
province or country in which you are resident in order to be able to enter into this  
Agreement. If you acquire the Software on behalf of an organization, you must be duly  
authorized to represent the organization and conclude this Agreement on behalf of the  
organization.

## 1. Definitions

1.1. Software means software including any Updates and related materials.

1.2. Standard version of the Software means free of charge version of the Software  
provided to users of corporate software products of the Rightholder.

1.3. Extended version of the Software means version of the Software which functionality is  
available only after activation or key file installation.

1.4. Rightholder (owner of all rights, whether exclusive or otherwise to the Software)  
means AO Kaspersky Lab, a company incorporated according to the laws of the Russian  
Federation.

1.5. Object of protection means operating system(s) and system virtual machines and  
hardware(s) including workstation, the mobile device and server for which the Software was  
designed and/or where the Software can be installed and/or used as well as email boxes and  
other objects protected or controlled by the Software.

1.6. End User (You/Your) means the organization for which the Software is downloaded or  
installed and it is represented hereby that such organization has authorized the person  
accepting this agreement to do so on its behalf. For purposes hereof the term  
"organization," without limitation, includes any partnership, limited liability company,  
corporation, association, joint stock company, trust, joint venture, labor organization,  
unincorporated organization, or governmental authority. If the Software was downloaded or  
installed on behalf of individual, End User ("You") further means such individual.

1.7. Partner(s) means organizations or individual(s), who distributes the Software based  
on an agreement and license with the Rightholder.

1.8. Update(s) means all upgrades, revisions, patches, enhancements, fixes, modifications,  
copies, additions or maintenance packs etc.

1.9. User Manual means user manual, administrator guide, implementation guide, reference  
book and related explanatory or other materials.

1.10. Activation Code is a unique set of characters which can be used to activate the  
Software.

1.11. Key File - means a file with the extension ".key" which can be used to activate the  
Software.

1.12. License Certificate means a document that is given to the User which is accompanied by a license key and activation code as well as further information about the license.

## 2. Grant of License

2.1. You are given a non-exclusive and non-assignable and revocable license to download, install, store, load, execute, and display (collectively "use") the Software according to the provisions of this Agreement and according to the restrictions described on the accompanying documentation, product packaging and/or in the User Manual ("License"). You are not entitled to sell, rent, sub-license, lease or lend or otherwise transfer the Software.

If you use the trial version of the Extended version of the Software you may use it only for evaluation purposes and only for the single applicable evaluation period, from the date of the initial trial version's activation. After termination of the applicable evaluation period You are given the rights to use the Extended version of the Software in accordance with the conditions described in the User Manual only.

Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the Software bundled with other software, the total permitted number of your Objects of protection for which all versions of the Software are used shall correspond to the number of Objects of protection specified in licenses you have obtained provided that unless the licensing terms provide otherwise, each acquired license entitles you to install and use the Software for such a number of Object(s) of protection as is specified in Clause 2.2.

2.2. Number of Object(s) of protection for which You have the right to use the Extended version of the Software is limited to the number of the Object(s) of protection that was specified in License Certificate. The number of Object(s) of protection for which You have the right to use the Standard version of the Software is unlimited.

2.3. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of your principal residence or in the country where You are using the Software.

2.4. After installation of the Standard version of the Software users of the Rightholder's commercial corporate software products have the right to receive the following services from the Rightholder or its Partners:

- Updates of the Standard version of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that You may receive become part of the Software and the terms and conditions of this Agreement apply to them;
- Technical Support via the Internet and Technical Support telephone hotline;
- Access to information and auxiliary resources of the Rightholder.

2.5. After activation or key file installation for the Extended version of the Software You have the right to receive the following services from the Rightholder or its Partners for the period specified in the License Certificate:

- Updates of the Extended version of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that you may receive become part of the Software and the terms and conditions of this Agreement apply to them;
- Technical Support via the Internet and Technical Support telephone hotline;
- Access to information and auxiliary resources of the Rightholder.

## 3. Activation and Term

3.1. If You modify Your computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat activation of the Extended version of the Software or license key file installation. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the License and/or legality of a copy of the Extended version of the Software installed and/or used on Your computer.

3.2. The duration of the evolution period for the Extended version of the Software is limited to either the single applicable evaluation period (30 days) from the time of the

Software's activation or before the start of the period of effective use of the Extended version of the Software according to this Agreement. If the Rightholder changes the duration of the evaluation period You will be informed via notification.

3.3. Your License to Use the Extended version of the Software is limited to the period of time as specified in the License Certificate, the remaining period can be viewed via means described in the User Manual.

3.4. After expiration of the period of effective use as specified in Clause 3.3 functionality of the Extended version of the Software will be limited to functionality of Standard version of the Software.

3.5. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License without refunding the purchase price or any part thereof.

3.6. You agree that in using the Software and in using any report or information derived as a result of using this Software, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.

3.7. Except as otherwise specifically provided herein, you may not transfer or assign any of the rights granted to you under this Agreement or any of your obligations pursuant hereto.

3.8. The period of use of the Standard version of the Software is not limited by the Rightholder.

#### 4. Technical Support

4.1. The Technical Support described in Clauses 2.4 and 2.5 of this Agreement is provided to You according to rules located at <http://support.kaspersky.com/support/rules>.

Technical support service: <http://support.kaspersky.com>.

#### 5. Conditions regarding Data Processing

5.1. Under this Section additional definitions are introduced:

Data Subject - means a natural person who is a representative of the End User and/or who uses the Software directly or indirectly, including a worker, contractor, employee, or client of the End User in respect of whom the data is transmitted and processed in the context of the End User's activities, including data which could be determined as personal data under the laws of some countries. Data Subject may also include any individual who communicates and transmits his or her data to the End User.

5.2. Where the Activation Code is used to activate the Software, in order to verify legitimate use of the Software, the End User agrees to periodically provide the Rightholder the following information: the type, version and localization of the installed Software, versions of the installed Updates, the identifier of the Computer and the identifier of the Software installation on the Computer, the activation code and the unique identifier of activation of the current license, the type, version and word size of the operating system, the name of the virtual environment when the Software is installed in the virtual environment, and identifiers of the Software components that are active at the time the information is provided.

The Rightholder can use such information also for gathering statistical information about the distribution and use of the Rightholder's Software.

By using the Activation Code, the End User gives its consent to automatically transmit the data specified in this Clause. In case the End User does not agree to provide this information to the Rightholder, the Key File should be used to activate the Software.

5.3. The Rightholder undertakes the processing of all data received from the End User in accordance with the instructions of the End User. License Agreement, in particular the provisions of Section 5 "Conditions regarding Data Processing," along with use of the functionality of the Software and its configuration by the End User are complete instructions issued by the End User to the Rightholder regarding data processing unless otherwise specified in a separate written agreement between the End User and the Rightholder or its Partners.

5.4. The End User is solely responsible for acquainting itself with the User Manual, particularly in regards to data processing, with the Rightholder's Privacy Policy, which describes data handling ([www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy)) and independently determining whether they comply with the End User's requirements.

5.5. The End User must comply with laws that apply to use of the Software, including laws

on confidential information, personal data, data protection. The End User is responsible for implementing and maintaining confidentiality and security measures in respect of data when using Software components that process data without the participation of the Rightholder. The End User must determine the appropriate technical and organizational measures for the protection and confidentiality of the data during use of such components of the Software.

5.6. During use of the Software, especially where the End User configures the Software to use the Kaspersky Security Network, the End User is fully responsible for ensuring that the processing of personal data of Data Subjects is lawful, particularly, within the meaning of Article 6 (1) (a) to (f) of Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR") (if Data Subject is in the European Union) or applicable laws on confidential information, personal data, data protection, or similar thereto.

5.7. In case that the End User wants to base the lawfulness of the processing on the consent of its Data Subjects, the End User must ensure that the consent which meets all requirements of the applicable laws, especially where the Data Subject is in the European Union and Article 6 (1) (a) GDPR applies, was given by each Data Subject of the End User prior to using the Software. The End User guarantees that consent of each Data Subject of the End User was obtained prior to the processing of personal data.

5.8. It is agreed between the Rightholder and End User that, in case of item 5.7 of this License Agreement, the End User is responsible for proving the existence of effective consent to the processing of personal data, especially according to Article 7 (1) GDPR where Data Subject is in the European Union. The End User guarantees that it is able to and will prove the existence of each Data Subject's consent at any time upon request by the Rightholder within 5 business days starting with the request of the Rightholder.

5.9. Furthermore, in case of item 5.7 of this License Agreement, the End User is obliged and has the full and sole responsibility to provide each individual Data Subject with all information required by applicable law to obtain consent, especially under Article 13 GDPR (if Data Subject is in the European Union), prior to using the Software. In particular, the End User is obliged to provide each Data Subject in the European Union, or where applicable law requires, with the Rightholder's Privacy Policy

([www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy)) prior to using the Software.

5.10. The End User shall be fully liable in relation to the Rightholder for any damage resulting from a breach of this License Agreement, in particular the End User's failure to obtain effective consent of Data Subject, where applicable, and/or from a failure to obtain sufficient effective consent and/or from the lack of proof and/or belated proof of effective consent of Data Subject and/or from any other violation of an obligation under this agreement.

5.11. The End User shall indemnify the Rightholder in relation to third parties from the claims arising from the failure of End User to fulfill obligations under Section 5 "Conditions regarding Data Processing" which third parties, especially the supervisory data protection authorities, assert against the Rightholder.

5.12. If You use the Rightholder's update servers to download the Updates, the End User, in order to increase the efficiency of the update procedure, agrees to periodically provide the Rightholder the following information: type and version of the installed software, update session ID, unique ID of the current license, and unique ID of software installation on the computer.

The Rightholder can use such information also for receiving statistical information about the distribution and use of the Rightholder's Software.

By downloading the Updates from the Rightholder's update servers, the End User gives its consent to automatically transmit the data specified in this Clause. In case the End User does not agree to provide this information to the Rightholder, the End User must obtain the Updates from a local shared folder as described in the User Manual.

## 6. Limitations

6.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and you shall not otherwise reduce any part of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Neither Software's binary code nor source may be used or reverse engineered to re-create the program algorithm, which is

proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.

6.2. You shall not transfer the rights to use the Software to any third party.

6.3. You shall not provide the activation code and/or license key file for the Extended version of the Software to third parties. The activation code and/or license key are deemed confidential data.

6.4. You shall not rent, lease or lend the Software to any third party.

6.5. You shall not use the Software in the creation of data or software used for detection, blocking or treating threats described in the User Manual.

6.6. Your key file or activation code for the Extended version of the Software can be blocked in case You breach any of the terms and conditions of this Agreement.

6.7. In case You breach the terms and conditions of this Agreement, the Rightholder shall be entitled to terminate this License with immediate effect and/or to block Your key file without being obligated to refund the purchase price or an part thereof. Such a right of termination and/or right of blocking Your key file exists, in particular, in the following cases:

- You use the Software for illegal purposes.
- You transmit or store material that infringes intellectual property rights or any other rights of third parties or is illegal, unauthorized, defamatory or offensive or invades the privacy of third parties.
- You transmit or store data owned by third parties, without obtaining beforehand the consent prescribed by law of the owner of the data to the data transmission.
- You transmit material containing software viruses or any other harmful computer codes, files or programs.
- You carry out any acts interfering with or interrupting the operation of the server or networks associated with the software.
- You make the attempt to gain unauthorized access to the computer systems or networks associated with the Software.
- You did not comply with the applicable local, state, national, international, and supranational laws and regulations or the specifications mentioned in the documentation or the related transfer documents of the authorized dealer from whom you purchased the Software.

6.8. If You are using the trial version of the Software You do not have the right to receive the Technical Support specified in Clause 4 of this Agreement and You don't have the right to transfer the license or the rights to use the Software to any third party.

6.9. Violation of the intellectual rights to the Software shall result in civil, administrative or criminal liability in accordance with the law.

## 7. Limited Warranty and Disclaimer

7.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the User Manual provided however that such limited warranty shall not apply to the following: (w) Your computer's deficiencies and related infringement for which Rightholder's expressly disclaims any warranty responsibility; (x) malfunctions, defects, or failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other third parties' or Your actions or causes beyond Rightholder's reasonable control; (y) any defect not made known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or software components installed on Your computer.

7.2. You acknowledge, accept and agree that no software is error free and You are advised to back-up the computer, with frequency and reliability suitable for You.

7.3. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the User Manual or in this Agreement.

7.4. The Rightholder does not guarantee operability of the Software after the expiration of the period specified in Clause 3.3 of this Agreement.

7.5. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clauses 2.4 and 2.5 of this Agreement.

7.6. The Rightholder does not guarantee protection from the threats described in the User Manual after the expiration of the period specified in Clauses 3.2 or 3.3 of this

Agreement or after the License to use the Software is terminated for any reason.

7.7. You acknowledge that the Software will be provisioned with Kaspersky standard settings applied by default and that it is Your sole responsibility to configure the Software to satisfy Your own requirements.

7.8. EXCEPT FOR THE GURANTEE DESCRIBED IN THIS AGREEMENT, THE SOFTWARE IS PROVIDED "AS IS" AND THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO THE RIGHTHOLDER.

7.9. EXCEPTION: In certain countries and/or jurisdictions, the exclusion of expressed or implied warranties is not permitted so that the aforementioned exclusion of liability does not apply to these countries. IN THIS CASE, THESE EXPRESSED OR IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THE GUARANTEE PERIOD IN THE RESPECTIVE COUNTRY (OR TO THE MINIMUM PERIOD REQUIRED BY APPLICABLE LAW).

## 8. Exclusion and Limitation of Liability

8.1. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE RIGHTHOLDER AND/OR ANY OF ITS PARTNERS, EVEN IF THE RIGHTHOLDER AND/OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXCLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY SUCH DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

8.2. FOR GERMAN CONSUMERS: If you are a German customer, the limitations specified in the aforementioned paragraph "Exclusion and Limitation of Liability" do not apply to you. Instead, the following provision shall apply to damages or compensation for futile expenses, for whatever legal reason, including unlawful acts:

The Rightholder shall be liable in the event of intent or gross negligence, claims according to the Product Liability Act as well as injury to life, body and health according to the German statutory provisions. The Rightholder shall not be liable for slight negligence, except for violations of essential contractual duties. In these cases, the Rightholder's liability is limited to typical, foreseeable damage. In all other cases, the Rightholder shall not be liable for slight negligence.

8.3 NOTHING IN THIS AGREEMENT IMPAIRS RIGHTS YOU HOLD ACCORDING TO A CONSUMER PROTECTION ACT OR ANY OTHER ACT IN THE COUNTRY, WHICH CANNOT BE REPEALED BY THIS AGREEMENT.

## 9. Open Source Software and Other Third Party Licenses

9.1. The Software may include some software programs that are licensed (or sublicensed) to

the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to [source@kaspersky.com](mailto:source@kaspersky.com) or the source code is supplied with the Software. If any Open Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

## 10. Intellectual Property Ownership

10.1. You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any the Trademarks or Service Marks of the Rightholder and/or its partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give you any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. The possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.

10.2. You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

## 11. Third-Party Fees

The Rightholder is not responsible for the fees charged by your data provider (e.g. Internet access provider) or your mobile service provider incurred for the use of the latter's services. Specific use of the Software requires the access to and the communication with servers of the Rightholder via the network of your service provider. In addition, they are responsible for the costs incurred in connection with the device used by you. You have to assure that your device meets with the necessary system requirements for the use of the Software, including the receipt of updates. The Rightholder is entitled to modify the requirements at any time.

## 12. Governing Law; Arbitration

12.1. This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded.

If you are an individual, this does not impair your rights according to the consumer protection of the country in which you are resident.

Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the International Commercial Arbitration Court at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such

arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 15 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

### 13. Period for Bringing Actions

13.1. No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

EXCEPTION FOR GERMAN CUSTOMERS: If you are a German individual customer, the provisions under item 16 do not apply to you.

### 14. Entire Agreement; Severability; No Waiver

14.1. This Agreement is the entire agreement between you and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms.

14.2. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent.

14.3. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Rightholder's failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

### 15. Rightholder Contact Information

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

AO Kaspersky Lab, 39A/3 Leningradskoe Shosse,  
Moscow, 125212  
Russian Federation  
E-mail: [info@kaspersky.com](mailto:info@kaspersky.com)  
Web site: [www.kaspersky.com](http://www.kaspersky.com)

## KASPERSKY LAB - PRODUCTS AND SERVICES PRIVACY POLICY

### Introduction

AO Kaspersky Lab, located at bldg. 3, 39A, Leningradskoe Shosse, Moscow, 125212, Russian Federation and all companies belonging to the group "Kaspersky Lab" respect your privacy. This Products and Services Privacy Policy (Privacy Policy) describes how we use the information you provide when you use our products and services, and the choices you can make about our use of the information. We also describe the measures we take to protect the information and how you can contact us about our privacy practices.

In connection with specific products or services offered by Kaspersky Lab, you are provided with the agreements, terms of use, and statements that supplement this policy relating to data handling.

This policy may be changed because of changes in legislation, the requirements of the authorities or to reflect changes in our practices concerning the processing of personal data. The revised policy will be posted on our website and will be effective immediately upon being posted. You can read at any time the policy currently in effect on our website: [www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy).

This version of the policy is effective as of January 1, 2019.

### The Sources of Information

Kaspersky Lab may obtain information about you from various sources, namely:



- . products and services;
- . by your signing up for a Kaspersky Lab products or services;
- . in response to technical support or other communication in order to ensure the required performance of products and services;
- . on our websites;
- . in response to marketing or other communications;
- . through participation in an offer, program or promotion.

You may also choose to consent to third parties disclosing information about you to us that those third parties have received.

#### Information Provided by Users and How We Use Information

Personal data processing by Kaspersky Lab is always carried out in a legal and fair manner.

You will always know what kind of information you provide to Kaspersky Lab before you start to use the products and services or confirm with your consent. The data which you provide depends on the services, products, and features you use. For more information about data you provide, please refer to End User License Agreement, Kaspersky Security Network Statement and other documentation of product and services that you use, especially:

#### FOR HOME USERS (B2C):

- . SECTION "B" OF THE EULA, WHICH DESCRIBES THE DATA THAT NEED TO BE PROCESSED IN ORDER TO PERFORM OBLIGATIONS UNDER THE CONTRACT;
- . KASPERSKY SECURITY NETWORK STATEMENT, WHICH DESCRIBES THE DATA THE PROCESSING OF WHICH MAY INCREASE THE REACTION SPEED OF PRODUCTS AND SERVICES IN THE EVENT OF THREATS TO INFORMATION SECURITY;
- . MARKETING STATEMENT, WHICH DESCRIBES THE DATA THE PROCESSING OF WHICH MAY IMPROVE THE PERFORMANCE OF PRODUCTS AND WILL ENABLE AN ASSESSMENT OF USER SATISFACTION REGARDING PRODUCT USE;
- . SEPARATE STATEMENTS RELATING TO SPECIFIC PRODUCT FEATURES, WHICH DESCRIBE THE DATA PROCESSED DURING THEIR USE, FOR EXAMPLE, ANTI-SPAM. YOU CAN FAMILIARIZE YOURSELF WITH SUCH STATEMENTS WHEN YOU TURN ON THE FEATURES IN THE PRODUCT.

#### FOR BUSINESS USERS (B2B):

- . SECTION "CONDITIONS REGARDING DATA PROCESSING" OF THE EULA, WHICH DESCRIBES THE DATA THAT NEED TO BE PROCESSED IN ORDER TO PERFORM OBLIGATIONS UNDER THE CONTRACT;
- . KASPERSKY SECURITY NETWORK STATEMENT, WHICH DESCRIBES THE DATA THE PROCESSING OF WHICH MAY INCREASE THE REACTION SPEED OF PRODUCTS AND SERVICES IN THE EVENT OF THREATS TO INFORMATION SECURITY. FOR SOME PRODUCTS, THE IT ADMINISTRATOR OR ANY OTHER EMPLOYEE RESPONSIBLE FOR SETTING UP THE PRODUCT CAN CHOOSE THE VOLUME OF DATA TO BE PROCESSED.

The data obtained for processing depends on the product or service, and it is recommended that users carefully read the agreements and related statements accepted during installation or usage of software or service.

Some data are non-personal, according to laws of certain countries. Regardless of the type of data and territory where data was received or processed, we use the highest standards of data protection and apply various legal, organizational, and technical measures in order to protect user data, guarantee safety and confidentiality, as well as ensure users' rights guaranteed under applicable law.

The data depends on the products and services you use, and could include the following:

- . License/ subscription information  
It is processed in order to recognize legitimate users. This data is needed to maintain communication between the product and Kaspersky Lab services - sending and receiving product databases, updates, etc.
- . Product information  
Data on the product's operation and its interaction with the user is also analyzed. For example, how long does threat scanning take? Which features are used more often than others? Answers to these and other questions help developers to improve products, making them faster and easier to use.
- . Device data

Data such as device type, operating system, etc. may be needed so the user doesn't have to buy a new license for the security product after reinstalling the operating system. This information also helps us to analyze cyberthreats, because it shows how many devices are affected by any specific threat.

. Threats detected

If a threat (new or known) is found on a device, information about that threat is sent to Kaspersky Lab. This enables us to analyze threats, their sources, principles of infection, etc., resulting in a higher quality of protection for every user.

. Information on installed applications

This information helps to create lists of 'white' or harmless applications and prevents security products from mistakenly identifying such applications as malicious. This data is also used to update and extend program categories for features like Parental Control and Application Startup Control. In addition, this information helps us to offer users security solutions that best match their needs.

. URLs visited

URLs can be sent to be checked whether they are malicious. This information also helps to create lists of 'white' or harmless websites and prevents security products from mistakenly identifying such websites as malicious. This data is also used to update and extend website categories for solutions like Kaspersky Safe Kids and provide better protection for financial transactions in such products as Kaspersky Fraud Prevention. In addition, this information helps us to offer users security solutions that best match their needs. Information about logins and passwords, if contained in the initial browser request from the user, is removed from the visited URL addresses up to the hostname or IP address. In any case, it is not Kaspersky Lab's purpose to process user logins and passwords, and Kaspersky Lab takes all reasonable and sufficient measures to avoid processing these data.

. Operating System events

New malware can often be identified only by its suspicious behavior. Because of this, the product analyzes data on processes running on the device. This makes it possible to identify early on processes that indicate malicious activity and to prevent any damaging consequences, such as the destruction of user data.

. Suspicious files and files that could be exploited by intruders

If an (as yet) unknown file, exhibiting suspicious behavior is detected on a device, it can be automatically sent for a more thorough analysis by machine learning-based technologies and, in rare cases, by a malware analyst. Personal files (such as photos or documents) are rarely malicious and do not behave suspiciously. As a result, the 'suspicious' category includes mainly executable files (.exe). For the purpose of investigating information security incidents, executable and non-executable "white files" or their parts may be sent.

. Wi-Fi connection data

This information is analyzed in order to warn users of insecure (i.e., poorly protected) Wi-Fi access points, helping to prevent personal data from being inadvertently intercepted.

. User contact data

Email addresses are used for authorization on the Kaspersky Lab web portals (My Kaspersky, Company Account, Kaspersky Endpoint Security Cloud, etc.), which enables users to manage their protection remotely. Email addresses are used to send security messages to (e.g., containing important alerts) to users of Kaspersky Lab products. Users can also choose to specify the names (or nicknames) by which they would like to be addressed on the My Kaspersky portal and in emails. Contact information is provided by users at their own discretion.

. Dump and trace files

By checking the special box in the product settings, users can also share error reports with Kaspersky Lab servers. This information helps (1) during analysis of errors that

occurred in the product and to modify it accordingly so that it will function more effectively moving forward, and (2) in the prevention and investigation of information security incidents.

. Content of your emails

During your use of the anti-spam functionality, we may receive and analyze information about emails, including content and senders to protect you from the spam and fraud. This functionality is intended to protect its users from any unwanted emails or spam. The anti-spam functionality analyzes information contained in emails reported by you as spam or as incorrectly identified as spam by the software.

. Data about stolen device

The Anti-theft feature provides certain remote access and control functions designed to protect data on your mobile phone in case of theft, as well allows you to receive information about the location of the stolen device. Anti-theft has to store data about your phone and approved users for these functions to work.

. Data for child protection feature

If a parent or holder of parental responsibility wants to use the child protection feature like Kaspersky Safe Kids, he or she can receive information about the child's device and information about the child's location. Additionally, the parent or holder of parental responsibility can configure parameters in order to block or permit specific websites and/or allow or prevent certain applications from running on the child's device. Kaspersky Lab does not collect children's data beyond the framework of such feature.

KASPERSKY LAB WILL ONLY PROCESS PERSONAL DATA FOR PARTICULAR, PRE-DETERMINED PURPOSES THAT ARE LEGITIMATE WITH REGARD TO APPLICABLE LAW, AND THAT ARE RELEVANT TO KASPERSKY LAB'S BUSINESS.

. To ensure the performance of a contract with users and to ensure the required performance of products and services for customers.

. To protect the user from known threats to information security.

. To verify that the license is legal.

. To update the anti-virus databases;

. To increase the effectiveness of the protection of your computer, in particular to provide a faster response to new information and network security threats, to increase the effectiveness of the performance of the software's protection component, to decrease the probability of false positive.

. To improve user interaction and experience with our products and services, in particular changing interfaces and providing the desired content and advertisement, related to Marketing purpose.

. To provide technical support of products and services for customers and to improve the quality of products and services.

Kaspersky Lab will retain personal data for as long as necessary to fulfill the purpose for which the data is processed in accordance with the objectives specified in the agreements (KSN statements, EULAs, consents), or to comply with applicable legal requirements.

LIMITATION OR RESTRICTION DATA PROCESSING

IF YOU CHOOSE NOT TO PROVIDE DATA THAT IS NECESSARY IN ORDER FOR A PRODUCT OR FEATURE TO WORK, YOU MAY NOT BE ABLE TO USE THAT PRODUCT OR FEATURE. THIS OBLIGATORY DATA IS LISTED IN THE END USER LICENSE AGREEMENT. THE KASPERSKY SECURITY NETWORK STATEMENT OR MARKETING STATEMENT CONTAINS A LIST OF DATA THAT USERS CAN DECIDE TO PROVIDE TO US AT ANY TIME BY CHECKING THE CORRESPONDING BOX IN THE PRODUCT SETTINGS (THEY CAN ALSO REVERSE THIS DECISION WHENEVER THEY CHOOSE).

What we aren't going to process

Through its products and services, Kaspersky Lab never process "sensitive" personal data such as religion, political views, sexual preference, or health, or other special categories of personal data. We do not wish to receive any such data and will not request it from you.

Kaspersky Lab's products must be installed and used by an adult. Children may use the device where Kaspersky Lab's product was installed only with permission from their parents or holder of parental responsibility. Except for "Data for child protection feature", we

do not intend to process personal data of children, nor do we want to receive such personal information of children.

Where we process Information

The personal data provided by users to Kaspersky Lab can be processed in the following countries, including countries outside European Union (EU) or the European Economic Area (EEA):

Within the EU or EEA:

- . Germany
- . Netherlands
- . France
- . United Kingdom

Outside of the EU or EEA:

- . Switzerland
- . Canada
- . Singapore
- . Russia
- . Japan
- . USA
- . Mexico
- . China
- . Azerbaijan

The list of countries where the data provided by the user may be processed can change. You can acquaint yourself with the current list of countries in the version of the Privacy Policy on the website [www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy).

According to our general business practice, the data received from users in the EU are processed on servers located in the EU and Russia.

The personal data may be processed at destinations outside the European Union (EU) or the European Economic Area (EEA) some of which have not been determined by the European Commission to have an adequate level of data protection. It may also be processed by staff operating outside EU or EEA who work for us or for one of our suppliers.

Whenever data is processed, we use the highest level of standards for data protection and apply a variety of legal measures in order to protect user data, guarantee safety and confidentiality, and ensure users' rights. To learn more about the European Commission's decisions on the adequacy of the protection of personal data in the countries where Kaspersky Lab processes data, please visit: [ec.europa.eu/justice/data-protection/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm)

Provision of Information

We never provide data or access to them for state organization or third parties. We may only disclose the Information as follows:

- . Within the Group of Companies Kaspersky Lab. Data can be shared.
- . Service Providers. We also may share your information with vendors that provide services to us, including companies that provide web analytics, data processing, advertising, e-mail distribution, payment processing, order fulfillment, and other services.

Please note that some of our products, for example Kaspersky Secure Connection, include applications of third parties whose privacy practices differ from Kaspersky Lab's. If you provide personal data to any of those applications, your data is governed by their privacy statements. You are responsible for acquainting yourself with the data processing rules and procedures described in the relevant privacy statements.

Your Rights and Options

You have certain rights regarding your personal data. We also offer you certain options about what personal data you provide to us, how we use that information, and how we communicate with you.

In most cases you can choose not to provide personal data to us when you use Kaspersky Lab's products, services, and websites. You may also refrain from submitting information directly to us. However, if you do not provide personal data when requested, you may not be able to benefit from the full range of Kaspersky Lab products and services and we may

not be able to provide you with information about products, services, and promotions. You can at any time choose not to receive marketing communications by e-mail by clicking on the unsubscribe link within the marketing e-mails you receive from us. If your employer provides your personal data to Kaspersky Lab, you may have certain options with respect to Kaspersky Lab's use or disclosure of the information. Please contact your employer to learn about and to exercise your options.

To the extent provided by applicable law, you may withdraw any consent you previously provided to us, or object at any time on legitimate grounds, to the processing of your personal data. We will apply your preferences going forward. In some circumstances, withdrawing your consent to Kaspersky Lab's use or disclosure of your personal data will mean that you cannot take advantage of certain Kaspersky Lab products or services. Subject to applicable law, you may have the right to: obtain confirmation that we hold personal data about you, request access to and receive information about your personal data, receive copies of your personal data that you provided to us, also in a machine-readable format and have it sent to another data controller, where technically possible, update and correct inaccuracies in your personal data, object to the processing of your personal data, have the information blocked, anonymized or deleted, as appropriate, as well as lodge a complaint with a supervisory authority. The right to access personal data may be limited in some circumstances by the requirements of local law. To exercise rights that depend on action from Kaspersky Lab, please contact us as set forth below.

If you provide us with any information or material relating to another individual, you should make sure that this sharing with us and our further use as described to you from time to time is in line with applicable laws; thus, for example, you should duly inform that individual about the processing of her/his personal data and obtain her/his consent, as may be necessary under applicable laws.

If we fall short of your expectations in processing your personal data or you wish to make a complaint about our privacy practices, please relate this to us, as it gives us an opportunity to fix the problem. You may contact us by using the contact details provided in the "How to Contact Us" section below. To assist us in responding to your request, please give full details of the issue. We attempt to review and respond to all complaints within a reasonable time.

#### The Privacy Principles

Personal data processing at Kaspersky Lab is based on the following principles:  
Consent and choice

- . Presenting to the users the choice whether or not to allow the processing of their personal data except where the users cannot freely withhold consent or where applicable law specifically allows the processing of personal data without the natural person's consent. The user's election must be freely given, specific and made on a knowledgeable basis;

- . Informing users, before obtaining consent, about their rights under the individual participation and access principle;

- . Providing users, before obtaining consent, with the information indicated by the openness, transparency and notice principle; and

- . Explaining to users the implications of granting or withholding consent.

#### Purpose legitimacy and specification

- . Ensuring that the purpose(s) complies with applicable law and relies on a permissible legal basis;

- . Communicating the purpose(s) to users before the information is used for the first time for a new purpose;

- . Using language for this specification which is both clear and appropriately adapted to the circumstances;

#### Data processing limitation

- . Limiting the gathering of personal data to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s).

- . Deleting and disposing of personal data whenever the purpose for personal data processing has expired, there are no legal requirements to keep the personal data, or whenever it is practical to do so.

#### Use, retention and disclosure limitation

- . Limiting the use, retention and disclosure of personal data to that which is

necessary in order to fulfil specific, explicit and legitimate purposes;

- . Limiting the use of personal data to the purposes specified by Kaspersky Lab prior to receiving the data, unless a different purpose is explicitly required by applicable law;

- . Retaining personal data only as long as necessary to fulfill the stated purposes, and thereafter securely destroying or anonymizing it; and

- . Locking (i.e. archiving, securing and exempting the personal data from further processing) any personal data when and for as long as the stated purposes have expired, but where retention is required by applicable laws.

#### Accuracy and quality

- . Ensuring that the personal data processed is accurate, complete, up-to-date (unless there is a legitimate basis for keeping outdated data), adequate and relevant for the purpose of use;

- . Ensuring the reliability of personal data provided from a source other than from users before it is processed;

- . Verifying, through appropriate means, the validity and correctness of the claims made by the user prior to making any changes to the personal data (in order to ensure that the changes are properly authorized), where it is appropriate to do so;

- . Establishing personal data processing procedures to help ensure accuracy and quality; and

- . Establishing control mechanisms to periodically check the accuracy and quality of personal data processing.

#### Openness, transparency and notice

- . Providing users with clear and easily accessible information about Kaspersky Lab's policies;

- . Establishing procedures and practices with respect to the processing of personal data;

- . Including in notices the fact that personal data is being processed, the purpose for which this is done, the types of privacy stakeholders to whom the personal data might be disclosed, and the identity of the entity which determines the above and on how to contact;

- . Disclosing the options and means offered by Kaspersky Lab to users for the purposes of limiting the processing of, and for accessing, correcting and removing their information;

- . Giving notice to users when major changes in the personal data handling procedures occur.

#### Individual participation and access

- . Giving users the ability to contact us (by using the contact details provided in the "How to Contact Us") and review their personal data, provided their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law;

- . Allowing users (by using the contact details provided in the "How to Contact Us" or by using interface of our products and services) to challenge the accuracy and completeness of the personal data and have it amended, corrected or removed as appropriate and possible in the specific context;

- . Providing any amendment, correction or removal to personal data processors and third parties to whom personal data had been disclosed, where they are known; and

- . Establishing procedures to enable users to exercise these rights in a simple, fast and efficient way, which does not entail undue delay or cost.

#### Information Security: How We Protect Your Privacy

Information security is Kaspersky Lab's core business. All data and all information provided by you is confidential by default. Kaspersky Lab will therefore always apply technical and organizational data security measures for the protection of personal data that are adequate and appropriate, taking into account the concrete risks resulting from the processing of personal data as well as up-to-date security standards and procedures. In order to, among other reasons, identify and fulfill the appropriate level of protection, Kaspersky Lab classifies processing systems with personal data and implements cascading sets of protective measures.

Kaspersky Lab also maintains physical, electronic and procedural safeguards to protect the

information against loss, misuse, damage or modification and unauthorized access or disclosure. Some of the other central features of our information security program are:

- . The Information Security Department, which designs, implements and provides oversight to our information security program;
- . A determination of personal data safety hazards in the course of processing in a Kaspersky Lab processing system;
- . Application of appropriate information security tools;
- . Performance evaluation of applied personal data security measures before commissioning processing systems;
- . Implementing controls to identify, authenticate and authorize access to various services or websites;
- . Discovering the facts surrounding unauthorized access to personal data and adopting corresponding measures;
- . Recovery of personal data that was modified or destructed;
- . Establishing access rules to personal data processed in Kaspersky Lab processing systems and also recording and accounting for all actions undertaken with personal data in these systems;
- . Encryption between our clients and servers (and between our various data centers);
- . We restrict access of our employees and contractors who need to know the information in order to process it for us and who are subject to strict contractual confidentiality obligations, to personal information. They may be disciplined or their contract terminated if they fail to meet these obligations;
- . Monitoring of our systems infrastructure to detect weaknesses and potential intrusions;
- . Monitoring measures taken to ensure the security of personal data;
- . Providing Kaspersky Lab personnel with relevant training and continually updating our security practices in light of new risks and developments in technology.

#### How to Contact Us

If you have any questions or comments about this Privacy Policy, Kaspersky Lab's privacy practices or if you would like us to update or remove information or preferences you provided to us, please visit <https://www.kaspersky.com/global-privacy-policy>, or, according to point (a) of Article 13 (1) and Article 27 (1) of Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR"), you may contact our Kaspersky Lab EU representative via e-mail or phone: Kaspersky Labs GmbH, Ingolstadt, Germany, [info@kaspersky.de](mailto:info@kaspersky.de), +49 (0) 841 98 18 90.

Kaspersky Security Center 11 Web Console, iOS MDM Server, Microsoft Exchange Mobile Devices Server, Administration Console KASPERSKY LAB END USER LICENSE AGREEMENTS; AND Products and Services PRIVACY POLICY

BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR BY USING THE SOFTWARE YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE OR DO NOT USE THE SOFTWARE.

IF LICENSE CONTRACT OR SIMILAR DOCUMENT ACCOMPANIES SOFTWARE, TERMS OF THE SOFTWARE USE DEFINED IN SUCH DOCUMENT PREVAIL OVER CURRENT END USER LICENSE AGREEMENT.

#### 1. Definitions

1.1. Software means software Kaspersky Security Center 11 Web Console, iOS MDM Server, Microsoft Exchange Mobile Devices Server, Administration Console including any Updates and related materials.

1.2. Rightholder (owner of all rights, whether exclusive or otherwise to the Software) means AO Kaspersky Lab, a company incorporated according to the laws of the Russian Federation.

1.3. Computer(s) means combination of hardware(s), including personal computers, laptops, workstations, personal digital assistants, 'smart phones', hand-held devices, or other electronic devices, and operating system(s) (including system virtual machines) for which

the Software was designed where the Software will be installed and/or used.

1.4. End User (You/Your) means the organization for which the Software is downloaded or installed and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term "organization", without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority. If the Software was downloaded or installed on behalf of individual, End User ("You") further means such individual.

1.5. Partner(s) means organizations or individual(s), who distributes the Software based on an agreement and license with the Rightholder.

1.6. Update(s) means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance packs etc.

1.7. User Manual means user manual, administrator guide, reference book and related explanatory or other materials.

## 2. Grant of License

2.1. You are given a non-exclusive license to store, load, install, execute, and display (to "use") the free of charge Software, according to the all technical requirements described in the User Manual and according to the terms and conditions of this Agreement (the "License").

2.2. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software.

## 3. Term and termination

3.1. The Software can be used perpetually upon your acceptance of this Agreement.

3.2. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License.

3.3. You agree that in using the Software and in using any report or information derived as a result of using this Software, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.

## 4. Technical Support

4.1. Technical Support is provided only for clients of the commercial versions of the Rightholder's software in accordance with the Technical Support rules.

Technical support service and its rules are located at: <http://support.kaspersky.com>.

## 5. Limitations

5.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and you shall not otherwise reduce any part of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Neither Software's binary code nor source code may be used or reverse engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.

5.2. You shall not transfer the rights to use the Software to any third party.

5.3. You shall not rent, lease or lend the Software to any third party.

5.4. You shall not use the Software in the creation of data or software used for detection, blocking or treating threats described in the User Manual.

5.5. Violation of the intellectual rights to the Software shall result in civil, administrative or criminal liability in accordance with the law.

## 6. Limited Warranty and Disclaimer



6.1. THE SOFTWARE IS PROVIDED "AS IS" AND AO KASPERSKY LAB MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW AO KASPERSKY LAB AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESS OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, AO KASPERSKY LAB MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO THE RIGHTHOLDER.

## 7. Exclusion and Limitation of Liability

7.1. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE RIGHTHOLDER AND/OR ANY OF ITS PARTNERS, EVEN IF THE RIGHTHOLDER AND/OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

YOU AGREE THAT IN THE EVENT THE RIGHTHOLDER AND/OR ITS PARTNERS ARE FOUND LIABLE, THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS SHALL BE LIMITED BY THE COSTS OF THE SOFTWARE. IN NO CASE SHALL THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS EXCEED THE FEES PAID FOR THE SOFTWARE TO THE RIGHTHOLDER OR THE PARTNER (AS MAY BE APPLICABLE).

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXCLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY SUCH DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

## 8. GNU and Other Third-Party Licenses

8.1. The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code "Open-Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com or the source code is supplied with the Software. If any Open-Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open-Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

## 9. Intellectual Property Ownership

9.1. You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States of America, as well as other

countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any trademarks or service marks of the Rightholder and/or its partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give you any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.

9.2. You acknowledge that the source code is proprietary to the Rightholder and constitutes trade secrets of the Rightholder. You agree not to modify, adapt, translate, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software in any way.

9.3. You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

## 10. Governing Law; Arbitration

10.1. This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded.

If you are an individual, this does not impair your rights according to the consumer protection of the country in which you are resident.

Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the International Commercial Arbitration Court at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 11 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

## 11. Period for Bringing Actions

11.1. No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

## 12. Entire Agreement; Severability; No Waiver

12.1. This Agreement is the entire agreement between you and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Rightholder's

failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

### 13. Rightholder Contact Information

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

AO Kaspersky Lab, 39A/3, Leningradskoe Shosse  
Moscow, 125212  
Russian Federation  
E-mail: [info@kaspersky.com](mailto:info@kaspersky.com)  
Web site: [www.kaspersky.com](http://www.kaspersky.com)

### KASPERSKY LAB - PRODUCTS AND SERVICES PRIVACY POLICY

#### Introduction

AO Kaspersky Lab, located at bldg. 3, 39A, Leningradskoe Shosse, Moscow, 125212, Russian Federation and all companies belonging to the group "Kaspersky Lab" respect your privacy. This Products and Services Privacy Policy (Privacy Policy) describes how we use the information you provide when you use our products and services, and the choices you can make about our use of the information. We also describe the measures we take to protect the information and how you can contact us about our privacy practices.

In connection with specific products or services offered by Kaspersky Lab, you are provided with the agreements, terms of use, and statements that supplement this policy relating to data handling.

This policy may be changed because of changes in legislation, the requirements of the authorities or to reflect changes in our practices concerning the processing of personal data. The revised policy will be posted on our website and will be effective immediately upon being posted. You can read at any time the policy currently in effect on our website: [www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy).

This version of the policy is effective as of January 1, 2019.

#### The Sources of Information

Kaspersky Lab may obtain information about you from various sources, namely:

- . products and services;
- . by your signing up for a Kaspersky Lab products or services;
- . in response to technical support or other communication in order to ensure the required performance of products and services;
- . on our websites;
- . in response to marketing or other communications;
- . through participation in an offer, program or promotion.

You may also choose to consent to third parties disclosing information about you to us that those third parties have received.

#### Information Provided by Users and How We Use Information

Personal data processing by Kaspersky Lab is always carried out in a legal and fair manner.

You will always know what kind of information you provide to Kaspersky Lab before you start to use the products and services or confirm with your consent. The data which you provide depends on the services, products, and features you use. For more information about data you provide, please refer to End User License Agreement, Kaspersky Security Network Statement and other documentation of product and services that you use, especially:

#### FOR HOME USERS (B2C):

- . SECTION "B" OF THE EULA, WHICH DESCRIBES THE DATA THAT NEED TO BE PROCESSED IN ORDER TO PERFORM OBLIGATIONS UNDER THE CONTRACT;
- . KASPERSKY SECURITY NETWORK STATEMENT, WHICH DESCRIBES THE DATA THE PROCESSING OF WHICH MAY INCREASE THE REACTION SPEED OF PRODUCTS AND SERVICES IN THE EVENT OF THREATS TO INFORMATION SECURITY;
- . MARKETING STATEMENT, WHICH DESCRIBES THE DATA THE PROCESSING OF WHICH MAY IMPROVE THE PERFORMANCE OF PRODUCTS AND WILL ENABLE AN ASSESSMENT OF USER SATISFACTION REGARDING PRODUCT USE;

. SEPARATE STATEMENTS RELATING TO SPECIFIC PRODUCT FEATURES, WHICH DESCRIBE THE DATA PROCESSED DURING THEIR USE, FOR EXAMPLE, ANTI-SPAM. YOU CAN FAMILIARIZE YOURSELF WITH SUCH STATEMENTS WHEN YOU TURN ON THE FEATURES IN THE PRODUCT.

FOR BUSINESS USERS (B2B):

. SECTION "CONDITIONS REGARDING DATA PROCESSING" OF THE EULA, WHICH DESCRIBES THE DATA THAT NEED TO BE PROCESSED IN ORDER TO PERFORM OBLIGATIONS UNDER THE CONTRACT;

. KASPERSKY SECURITY NETWORK STATEMENT, WHICH DESCRIBES THE DATA THE PROCESSING OF WHICH MAY INCREASE THE REACTION SPEED OF PRODUCTS AND SERVICES IN THE EVENT OF THREATS TO INFORMATION SECURITY. FOR SOME PRODUCTS, THE IT ADMINISTRATOR OR ANY OTHER EMPLOYEE RESPONSIBLE FOR SETTING UP THE PRODUCT CAN CHOOSE THE VOLUME OF DATA TO BE PROCESSED.

The data obtained for processing depends on the product or service, and it is recommended that users carefully read the agreements and related statements accepted during installation or usage of software or service.

Some data are non-personal, according to laws of certain countries. Regardless of the type of data and territory where data was received or processed, we use the highest standards of data protection and apply various legal, organizational, and technical measures in order to protect user data, guarantee safety and confidentiality, as well as ensure users' rights guaranteed under applicable law.

The data depends on the products and services you use, and could include the following:

. License/ subscription information

It is processed in order to recognize legitimate users. This data is needed to maintain communication between the product and Kaspersky Lab services - sending and receiving product databases, updates, etc.

. Product information

Data on the product's operation and its interaction with the user is also analyzed. For example, how long does threat scanning take? Which features are used more often than others? Answers to these and other questions help developers to improve products, making them faster and easier to use.

. Device data

Data such as device type, operating system, etc. may be needed so the user doesn't have to buy a new license for the security product after reinstalling the operating system. This information also helps us to analyze cyberthreats, because it shows how many devices are affected by any specific threat.

. Threats detected

If a threat (new or known) is found on a device, information about that threat is sent to Kaspersky Lab. This enables us to analyze threats, their sources, principles of infection, etc., resulting in a higher quality of protection for every user.

. Information on installed applications

This information helps to create lists of 'white' or harmless applications and prevents security products from mistakenly identifying such applications as malicious. This data is also used to update and extend program categories for features like Parental Control and Application Startup Control. In addition, this information helps us to offer users security solutions that best match their needs.

. URLs visited

URLs can be sent to be checked whether they are malicious. This information also helps to create lists of 'white' or harmless websites and prevents security products from mistakenly identifying such websites as malicious. This data is also used to update and extend website categories for solutions like Kaspersky Safe Kids and provide better protection for financial transactions in such products as Kaspersky Fraud Prevention. In addition, this information helps us to offer users security solutions that best match their needs. Information about logins and passwords, if contained in the initial browser request from the user, is removed from the visited URL addresses up to the hostname or IP address. In any case, it is not Kaspersky Lab's purpose to process user logins and passwords, and Kaspersky Lab takes all reasonable and sufficient measures to avoid

processing these data.

. Operating System events

New malware can often be identified only by its suspicious behavior. Because of this, the product analyzes data on processes running on the device. This makes it possible to identify early on processes that indicate malicious activity and to prevent any damaging consequences, such as the destruction of user data.

. Suspicious files and files that could be exploited by intruders

If an (as yet) unknown file, exhibiting suspicious behavior is detected on a device, it can be automatically sent for a more thorough analysis by machine learning-based technologies and, in rare cases, by a malware analyst. Personal files (such as photos or documents) are rarely malicious and do not behave suspiciously. As a result, the 'suspicious' category includes mainly executable files (.exe). For the purpose of investigating information security incidents, executable and non-executable "white files" or their parts may be sent.

. Wi-Fi connection data

This information is analyzed in order to warn users of insecure (i.e., poorly protected) Wi-Fi access points, helping to prevent personal data from being inadvertently intercepted.

. User contact data

Email addresses are used for authorization on the Kaspersky Lab web portals (My Kaspersky, Company Account, Kaspersky Endpoint Security Cloud, etc.), which enables users to manage their protection remotely. Email addresses are used to send security messages to (e.g., containing important alerts) to users of Kaspersky Lab products. Users can also choose to specify the names (or nicknames) by which they would like to be addressed on the My Kaspersky portal and in emails. Contact information is provided by users at their own discretion.

. Dump and trace files

By checking the special box in the product settings, users can also share error reports with Kaspersky Lab servers. This information helps (1) during analysis of errors that occurred in the product and to modify it accordingly so that it will function more effectively moving forward, and (2) in the prevention and investigation of information security incidents.

. Content of your emails

During your use of the anti-spam functionality, we may receive and analyze information about emails, including content and senders to protect you from the spam and fraud. This functionality is intended to protect its users from any unwanted emails or spam. The anti-spam functionality analyzes information contained in emails reported by you as spam or as incorrectly identified as spam by the software.

. Data about stolen device

The Anti-theft feature provides certain remote access and control functions designed to protect data on your mobile phone in case of theft, as well allows you to receive information about the location of the stolen device. Anti-theft has to store data about your phone and approved users for these functions to work.

. Data for child protection feature

If a parent or holder of parental responsibility wants to use the child protection feature like Kaspersky Safe Kids, he or she can receive information about the child's device and information about the child's location. Additionally, the parent or holder of parental responsibility can configure parameters in order to block or permit specific websites and/or allow or prevent certain applications from running on the child's device. Kaspersky Lab does not collect children's data beyond the framework of such feature.

KASPERSKY LAB WILL ONLY PROCESS PERSONAL DATA FOR PARTICULAR, PRE-DETERMINED PURPOSES THAT ARE LEGITIMATE WITH REGARD TO APPLICABLE LAW, AND THAT ARE RELEVANT TO KASPERSKY LAB'S BUSINESS.

- . To ensure the performance of a contract with users and to ensure the required performance of products and services for customers.
- . To protect the user from known threats to information security.
- . To verify that the license is legal.
- . To update the anti-virus databases;
- . To increase the effectiveness of the protection of your computer, in particular to provide a faster response to new information and network security threats, to increase the effectiveness of the performance of the software's protection component, to decrease the probability of false positive.
- . To improve user interaction and experience with our products and services, in particular changing interfaces and providing the desired content and advertisement, related to Marketing purpose.
- . To provide technical support of products and services for customers and to improve the quality of products and services.

Kaspersky Lab will retain personal data for as long as necessary to fulfill the purpose for which the data is processed in accordance with the objectives specified in the agreements (KSN statements, EULAs, consents), or to comply with applicable legal requirements.

#### LIMITATION OR RESTRICTION DATA PROCESSING

IF YOU CHOOSE NOT TO PROVIDE DATA THAT IS NECESSARY IN ORDER FOR A PRODUCT OR FEATURE TO WORK, YOU MAY NOT BE ABLE TO USE THAT PRODUCT OR FEATURE. THIS OBLIGATORY DATA IS LISTED IN THE END USER LICENSE AGREEMENT. THE KASPERSKY SECURITY NETWORK STATEMENT OR MARKETING STATEMENT CONTAINS A LIST OF DATA THAT USERS CAN DECIDE TO PROVIDE TO US AT ANY TIME BY CHECKING THE CORRESPONDING BOX IN THE PRODUCT SETTINGS (THEY CAN ALSO REVERSE THIS DECISION WHENEVER THEY CHOOSE).

What we aren't going to process

Through its products and services, Kaspersky Lab never process "sensitive" personal data such as religion, political views, sexual preference, or health, or other special categories of personal data. We do not wish to receive any such data and will not request it from you.

Kaspersky Lab's products must be installed and used by an adult. Children may use the device where Kaspersky Lab's product was installed only with permission from their parents or holder of parental responsibility. Except for "Data for child protection feature", we do not intend to process personal data of children, nor do we want to receive such personal information of children.

Where we process Information

The personal data provided by users to Kaspersky Lab can be processed in the following countries, including countries outside European Union (EU) or the European Economic Area (EEA):

Within the EU or EEA:

- . Germany
- . Netherlands
- . France
- . United Kingdom

Outside of the EU or EEA:

- . Switzerland
- . Canada
- . Singapore
- . Russia
- . Japan
- . USA
- . Mexico
- . China
- . Azerbaijan

The list of countries where the data provided by the user may be processed can change. You can acquaint yourself with the current list of countries in the version of the Privacy Policy on the website [www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy).

According to our general business practice, the data received from users in the EU are processed on servers located in the EU and Russia. The personal data may be processed at destinations outside the European Union (EU) or the European Economic Area (EEA) some of which have not been determined by the European Commission to have an adequate level of data protection. It may also be processed by staff operating outside EU or EEA who work for us or for one of our suppliers. Whenever data is processed, we use the highest level of standards for data protection and apply a variety of legal measures in order to protect user data, guarantee safety and confidentiality, and ensure users' rights. To learn more about the European Commission's decisions on the adequacy of the protection of personal data in the countries where Kaspersky Lab processes data, please visit: [ec.europa.eu/justice/data-protection/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm)

#### Provision of Information

We never provide data or access to them for state organization or third parties. We may only disclose the Information as follows:

- . Within the Group of Companies Kaspersky Lab. Data can be shared.
- . Service Providers. We also may share your information with vendors that provide services to us, including companies that provide web analytics, data processing, advertising, e-mail distribution, payment processing, order fulfillment, and other services.

Please note that some of our products, for example Kaspersky Secure Connection, include applications of third parties whose privacy practices differ from Kaspersky Lab's. If you provide personal data to any of those applications, your data is governed by their privacy statements. You are responsible for acquainting yourself with the data processing rules and procedures described in the relevant privacy statements.

#### Your Rights and Options

You have certain rights regarding your personal data. We also offer you certain options about what personal data you provide to us, how we use that information, and how we communicate with you.

In most cases you can choose not to provide personal data to us when you use Kaspersky Lab's products, services, and websites. You may also refrain from submitting information directly to us. However, if you do not provide personal data when requested, you may not be able to benefit from the full range of Kaspersky Lab products and services and we may not be able to provide you with information about products, services, and promotions. You can at any time choose not to receive marketing communications by e-mail by clicking on the unsubscribe link within the marketing e-mails you receive from us.

If your employer provides your personal data to Kaspersky Lab, you may have certain options with respect to Kaspersky Lab's use or disclosure of the information. Please contact your employer to learn about and to exercise your options.

To the extent provided by applicable law, you may withdraw any consent you previously provided to us, or object at any time on legitimate grounds, to the processing of your personal data. We will apply your preferences going forward. In some circumstances, withdrawing your consent to Kaspersky Lab's use or disclosure of your personal data will mean that you cannot take advantage of certain Kaspersky Lab products or services.

Subject to applicable law, you may have the right to: obtain confirmation that we hold personal data about you, request access to and receive information about your personal data, receive copies of your personal data that you provided to us, also in a machine-readable format and have it sent to another data controller, where technically possible, update and correct inaccuracies in your personal data, object to the processing of your personal data, have the information blocked, anonymized or deleted, as appropriate, as well as lodge a complaint with a supervisory authority. The right to access personal data may be limited in some circumstances by the requirements of local law. To exercise rights that depend on action from Kaspersky Lab, please contact us as set forth below.

If you provide us with any information or material relating to another individual, you should make sure that this sharing with us and our further use as described to you from time to time is in line with applicable laws; thus, for example, you should duly inform that individual about the processing of her/his personal data and obtain her/his consent, as may be necessary under applicable laws.

If we fall short of your expectations in processing your personal data or you wish to make a complaint about our privacy practices, please relate this to us, as it gives us an opportunity to fix the problem. You may contact us by using the contact details provided

in the "How to Contact Us" section below. To assist us in responding to your request, please give full details of the issue. We attempt to review and respond to all complaints within a reasonable time.

#### The Privacy Principles

Personal data processing at Kaspersky Lab is based on the following principles:

##### Consent and choice

- . Presenting to the users the choice whether or not to allow the processing of their personal data except where the users cannot freely withhold consent or where applicable law specifically allows the processing of personal data without the natural person's consent. The user's election must be freely given, specific and made on a knowledgeable basis;
- . Informing users, before obtaining consent, about their rights under the individual participation and access principle;
- . Providing users, before obtaining consent, with the information indicated by the openness, transparency and notice principle; and
- . Explaining to users the implications of granting or withholding consent.

##### Purpose legitimacy and specification

- . Ensuring that the purpose(s) complies with applicable law and relies on a permissible legal basis;
- . Communicating the purpose(s) to users before the information is used for the first time for a new purpose;
- . Using language for this specification which is both clear and appropriately adapted to the circumstances;

##### Data processing limitation

- . Limiting the gathering of personal data to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s).
- . Deleting and disposing of personal data whenever the purpose for personal data processing has expired, there are no legal requirements to keep the personal data, or whenever it is practical to do so.

##### Use, retention and disclosure limitation

- . Limiting the use, retention and disclosure of personal data to that which is necessary in order to fulfil specific, explicit and legitimate purposes;
- . Limiting the use of personal data to the purposes specified by Kaspersky Lab prior to receiving the data, unless a different purpose is explicitly required by applicable law;
- . Retaining personal data only as long as necessary to fulfill the stated purposes, and thereafter securely destroying or anonymizing it; and
- . Locking (i.e. archiving, securing and exempting the personal data from further processing) any personal data when and for as long as the stated purposes have expired, but where retention is required by applicable laws.

##### Accuracy and quality

- . Ensuring that the personal data processed is accurate, complete, up-to-date (unless there is a legitimate basis for keeping outdated data), adequate and relevant for the purpose of use;
- . Ensuring the reliability of personal data provided from a source other than from users before it is processed;
- . Verifying, through appropriate means, the validity and correctness of the claims made by the user prior to making any changes to the personal data (in order to ensure that the changes are properly authorized), where it is appropriate to do so;
- . Establishing personal data processing procedures to help ensure accuracy and quality; and
- . Establishing control mechanisms to periodically check the accuracy and quality of personal data processing.

##### Openness, transparency and notice

- . Providing users with clear and easily accessible information about Kaspersky Lab's policies;
- . Establishing procedures and practices with respect to the processing of personal



data;

- . Including in notices the fact that personal data is being processed, the purpose for which this is done, the types of privacy stakeholders to whom the personal data might be disclosed, and the identity of the entity which determines the above and on how to contact;

- . Disclosing the options and means offered by Kaspersky Lab to users for the purposes of limiting the processing of, and for accessing, correcting and removing their information;

- . Giving notice to users when major changes in the personal data handling procedures occur.

#### Individual participation and access

- . Giving users the ability to contact us (by using the contact details provided in the "How to Contact Us") and review their personal data, provided their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law;

- . Allowing users (by using the contact details provided in the "How to Contact Us" or by using interface of our products and services) to challenge the accuracy and completeness of the personal data and have it amended, corrected or removed as appropriate and possible in the specific context;

- . Providing any amendment, correction or removal to personal data processors and third parties to whom personal data had been disclosed, where they are known; and

- . Establishing procedures to enable users to exercise these rights in a simple, fast and efficient way, which does not entail undue delay or cost.

#### Information Security: How We Protect Your Privacy

Information security is Kaspersky Lab's core business. All data and all information provided by you is confidential by default. Kaspersky Lab will therefore always apply technical and organizational data security measures for the protection of personal data that are adequate and appropriate, taking into account the concrete risks resulting from the processing of personal data as well as up-to-date security standards and procedures. In order to, among other reasons, identify and fulfill the appropriate level of protection, Kaspersky Lab classifies processing systems with personal data and implements cascading sets of protective measures.

Kaspersky Lab also maintains physical, electronic and procedural safeguards to protect the information against loss, misuse, damage or modification and unauthorized access or disclosure. Some of the other central features of our information security program are:

- . The Information Security Department, which designs, implements and provides oversight to our information security program;

- . A determination of personal data safety hazards in the course of processing in a Kaspersky Lab processing system;

- . Application of appropriate information security tools;

- . Performance evaluation of applied personal data security measures before commissioning processing systems;

- . Implementing controls to identify, authenticate and authorize access to various services or websites;

- . Discovering the facts surrounding unauthorized access to personal data and adopting corresponding measures;

- . Recovery of personal data that was modified or destructed;

- . Establishing access rules to personal data processed in Kaspersky Lab processing systems and also recording and accounting for all actions undertaken with personal data in these systems;

- . Encryption between our clients and servers (and between our various data centers);

- . We restrict access of our employees and contractors who need to know the information in order to process it for us and who are subject to strict contractual confidentiality obligations, to personal information. They may be disciplined or their contract terminated if they fail to meet these obligations;

- . Monitoring of our systems infrastructure to detect weaknesses and potential intrusions;

- . Monitoring measures taken to ensure the security of personal data;

- . Providing Kaspersky Lab personnel with relevant training and continually updating our security practices in light of new risks and developments in technology.

#### How to Contact Us

If you have any questions or comments about this Privacy Policy, Kaspersky Lab's privacy practices or if you would like us to update or remove information or preferences you provided to us, please visit <https://www.kaspersky.com/global-privacy-policy>, or, according to point (a) of Article 13 (1) and Article 27 (1) of Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR"), you may contact our Kaspersky Lab EU representative via e-mail or phone: Kaspersky Labs GmbH, Ingolstadt, Germany, [info@kaspersky.de](mailto:info@kaspersky.de), +49 (0) 841 98 18 90.

Kaspersky Endpoint Security for Linux END USER LICENSE AGREEMENT; AND  
Products and Services PRIVACY POLICY

KASPERSKY LAB END USER LICENSE AGREEMENT ("LICENSE AGREEMENT")

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

CLICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE WINDOW CONTAINING THE LICENSE AGREEMENT, OR BY ENTERING CORRESPONDING SYMBOL(-S), YOU CONFIRM IN A LEGALLY BINDING WAY THAT YOU AS THE ORGANIZATION FOR WHICH THE SOFTWARE IS DOWNLOADED OR ACQUIRED HAVE AUTHORIZED THE NATURAL PERSON ACCEPTING THIS LICENSE AGREEMENT TO ENTER INTO THIS LICENSE AGREEMENT FOR AND ON BEHALF OF YOU. FURTHERMORE, YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS LICENSE AGREEMENT AND AGREE THAT THIS LICENSE AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

IF LICENSE CONTRACT OR SIMILAR DOCUMENT ACCOMPANIES SOFTWARE, TERMS OF THE SOFTWARE USE DEFINED IN SUCH DOCUMENT PREVAIL OVER THE CURRENT LICENSE AGREEMENT.

AFTER CLICKING THE ACCEPT BUTTON IN THE WINDOW CONTAINING THE LICENSE AGREEMENT OR AFTER ENTERING CORRESPONDING SYMBOL(-S), YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

## 1. Definitions

1.1. Software means software including any Updates and related materials.

1.2. Rightholder (owner of all rights, whether exclusive or otherwise, to the Software) means AO Kaspersky Lab, a company incorporated according to the laws of the Russian Federation.

1.3. Computer(s) means combination of hardware(s), including personal computers, laptops, workstations, personal digital assistants, 'smart phones', hand-held devices, or other electronic devices, and operating system(s) (including system virtual machines) for which the Software was designed where the Software will be installed and/or used.

1.4. End User (You/Your) - means the organization for which the Software is downloaded or acquired and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term "organization," without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.

1.5. Partner(s) means organizations or individual(s) who distributes the Software based on an agreement and license with the Rightholder.

1.6. Update(s) means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions, or maintenance packs, etc.

1.7. User Manual means user manual, administrator guide, reference book and related explanatory or other materials.

The on-line version of the User Manual is available on the Rightholder website: [www.kaspersky.com](http://www.kaspersky.com) and may be updated when necessary.

1.8. Activation Code is a unique set of characters which can be used to activate the Software.

1.9. Key File - means a file with the extension ".key" which can be used to activate the Software.

1.10. License Certificate means a document that is given to the End User which is accompanied by a Key File and Activation Code as well as further information about the license.

1.11. Web-Portal means services provided by the Rightholder and used for management of the installed Software and granted licenses, as well as to obtain and/or store information obtained from the Software and for contacting technical support. As a Web resource, "Company Account", "Kaspersky Endpoint Security Cloud" can be used. Any other Web resource that is used for the above purposes may also be used.

## 2. Grant of license

2.1. You are granted a non-exclusive license to use the Software within the scope of the functionality described in the User Manual or on the Rightholder's Technical Support website, provided You comply with all technical requirements described in the User Manual, as well as restrictions and terms of use specified in this License Agreement.

Trial Version. If You have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, You may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.

Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If You use different versions of the Software or different language editions of the Software, if You receive the Software on multiple media, if You otherwise receive multiple copies of the Software, or if You received the Software bundled with other software, the total permitted number of Your Computers on which all versions of the Software are installed shall correspond to the number of Computers specified in licenses You have obtained provided that unless the licensing terms provide otherwise, each acquired license entitles You to install and use the Software on such a number of Computer(s) as is specified in Clause 2.2.

2.2. You have the right to use the Software for protection of such a number of Computer(s) as is specified on the License Certificate.

2.3. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when You lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of Your principal residence or in the country where You are using the Software.

2.4. From the time of the Software activation or after license Key File installation (with the exception of a trial version of the Software) You have the right to receive the following services from the Rightholder or its Partners for the period specified in the License Certificate:

- Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that You may receive become part of the Software and the terms and conditions of this Agreement apply to them;
- Technical Support via the Internet and Technical Support telephone hotline;
- Access to information and auxiliary resources of the Rightholder.

## 3. Activation and Term

3.1. If You modify Your Computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat activation of the Software or license Key File installation.

3.2. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period (30 days) from the time of the Software activation according to this Agreement provided that the trial version does not entitle You Updates and Technical support via the Internet and Technical support telephone hotline. If Rightholder sets another duration for the single applicable evaluation period You will be informed via notification.

3.3. Your license to Use the Software is limited to the period of time as specified in the License Certificate, the remaining period can be viewed via means described in the User Manual.

3.4. Software functionality depends on the type of license being used, which is specified in the License Certificate. Software functionality corresponds to the description in the

User Manual.

3.5. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the license and/or legality of a copy of the Software installed and/or used on Your Computer. If there is no appropriate license or verification of the license cannot be performed in a reasonable amount of time, the Software will work with limited functionality.

3.6. You agree that in using the Software and in using any report or information derived as a result of using this Software, You will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.

3.7. Except as otherwise specifically provided herein, You may not transfer or assign any of the rights granted to You under this Agreement or any of Your obligations pursuant hereto.

#### 4. Technical Support

4.1. The Technical Support described in Clause 2.4 of this Agreement is provided to You (except for a trial version of the Software) in accordance with Technical Support rules. Technical support service and its rules are located at: [support.kaspersky.com](https://support.kaspersky.com).

#### 5. Conditions regarding Data Processing

5.1. Under this Section additional definitions are introduced:

Data Subject - means a natural person who is a representative of the End User and/or who uses the Software directly or indirectly, including a worker, contractor, employee, or client of the End User in respect of whom the data is transmitted and processed in the context of the End User's activities, including data which could be determined as personal data under the laws of some countries. Data Subject may also include any individual who communicates and transmits his or her data to the End User.

5.2. Where the Activation Code is used to activate the Software, in order to verify legitimate use of the Software, the End User agrees to periodically provide the Rightholder the following information: the type, version and localization of the installed Software, versions of the installed Updates, the identifier of the Computer and the identifier of the Software installation on the Computer, the activation code and the unique identifier of activation of the current license, the type, version and word size of the operating system, the name of the virtual environment when the Software is installed in the virtual environment, and identifiers of the Software components that are active at the time the information is provided.

The Rightholder can use such information also for gathering statistical information about the distribution and use of the Rightholder's Software.

By using the Activation Code, the End User gives its consent to automatically transmit the data specified in this Clause. In case the End User does not agree to provide this information to the Rightholder, the Key File should be used to activate the Software.

5.3. The Rightholder undertakes the processing of all data received from the End User in accordance with the instructions of the End User. License Agreement, in particular the provisions of Section 5 "Conditions regarding Data Processing," along with use of the functionality of the Software and its configuration by the End User are complete instructions issued by the End User to the Rightholder regarding data processing unless otherwise specified in a separate written agreement between the End User and the Rightholder or its Partners.

5.4. The End User is solely responsible for acquainting itself with the User Manual, particularly in regards to data processing, with the Rightholder's Privacy Policy, which describes data handling ([www.kaspersky.com/Products-and-Services-Privacy-Policy](https://www.kaspersky.com/Products-and-Services-Privacy-Policy)) and independently determining whether they comply with the End User's requirements.

5.5. The End User must comply with laws that apply to use of the Software, including laws on confidential information, personal data, data protection. The End User is responsible for implementing and maintaining confidentiality and security measures in respect of data when using Software components that process data without the participation of the Rightholder. The End User must determine the appropriate technical and organizational measures for the protection and confidentiality of the data during use of such components of the Software.

5.6. During use of the Software, especially where the End User configures the Software to use the Kaspersky Security Network, the End User is fully responsible for ensuring that the processing of personal data of Data Subjects is lawful, particularly, within the

meaning of Article 6 (1) (a) to (f) of Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR") (if Data Subject is in the European Union) or applicable laws on confidential information, personal data, data protection, or similar thereto.

5.7. In case that the End User wants to base the lawfulness of the processing on the consent of its Data Subjects, the End User must ensure that the consent which meets all requirements of the applicable laws, especially where the Data Subject is in the European Union and Article 6 (1) (a) GDPR applies, was given by each Data Subject of the End User prior to using the Software. The End User guarantees that consent of each Data Subject of the End User was obtained prior to the processing of personal data.

5.8. It is agreed between the Rightholder and End User that, in case of item 5.7 of this License Agreement, the End User is responsible for proving the existence of effective consent to the processing of personal data, especially according to Article 7 (1) GDPR where Data Subject is in the European Union. The End User guarantees that it is able to and will prove the existence of each Data Subject's consent at any time upon request by the Rightholder within 5 business days starting with the request of the Rightholder.

5.9. Furthermore, in case of item 5.7 of this License Agreement, the End User is obliged and has the full and sole responsibility to provide each individual Data Subject with all information required by applicable law to obtain consent, especially under Article 13 GDPR (if Data Subject is in the European Union), prior to using the Software. In particular, the End User is obliged to provide each Data Subject in the European Union, or where applicable law requires, with the Rightholder's Privacy Policy

([www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy)) prior to using the Software.

5.10. The End User shall be fully liable in relation to the Rightholder for any damage resulting from a breach of this License Agreement, in particular the End User's failure to obtain effective consent of Data Subject, where applicable, and/or from a failure to obtain sufficient effective consent and/or from the lack of proof and/or belated proof of effective consent of Data Subject and/or from any other violation of an obligation under this agreement.

5.11. The End User shall indemnify the Rightholder in relation to third parties from the claims arising from the failure of End User to fulfill obligations under Section 5 "Conditions regarding Data Processing" which third parties, especially the supervisory data protection authorities, assert against the Rightholder.

5.12. If You use the Rightholder's update servers to download the Updates, the End User, in order to increase the efficiency of the update procedure, agrees to periodically provide the Rightholder the following information: the version and localization of the installed Software, identifiers of the Software components to be updated, the identifier of the Software installation on the computer, the type, version and bit count of the operating system.

The Rightholder can use such information also for receiving statistical information about the distribution and use of the Rightholder's Software.

By downloading the Updates from the Rightholder's update servers, the End User gives its consent to automatically transmit the data specified in this Clause. In case the End User does not agree to provide this information to the Rightholder, the End User must obtain the Updates from a local shared folder as described in the User Manual.

## 6. Limitations

6.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and You shall not otherwise reduce any part of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Neither Software's binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the license granted hereunder and may result in criminal and/or civil prosecution against You.

6.2. You shall not transfer the rights to use the Software to any third party.

6.3. You shall not provide the Activation Code and/or Key File to third parties or allow third parties access to the Activation Code and/or Key File, which are deemed confidential data of Rightholder.

6.4. You shall not rent, lease or lend the Software to any third party.

6.5. You shall not use the Software in the creation of data or Software used for detection, blocking or treating threats described in the User Manual.

6.6. Your Key File can be blocked in case You breach any of the terms and conditions of this Agreement.

6.7. If You are using the trial version of the Software You do not have the right to receive the Technical Support specified in Clause 4 of this Agreement and You don't have the right to transfer the license or the rights to use the Software to any third party.

6.8. Violation of the intellectual rights to the Software shall result in civil, administrative or criminal liability in accordance with the law.

## 7. Limited Warranty and Disclaimer

7.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the User Manual provided however that such limited warranty shall not apply to the following: (w) Your Computer's deficiencies and related infringement for which Rightholder's expressly disclaims any warranty responsibility; (x) malfunctions, defects, or failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other third parties' or Your actions or causes beyond Rightholder's reasonable control; (y) any defect not made known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or Software components installed on Your Computer.

7.2. You acknowledge, accept and agree that no software is error free and You are advised to back-up the Computer, with frequency and reliability suitable for You.

7.3. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the User Manual or in this Agreement.

7.4. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clause 2.4 of this Agreement.

7.5. The Rightholder does not guarantee protection from the threats described in the User Manual after the expiration of the period specified in the License Certificate or after the license to use the Software is terminated for any reason.

7.6. You acknowledge that the Software will be provisioned with Rightholder standard settings applied by default and that it is Your sole responsibility to configure the Software to satisfy Your own requirements.

7.7. THE SOFTWARE IS PROVIDED "AS IS" AND THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO THE RIGHTHOLDER.

## 8. Interaction with iptables subsystem

8.1. You acknowledge that the management of iptables, when firewall control functionality or protection against encryption is activated in the Software, is transferred to the Software according to the specified settings. The settings and rules specified in iptables are not transferred to the Software. All settings and rules in iptables are deleted after the firewall management functionality or protection against encryption is activated. All changes to the settings and rules are made only through the Software.

## 9. Exclusion and Limitation of Liability

9.1. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF

PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE RIGHTHOLDER AND/OR ANY OF ITS PARTNERS, EVEN IF THE RIGHTHOLDER AND/OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

YOU AGREE THAT IN THE EVENT THE RIGHTHOLDER AND/OR ITS PARTNERS ARE FOUND LIABLE, THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS SHALL BE LIMITED BY THE COSTS OF THE SOFTWARE. IN NO CASE SHALL THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS EXCEED THE FEES PAID FOR THE SOFTWARE TO THE RIGHTHOLDER OR THE PARTNER (AS MAY BE APPLICABLE).

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXCLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY SUCH DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

#### 10. GNU and Other Third Party licenses

10.1. The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any Software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to [source@kaspersky.com](mailto:source@kaspersky.com) or the source code is supplied with the Software. If any Open Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

#### 11. Intellectual Property Ownership

11.1. You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its Partners and that the Rightholder and its Partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any the Trademarks or Service Marks of the Rightholder and/or its Partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give You any rights of ownership in that Trademark. The Rightholder and/or its Partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to You any title to the intellectual property in the Software, and You will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant You any intellectual property rights in the Software and You acknowledge that the license, as further defined herein, granted under this Agreement only provides You with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to You in this Agreement.

11.2. You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

## 12. Governing Law; Arbitration

12.1. This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the International Commercial Arbitration Court at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 12 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

## 13. Period for Bringing Actions

13.1. No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

## 14. Entire Agreement; Severability; No Waiver

14.1. This Agreement is the entire agreement between You and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to subject matter of this Agreement. You acknowledge that You have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by You and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Rightholder's failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

## 15. Rightholder Contact Information

Should You have any questions concerning this Agreement, or if You desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

AO Kaspersky Lab, Bldg. 3, 39A, Leningradskoe Shosse  
Moscow, 125212  
Russian Federation  
E-mail: [info@kaspersky.com](mailto:info@kaspersky.com)  
Web site: [www.kaspersky.com](http://www.kaspersky.com)

## KASPERSKY LAB - PRODUCTS AND SERVICES PRIVACY POLICY

### Introduction

AO Kaspersky Lab, located at bldg. 3, 39A, Leningradskoe Shosse, Moscow, 125212, Russian Federation and all companies belonging to the group "Kaspersky Lab" respect your privacy. This Products and Services Privacy Policy (Privacy Policy) describes how we use the information you provide when you use our products and services, and the choices you can make about our use of the information. We also describe the measures we take to protect the information and how you can contact us about our privacy practices.

In connection with specific products or services offered by Kaspersky Lab, you are provided with the agreements, terms of use, and statements that supplement this policy



relating to data handling.

This policy may be changed because of changes in legislation, the requirements of the authorities or to reflect changes in our practices concerning the processing of personal data. The revised policy will be posted on our website and will be effective immediately upon being posted. You can read at any time the policy currently in effect on our website: [www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy).

This version of the policy is effective as of January 1, 2019.

#### The Sources of Information

Kaspersky Lab may obtain information about you from various sources, namely:

- . products and services;
- . by your signing up for a Kaspersky Lab products or services;
- . in response to technical support or other communication in order to ensure the required performance of products and services;
- . on our websites;
- . in response to marketing or other communications;
- . through participation in an offer, program or promotion.

You may also choose to consent to third parties disclosing information about you to us that those third parties have received.

#### Information Provided by Users and How We Use Information

Personal data processing by Kaspersky Lab is always carried out in a legal and fair manner.

You will always know what kind of information you provide to Kaspersky Lab before you start to use the products and services or confirm with your consent. The data which you provide depends on the services, products, and features you use. For more information about data you provide, please refer to End User License Agreement, Kaspersky Security Network Statement and other documentation of product and services that you use, especially:

#### FOR HOME USERS (B2C):

- . SECTION "B" OF THE EULA, WHICH DESCRIBES THE DATA THAT NEED TO BE PROCESSED IN ORDER TO PERFORM OBLIGATIONS UNDER THE CONTRACT;
- . KASPERSKY SECURITY NETWORK STATEMENT, WHICH DESCRIBES THE DATA THE PROCESSING OF WHICH MAY INCREASE THE REACTION SPEED OF PRODUCTS AND SERVICES IN THE EVENT OF THREATS TO INFORMATION SECURITY;
- . MARKETING STATEMENT, WHICH DESCRIBES THE DATA THE PROCESSING OF WHICH MAY IMPROVE THE PERFORMANCE OF PRODUCTS AND WILL ENABLE AN ASSESSMENT OF USER SATISFACTION REGARDING PRODUCT USE;
- . SEPARATE STATEMENTS RELATING TO SPECIFIC PRODUCT FEATURES, WHICH DESCRIBE THE DATA PROCESSED DURING THEIR USE, FOR EXAMPLE, ANTI-SPAM. YOU CAN FAMILIARIZE YOURSELF WITH SUCH STATEMENTS WHEN YOU TURN ON THE FEATURES IN THE PRODUCT.

#### FOR BUSINESS USERS (B2B):

- . SECTION "CONDITIONS REGARDING DATA PROCESSING" OF THE EULA, WHICH DESCRIBES THE DATA THAT NEED TO BE PROCESSED IN ORDER TO PERFORM OBLIGATIONS UNDER THE CONTRACT;
- . KASPERSKY SECURITY NETWORK STATEMENT, WHICH DESCRIBES THE DATA THE PROCESSING OF WHICH MAY INCREASE THE REACTION SPEED OF PRODUCTS AND SERVICES IN THE EVENT OF THREATS TO INFORMATION SECURITY. FOR SOME PRODUCTS, THE IT ADMINISTRATOR OR ANY OTHER EMPLOYEE RESPONSIBLE FOR SETTING UP THE PRODUCT CAN CHOOSE THE VOLUME OF DATA TO BE PROCESSED.

The data obtained for processing depends on the product or service, and it is recommended that users carefully read the agreements and related statements accepted during installation or usage of software or service.

Some data are non-personal, according to laws of certain countries. Regardless of the type of data and territory where data was received or processed, we use the highest standards of data protection and apply various legal, organizational, and technical measures in order to protect user data, guarantee safety and confidentiality, as well as ensure users' rights guaranteed under applicable law.

The data depends on the products and services you use, and could include the following:

- . License/ subscription information

It is processed in order to recognize legitimate users. This data is needed to maintain

communication between the product and Kaspersky Lab services - sending and receiving product databases, updates, etc.

. Product information

Data on the product's operation and its interaction with the user is also analyzed. For example, how long does threat scanning take? Which features are used more often than others? Answers to these and other questions help developers to improve products, making them faster and easier to use.

. Device data

Data such as device type, operating system, etc. may be needed so the user doesn't have to buy a new license for the security product after reinstalling the operating system. This information also helps us to analyze cyberthreats, because it shows how many devices are affected by any specific threat.

. Threats detected

If a threat (new or known) is found on a device, information about that threat is sent to Kaspersky Lab. This enables us to analyze threats, their sources, principles of infection, etc., resulting in a higher quality of protection for every user.

. Information on installed applications

This information helps to create lists of 'white' or harmless applications and prevents security products from mistakenly identifying such applications as malicious. This data is also used to update and extend program categories for features like Parental Control and Application Startup Control. In addition, this information helps us to offer users security solutions that best match their needs.

. URLs visited

URLs can be sent to be checked whether they are malicious. This information also helps to create lists of 'white' or harmless websites and prevents security products from mistakenly identifying such websites as malicious. This data is also used to update and extend website categories for solutions like Kaspersky Safe Kids and provide better protection for financial transactions in such products as Kaspersky Fraud Prevention. In addition, this information helps us to offer users security solutions that best match their needs. Information about logins and passwords, if contained in the initial browser request from the user, is removed from the visited URL addresses up to the hostname or IP address. In any case, it is not Kaspersky Lab's purpose to process user logins and passwords, and Kaspersky Lab takes all reasonable and sufficient measures to avoid processing these data.

. Operating System events

New malware can often be identified only by its suspicious behavior. Because of this, the product analyzes data on processes running on the device. This makes it possible to identify early on processes that indicate malicious activity and to prevent any damaging consequences, such as the destruction of user data.

. Suspicious files and files that could be exploited by intruders

If an (as yet) unknown file, exhibiting suspicious behavior is detected on a device, it can be automatically sent for a more thorough analysis by machine learning-based technologies and, in rare cases, by a malware analyst. Personal files (such as photos or documents) are rarely malicious and do not behave suspiciously. As a result, the 'suspicious' category includes mainly executable files (.exe). For the purpose of investigating information security incidents, executable and non-executable "white files" or their parts may be sent.

. Wi-Fi connection data

This information is analyzed in order to warn users of insecure (i.e., poorly protected) Wi-Fi access points, helping to prevent personal data from being inadvertently intercepted.

. User contact data

Email addresses are used for authorization on the Kaspersky Lab web portals (My Kaspersky,

Company Account, Kaspersky Endpoint Security Cloud, etc.), which enables users to manage their protection remotely. Email addresses are used to send security messages to (e.g., containing important alerts) to users of Kaspersky Lab products. Users can also choose to specify the names (or nicknames) by which they would like to be addressed on the My Kaspersky portal and in emails. Contact information is provided by users at their own discretion.

. Dump and trace files

By checking the special box in the product settings, users can also share error reports with Kaspersky Lab servers. This information helps (1) during analysis of errors that occurred in the product and to modify it accordingly so that it will function more effectively moving forward, and (2) in the prevention and investigation of information security incidents.

. Content of your emails

During your use of the anti-spam functionality, we may receive and analyze information about emails, including content and senders to protect you from the spam and fraud. This functionality is intended to protect its users from any unwanted emails or spam. The anti-spam functionality analyzes information contained in emails reported by you as spam or as incorrectly identified as spam by the software.

. Data about stolen device

The Anti-theft feature provides certain remote access and control functions designed to protect data on your mobile phone in case of theft, as well allows you to receive information about the location of the stolen device. Anti-theft has to store data about your phone and approved users for these functions to work.

. Data for child protection feature

If a parent or holder of parental responsibility wants to use the child protection feature like Kaspersky Safe Kids, he or she can receive information about the child's device and information about the child's location. Additionally, the parent or holder of parental responsibility can configure parameters in order to block or permit specific websites and/or allow or prevent certain applications from running on the child's device. Kaspersky Lab does not collect children's data beyond the framework of such feature.

KASPERSKY LAB WILL ONLY PROCESS PERSONAL DATA FOR PARTICULAR, PRE-DETERMINED PURPOSES THAT ARE LEGITIMATE WITH REGARD TO APPLICABLE LAW, AND THAT ARE RELEVANT TO KASPERSKY LAB'S BUSINESS.

. To ensure the performance of a contract with users and to ensure the required performance of products and services for customers.

. To protect the user from known threats to information security.

. To verify that the license is legal.

. To update the anti-virus databases;

. To increase the effectiveness of the protection of your computer, in particular to provide a faster response to new information and network security threats, to increase the effectiveness of the performance of the software's protection component, to decrease the probability of false positive.

. To improve user interaction and experience with our products and services, in particular changing interfaces and providing the desired content and advertisement, related to Marketing purpose.

. To provide technical support of products and services for customers and to improve the quality of products and services.

Kaspersky Lab will retain personal data for as long as necessary to fulfill the purpose for which the data is processed in accordance with the objectives specified in the agreements (KSN statements, EULAs, consents), or to comply with applicable legal requirements.

LIMITATION OR RESTRICTION DATA PROCESSING

IF YOU CHOOSE NOT TO PROVIDE DATA THAT IS NECESSARY IN ORDER FOR A PRODUCT OR FEATURE TO WORK, YOU MAY NOT BE ABLE TO USE THAT PRODUCT OR FEATURE. THIS OBLIGATORY DATA IS LISTED IN THE END USER LICENSE AGREEMENT. THE KASPERSKY SECURITY NETWORK STATEMENT OR MARKETING STATEMENT CONTAINS A LIST OF DATA THAT USERS CAN DECIDE TO PROVIDE TO US AT ANY TIME BY

CHECKING THE CORRESPONDING BOX IN THE PRODUCT SETTINGS (THEY CAN ALSO REVERSE THIS DECISION WHENEVER THEY CHOOSE).

What we aren't going to process

Through its products and services, Kaspersky Lab never process "sensitive" personal data such as religion, political views, sexual preference, or health, or other special categories of personal data. We do not wish to receive any such data and will not request it from you.

Kaspersky Lab's products must be installed and used by an adult. Children may use the device where Kaspersky Lab's product was installed only with permission from their parents or holder of parental responsibility. Except for "Data for child protection feature", we do not intend to process personal data of children, nor do we want to receive such personal information of children.

Where we process Information

The personal data provided by users to Kaspersky Lab can be processed in the following countries, including countries outside European Union (EU) or the European Economic Area (EEA):

Within the EU or EEA:

- . Germany
- . Netherlands
- . France
- . United Kingdom

Outside of the EU or EEA:

- . Switzerland
- . Canada
- . Singapore
- . Russia
- . Japan
- . USA
- . Mexico
- . China
- . Azerbaijan

The list of countries where the data provided by the user may be processed can change. You can acquaint yourself with the current list of countries in the version of the Privacy Policy on the website [www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy).

According to our general business practice, the data received from users in the EU are processed on servers located in the EU and Russia.

The personal data may be processed at destinations outside the European Union (EU) or the European Economic Area (EEA) some of which have not been determined by the European Commission to have an adequate level of data protection. It may also be processed by staff operating outside EU or EEA who work for us or for one of our suppliers.

Whenever data is processed, we use the highest level of standards for data protection and apply a variety of legal measures in order to protect user data, guarantee safety and confidentiality, and ensure users' rights. To learn more about the European Commission's decisions on the adequacy of the protection of personal data in the countries where Kaspersky Lab processes data, please visit: [ec.europa.eu/justice/data-protection/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm)

Provision of Information

We never provide data or access to them for state organization or third parties. We may only disclose the Information as follows:

- . Within the Group of Companies Kaspersky Lab. Data can be shared.
- . Service Providers. We also may share your information with vendors that provide services to us, including companies that provide web analytics, data processing, advertising, e-mail distribution, payment processing, order fulfillment, and other services.

Please note that some of our products, for example Kaspersky Secure Connection, include applications of third parties whose privacy practices differ from Kaspersky Lab's. If you provide personal data to any of those applications, your data is governed by their privacy

statements. You are responsible for acquainting yourself with the data processing rules and procedures described in the relevant privacy statements.

#### Your Rights and Options

You have certain rights regarding your personal data. We also offer you certain options about what personal data you provide to us, how we use that information, and how we communicate with you.

In most cases you can choose not to provide personal data to us when you use Kaspersky Lab's products, services, and websites. You may also refrain from submitting information directly to us. However, if you do not provide personal data when requested, you may not be able to benefit from the full range of Kaspersky Lab products and services and we may not be able to provide you with information about products, services, and promotions. You can at any time choose not to receive marketing communications by e-mail by clicking on the unsubscribe link within the marketing e-mails you receive from us.

If your employer provides your personal data to Kaspersky Lab, you may have certain options with respect to Kaspersky Lab's use or disclosure of the information. Please contact your employer to learn about and to exercise your options.

To the extent provided by applicable law, you may withdraw any consent you previously provided to us, or object at any time on legitimate grounds, to the processing of your personal data. We will apply your preferences going forward. In some circumstances, withdrawing your consent to Kaspersky Lab's use or disclosure of your personal data will mean that you cannot take advantage of certain Kaspersky Lab products or services.

Subject to applicable law, you may have the right to: obtain confirmation that we hold personal data about you, request access to and receive information about your personal data, receive copies of your personal data that you provided to us, also in a machine-readable format and have it sent to another data controller, where technically possible, update and correct inaccuracies in your personal data, object to the processing of your personal data, have the information blocked, anonymized or deleted, as appropriate, as well as lodge a complaint with a supervisory authority. The right to access personal data may be limited in some circumstances by the requirements of local law. To exercise rights that depend on action from Kaspersky Lab, please contact us as set forth below.

If you provide us with any information or material relating to another individual, you should make sure that this sharing with us and our further use as described to you from time to time is in line with applicable laws; thus, for example, you should duly inform that individual about the processing of her/his personal data and obtain her/his consent, as may be necessary under applicable laws.

If we fall short of your expectations in processing your personal data or you wish to make a complaint about our privacy practices, please relate this to us, as it gives us an opportunity to fix the problem. You may contact us by using the contact details provided in the "How to Contact Us" section below. To assist us in responding to your request, please give full details of the issue. We attempt to review and respond to all complaints within a reasonable time.

#### The Privacy Principles

Personal data processing at Kaspersky Lab is based on the following principles:

##### Consent and choice

- . Presenting to the users the choice whether or not to allow the processing of their personal data except where the users cannot freely withhold consent or where applicable law specifically allows the processing of personal data without the natural person's consent. The user's election must be freely given, specific and made on a knowledgeable basis;

- . Informing users, before obtaining consent, about their rights under the individual participation and access principle;

- . Providing users, before obtaining consent, with the information indicated by the openness, transparency and notice principle; and

- . Explaining to users the implications of granting or withholding consent.

##### Purpose legitimacy and specification

- . Ensuring that the purpose(s) complies with applicable law and relies on a permissible legal basis;

- . Communicating the purpose(s) to users before the information is used for the first time for a new purpose;

- . Using language for this specification which is both clear and appropriately adapted to the circumstances;

#### Data processing limitation

- . Limiting the gathering of personal data to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s).
- . Deleting and disposing of personal data whenever the purpose for personal data processing has expired, there are no legal requirements to keep the personal data, or whenever it is practical to do so.

#### Use, retention and disclosure limitation

- . Limiting the use, retention and disclosure of personal data to that which is necessary in order to fulfil specific, explicit and legitimate purposes;
- . Limiting the use of personal data to the purposes specified by Kaspersky Lab prior to receiving the data, unless a different purpose is explicitly required by applicable law;
- . Retaining personal data only as long as necessary to fulfill the stated purposes, and thereafter securely destroying or anonymizing it; and
- . Locking (i.e. archiving, securing and exempting the personal data from further processing) any personal data when and for as long as the stated purposes have expired, but where retention is required by applicable laws.

#### Accuracy and quality

- . Ensuring that the personal data processed is accurate, complete, up-to-date (unless there is a legitimate basis for keeping outdated data), adequate and relevant for the purpose of use;
- . Ensuring the reliability of personal data provided from a source other than from users before it is processed;
- . Verifying, through appropriate means, the validity and correctness of the claims made by the user prior to making any changes to the personal data (in order to ensure that the changes are properly authorized), where it is appropriate to do so;
- . Establishing personal data processing procedures to help ensure accuracy and quality; and
- . Establishing control mechanisms to periodically check the accuracy and quality of personal data processing.

#### Openness, transparency and notice

- . Providing users with clear and easily accessible information about Kaspersky Lab's policies;
- . Establishing procedures and practices with respect to the processing of personal data;
- . Including in notices the fact that personal data is being processed, the purpose for which this is done, the types of privacy stakeholders to whom the personal data might be disclosed, and the identity of the entity which determines the above and on how to contact;
- . Disclosing the options and means offered by Kaspersky Lab to users for the purposes of limiting the processing of, and for accessing, correcting and removing their information;
- . Giving notice to users when major changes in the personal data handling procedures occur.

#### Individual participation and access

- . Giving users the ability to contact us (by using the contact details provided in the "How to Contact Us") and review their personal data, provided their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law;
- . Allowing users (by using the contact details provided in the "How to Contact Us" or by using interface of our products and services) to challenge the accuracy and completeness of the personal data and have it amended, corrected or removed as appropriate and possible in the specific context;
- . Providing any amendment, correction or removal to personal data processors and third parties to whom personal data had been disclosed, where they are known; and
- . Establishing procedures to enable users to exercise these rights in a simple, fast and efficient way, which does not entail undue delay or cost.

## Information Security: How We Protect Your Privacy

Information security is Kaspersky Lab's core business. All data and all information provided by you is confidential by default. Kaspersky Lab will therefore always apply technical and organizational data security measures for the protection of personal data that are adequate and appropriate, taking into account the concrete risks resulting from the processing of personal data as well as up-to-date security standards and procedures. In order to, among other reasons, identify and fulfill the appropriate level of protection, Kaspersky Lab classifies processing systems with personal data and implements cascading sets of protective measures.

Kaspersky Lab also maintains physical, electronic and procedural safeguards to protect the information against loss, misuse, damage or modification and unauthorized access or disclosure. Some of the other central features of our information security program are:

- . The Information Security Department, which designs, implements and provides oversight to our information security program;
- . A determination of personal data safety hazards in the course of processing in a Kaspersky Lab processing system;
- . Application of appropriate information security tools;
- . Performance evaluation of applied personal data security measures before commissioning processing systems;
- . Implementing controls to identify, authenticate and authorize access to various services or websites;
- . Discovering the facts surrounding unauthorized access to personal data and adopting corresponding measures;
- . Recovery of personal data that was modified or destructed;
- . Establishing access rules to personal data processed in Kaspersky Lab processing systems and also recording and accounting for all actions undertaken with personal data in these systems;
- . Encryption between our clients and servers (and between our various data centers);
- . We restrict access of our employees and contractors who need to know the information in order to process it for us and who are subject to strict contractual confidentiality obligations, to personal information. They may be disciplined or their contract terminated if they fail to meet these obligations;
- . Monitoring of our systems infrastructure to detect weaknesses and potential intrusions;
- . Monitoring measures taken to ensure the security of personal data;
- . Providing Kaspersky Lab personnel with relevant training and continually updating our security practices in light of new risks and developments in technology.

## How to Contact Us

If you have any questions or comments about this Privacy Policy, Kaspersky Lab's privacy practices or if you would like us to update or remove information or preferences you provided to us, please visit <https://www.kaspersky.com/global-privacy-policy>, or, according to point (a) of Article 13 (1) and Article 27 (1) of Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR"), you may contact our Kaspersky Lab EU representative via e-mail or phone: Kaspersky Labs GmbH, Ingolstadt, Germany, [info@kaspersky.de](mailto:info@kaspersky.de), +49 (0) 841 98 18 90.

Kaspersky Security 10.1.2 for Windows Server END USER LICENSE AGREEMENT; AND  
Products and Services PRIVACY POLICY

## KASPERSKY LAB END USER LICENSE AGREEMENT ("LICENSE AGREEMENT")

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

CLICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE WINDOW CONTAINING THE LICENSE AGREEMENT, OR BY ENTERING CORRESPONDING SYMBOL(-S), YOU CONFIRM IN A LEGALLY BINDING WAY THAT YOU AS THE ORGANIZATION FOR WHICH THE SOFTWARE IS DOWNLOADED OR ACQUIRED HAVE AUTHORIZED THE NATURAL PERSON ACCEPTING THIS LICENSE AGREEMENT TO ENTER INTO THIS LICENSE AGREEMENT FOR AND ON BEHALF OF YOU. FURTHERMORE, YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS LICENSE AGREEMENT AND AGREE

THAT THIS LICENSE AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

IF LICENSE CONTRACT OR SIMILAR DOCUMENT ACCOMPANIES SOFTWARE, TERMS OF THE SOFTWARE USE DEFINED IN SUCH DOCUMENT PREVAIL OVER THE CURRENT LICENSE AGREEMENT.

AFTER CLICKING THE ACCEPT BUTTON IN THE WINDOW CONTAINING THE LICENSE AGREEMENT OR AFTER ENTERING CORRESPONDING SYMBOL(-S), YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

## 1. Definitions

1.1. Software means software including any Updates and related materials.

1.2. Rightholder (owner of all rights, whether exclusive or otherwise, to the Software) means AO Kaspersky Lab, a company incorporated according to the laws of the Russian Federation.

1.3. Computer(s) means combination of hardware(s), including personal computers, laptops, workstations, personal digital assistants, 'smart phones', hand-held devices, or other electronic devices, and operating system(s) (including system virtual machines) for which the Software was designed where the Software will be installed and/or used.

1.4. End User (You/Your) - means the organization for which the Software is downloaded or acquired and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term "organization," without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.

1.5. Partner(s) means organizations or individual(s) who distributes the Software based on an agreement and license with the Rightholder.

1.6. Update(s) means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions, or maintenance packs, etc.

1.7. User Manual means user manual, administrator guide, reference book and related explanatory or other materials.

The on-line version of the User Manual is available on the Rightholder website: [www.kaspersky.com](http://www.kaspersky.com) and may be updated when necessary.

1.8. Activation Code is a unique set of characters which can be used to activate the Software.

1.9. Key File - means a file with the extension ".key" which can be used to activate the Software.

1.10. License Certificate means a document that is given to the End User which is accompanied by a Key File and Activation Code as well as further information about the license.

1.11. Web-Portal means services provided by the Rightholder and used for management of the installed Software and granted licenses, as well as to obtain and/or store information obtained from the Software and for contacting technical support. As a Web resource, "Company Account", "Kaspersky Endpoint Security Cloud" can be used. Any other Web resource that is used for the above purposes may also be used.

## 2. Grant of license

2.1. You are granted a non-exclusive license to use the Software within the scope of the functionality described in the User Manual or on the Rightholder's Technical Support website, provided You comply with all technical requirements described in the User Manual, as well as restrictions and terms of use specified in this License Agreement.

Trial Version. If You have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, You may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.

Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If You use different versions of the Software or different language editions of the Software, if You receive the Software on multiple media, if You otherwise receive multiple copies of the Software, or if You received the Software bundled with



other software, the total permitted number of Your Computers on which all versions of the Software are installed shall correspond to the number of Computers specified in licenses You have obtained provided that unless the licensing terms provide otherwise, each acquired license entitles You to install and use the Software on such a number of Computer(s) as is specified in Clause 2.2.

2.2. You have the right to use the Software for protection of such a number of Computer(s) as is specified on the License Certificate.

2.3. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost, destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when You lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of Your principal residence or in the country where You are using the Software.

2.4. From the time of the Software activation or after license Key File installation (with the exception of a trial version of the Software) You have the right to receive the following services from the Rightholder or its Partners for the period specified in the License Certificate:

- Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that You may receive become part of the Software and the terms and conditions of this Agreement apply to them;
- Technical Support via the Internet and Technical Support telephone hotline;
- Access to information and auxiliary resources of the Rightholder.

### 3. Activation and Term

3.1. If You modify Your Computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat activation of the Software or license Key File installation.

3.2. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period (30 days) from the time of the Software activation according to this Agreement provided that the trial version does not entitle You Updates and Technical support via the Internet and Technical support telephone hotline. If Rightholder sets another duration for the single applicable evaluation period You will be informed via notification.

3.3. Your license to Use the Software is limited to the period of time as specified in the License Certificate, the remaining period can be viewed via means described in the User Manual.

3.4. Software functionality depends on the type of license being used, which is specified in the License Certificate. Software functionality corresponds to the description in the User Manual.

3.5. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the license and/or legality of a copy of the Software installed and/or used on Your Computer. If there is no appropriate license or verification of the license cannot be performed in a reasonable amount of time, the Software will work with limited functionality.

3.6. You agree that in using the Software and in using any report or information derived as a result of using this Software, You will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.

3.7. Except as otherwise specifically provided herein, You may not transfer or assign any of the rights granted to You under this Agreement or any of Your obligations pursuant hereto.

### 4. Technical Support

4.1. The Technical Support described in Clause 2.4 of this Agreement is provided to You (except for a trial version of the Software) in accordance with Technical Support rules. Technical support service and its rules are located at: [support.kaspersky.com](http://support.kaspersky.com).

### 5. Conditions regarding Data Processing

5.1. Under this Section additional definitions are introduced:

Data Subject - means a natural person who is a representative of the End User and/or who uses the Software directly or indirectly, including a worker, contractor, employee, or client of the End User in respect of whom the data is transmitted and processed in the

context of the End User's activities, including data which could be determined as personal data under the laws of some countries. Data Subject may also include any individual who communicates and transmits his or her data to the End User.

5.2. Where the Activation Code is used to activate the Software, in order to verify legitimate use of the Software, the End User agrees to periodically provide the Rightholder the following information: the type, version and localization of the installed Software, versions of the installed Updates, the identifier of the Computer, time on the Computer and the identifier of the Software installation on the Computer, the identifier of the Software installation package, hashsum of the current activation code and the previous activation code, the type, version and word size of the operating system, the name of the virtual environment when the Software is installed in the virtual environment, the identifiers of the Software components that are active at the time the information is provided, the identifier of the regional Software activation center, the hashsum, creation date and the identifier of the Software activation ticket, Software activation date and the license expiration date, the unique identifier of a current license.

The Rightholder can use such information also for gathering statistical information about the distribution and use of the Rightholder's Software.

By using the Activation Code, the End User gives its consent to automatically transmit the data specified in this Clause. In case the End User does not agree to provide this information to the Rightholder, the Key File should be used to activate the Software.

5.3. If You use the Rightholder's update servers to download the Updates, the End User, in order to increase the efficiency of the update procedure, agrees to periodically provide the Rightholder the following information: the full version with a build number of the installed Software, the identifier of the Software installation on the computer, the identifier of the Software, Software activation type, license identifier, unique identifier of an update task launch.

The Rightholder can use such information also for receiving statistical information about the distribution and use of the Rightholder's Software.

By downloading the Updates from the Rightholder's update servers, the End User gives its consent to automatically transmit the data specified in this Clause. In case the End User does not agree to provide this information to the Rightholder, the End User must obtain the Updates from a local shared folder as described in the User Manual.

5.4. The Rightholder undertakes the processing of all data received from the End User in accordance with the instructions of the End User. License Agreement, in particular the provisions of Section 5 "Conditions regarding Data Processing," along with use of the functionality of the Software and its configuration by the End User are complete instructions issued by the End User to the Rightholder regarding data processing unless otherwise specified in a separate written agreement between the End User and the Rightholder or its Partners.

5.5. The End User is solely responsible for acquainting itself with the User Manual, particularly in regards to data processing, with the Rightholder's Privacy Policy, which describes data handling ([www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy)) and independently determining whether they comply with the End User's requirements.

5.6. The End User must comply with laws that apply to use of the Software, including laws on confidential information, personal data, data protection. The End User is responsible for implementing and maintaining confidentiality and security measures in respect of data when using Software components that process data without the participation of the Rightholder. The End User must determine the appropriate technical and organizational measures for the protection and confidentiality of the data during use of such components of the Software.

5.7. During use of the Software, especially where the End User configures the Software to use the Kaspersky Security Network, the End User is fully responsible for ensuring that the processing of personal data of Data Subjects is lawful, particularly, within the meaning of Article 6 (1) (a) to (f) of Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR") (if Data Subject is in the European Union) or applicable laws on confidential information, personal data, data protection, or similar thereto.

5.8. In case that the End User wants to base the lawfulness of the processing on the consent of its Data Subjects, the End User must ensure that the consent which meets all requirements of the applicable laws, especially where the Data Subject is in the European Union and Article 6 (1) (a) GDPR applies, was given by each Data Subject of the End User prior to using the Software. The End User guarantees that consent of each Data Subject of the End User was obtained prior to the processing of personal data.

5.9. It is agreed between the Rightholder and End User that, in case of item 5.8 of this License Agreement, the End User is responsible for proving the existence of effective consent to the processing of personal data, especially according to Article 7 (1) GDPR where Data Subject is in the European Union. The End User guarantees that it is able to and will prove the existence of each Data Subject's consent at any time upon request by the Rightholder within 5 business days starting with the request of the Rightholder.

5.10. Furthermore, in case of item 5.8 of this License Agreement, the End User is obliged and has the full and sole responsibility to provide each individual Data Subject with all information required by applicable law to obtain consent, especially under Article 13 GDPR (if Data Subject is in the European Union), prior to using the Software. In particular, the End User is obliged to provide each Data Subject in the European Union, or where applicable law requires, with the Rightholder's Privacy Policy

([www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy)) prior to using the Software.

5.11. The End User shall be fully liable in relation to the Rightholder for any damage resulting from a breach of this License Agreement, in particular the End User's failure to obtain effective consent of Data Subject, where applicable, and/or from a failure to obtain sufficient effective consent and/or from the lack of proof and/or belated proof of effective consent of Data Subject and/or from any other violation of an obligation under this agreement.

5.12. The End User shall indemnify the Rightholder in relation to third parties from the claims arising from the failure of End User to fulfill obligations under Section 5 "Conditions regarding Data Processing" which third parties, especially the supervisory data protection authorities, assert against the Rightholder .

## 6. Limitations

6.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and You shall not otherwise reduce any part of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Neither Software's binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the license granted hereunder and may result in criminal and/or civil prosecution against You.

6.2. You shall not transfer the rights to use the Software to any third party.

6.3. You shall not provide the Activation Code and/or Key File to third parties or allow third parties access to the Activation Code and/or Key File, which are deemed confidential data of Rightholder.

6.4. You shall not rent, lease or lend the Software to any third party.

6.5. You shall not use the Software in the creation of data or Software used for detection, blocking or treating threats described in the User Manual.

6.6. Your Key File can be blocked in case You breach any of the terms and conditions of this Agreement.

6.7. If You are using the trial version of the Software You do not have the right to receive the Technical Support specified in Clause 4 of this Agreement and You don't have the right to transfer the license or the rights to use the Software to any third party.

6.8. Violation of the intellectual rights to the Software shall result in civil, administrative or criminal liability in accordance with the law.

## 7. Limited Warranty and Disclaimer

7.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the User Manual provided however that such limited warranty shall not apply to the following: (w) Your Computer's deficiencies and related infringement for which Rightholder's expressly disclaims any warranty responsibility; (x) malfunctions, defects, or failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other third parties' or Your actions or causes beyond Rightholder's reasonable control; (y) any defect not made

known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or Software components installed on Your Computer.

7.2. You acknowledge, accept and agree that no software is error free and You are advised to back-up the Computer, with frequency and reliability suitable for You.

7.3. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the User Manual or in this Agreement.

7.4. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clause 2.4 of this Agreement.

7.5. The Rightholder does not guarantee protection from the threats described in the User Manual after the expiration of the period specified in the License Certificate or after the license to use the Software is terminated for any reason.

7.6. You acknowledge that the Software will be provisioned with Rightholder standard settings applied by default and that it is Your sole responsibility to configure the Software to satisfy Your own requirements.

7.7. THE SOFTWARE IS PROVIDED "AS IS" AND THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DISCLOSED TO THE RIGHTHOLDER.

#### 8. Interaction with Microsoft Windows Firewall

8.1. You acknowledge that Windows Firewall, being turned on at the time of installation of the Software, can be turned off. Settings and rules of Windows Firewall are not exported to the installed Software.

#### 9. Exclusion and Limitation of Liability

9.1. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE RIGHTHOLDER AND/OR ANY OF ITS PARTNERS, EVEN IF THE RIGHTHOLDER AND/OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

YOU AGREE THAT IN THE EVENT THE RIGHTHOLDER AND/OR ITS PARTNERS ARE FOUND LIABLE, THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS SHALL BE LIMITED BY THE COSTS OF THE SOFTWARE. IN NO CASE SHALL THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS EXCEED THE FEES PAID FOR THE SOFTWARE TO THE RIGHTHOLDER OR THE PARTNER (AS MAY BE APPLICABLE).

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXCLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY SUCH DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

#### 10. GNU and Other Third Party licenses

10.1. The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any Software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to [source@kaspersky.com](mailto:source@kaspersky.com) or the source code is supplied with the Software. If any Open Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

## 11. Intellectual Property Ownership

11.1. You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its Partners and that the Rightholder and its Partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any the Trademarks or Service Marks of the Rightholder and/or its Partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give You any rights of ownership in that Trademark. The Rightholder and/or its Partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to You any title to the intellectual property in the Software, and You will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant You any intellectual property rights in the Software and You acknowledge that the license, as further defined herein, granted under this Agreement only provides You with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to You in this Agreement.

11.2. You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

## 12. Governing Law; Arbitration

12.1. This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the International Commercial Arbitration Court at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 12 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

## 13. Period for Bringing Actions

13.1. No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

#### 14. Entire Agreement; Severability; No Waiver

14.1. This Agreement is the entire agreement between You and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to subject matter of this Agreement. You acknowledge that You have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by You and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Rightholder's failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

#### 15. Rightholder Contact Information

Should You have any questions concerning this Agreement, or if You desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

AO Kaspersky Lab, Bldg. 3, 39A, Leningradskoe Shosse  
Moscow, 125212  
Russian Federation  
E-mail: [info@kaspersky.com](mailto:info@kaspersky.com)  
Web site: [www.kaspersky.com](http://www.kaspersky.com)

#### KASPERSKY LAB - PRODUCTS AND SERVICES PRIVACY POLICY

##### Introduction

AO Kaspersky Lab, located at bldg. 3, 39A, Leningradskoe Shosse, Moscow, 125212, Russian Federation and all companies belonging to the group "Kaspersky Lab" respect your privacy. This Products and Services Privacy Policy (Privacy Policy) describes how we use the information you provide when you use our products and services, and the choices you can make about our use of the information. We also describe the measures we take to protect the information and how you can contact us about our privacy practices.

In connection with specific products or services offered by Kaspersky Lab, you are provided with the agreements, terms of use, and statements that supplement this policy relating to data handling.

This policy may be changed because of changes in legislation, the requirements of the authorities or to reflect changes in our practices concerning the processing of personal data. The revised policy will be posted on our website and will be effective immediately upon being posted. You can read at any time the policy currently in effect on our website: [www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy).

This version of the policy is effective as of January 1, 2019.

##### The Sources of Information

Kaspersky Lab may obtain information about you from various sources, namely:

- . products and services;
- . by your signing up for a Kaspersky Lab products or services;
- . in response to technical support or other communication in order to ensure the required performance of products and services;
- . on our websites;
- . in response to marketing or other communications;
- . through participation in an offer, program or promotion.

You may also choose to consent to third parties disclosing information about you to us that those third parties have received.

##### Information Provided by Users and How We Use Information

Personal data processing by Kaspersky Lab is always carried out in a legal and fair manner.

You will always know what kind of information you provide to Kaspersky Lab before you start to use the products and services or confirm with your consent. The data which you provide depends on the services, products, and features you use. For more information

about data you provide, please refer to End User License Agreement, Kaspersky Security Network Statement and other documentation of product and services that you use, especially:

FOR HOME USERS (B2C):

- . SECTION "B" OF THE EULA, WHICH DESCRIBES THE DATA THAT NEED TO BE PROCESSED IN ORDER TO PERFORM OBLIGATIONS UNDER THE CONTRACT;
- . KASPERSKY SECURITY NETWORK STATEMENT, WHICH DESCRIBES THE DATA THE PROCESSING OF WHICH MAY INCREASE THE REACTION SPEED OF PRODUCTS AND SERVICES IN THE EVENT OF THREATS TO INFORMATION SECURITY;
- . MARKETING STATEMENT, WHICH DESCRIBES THE DATA THE PROCESSING OF WHICH MAY IMPROVE THE PERFORMANCE OF PRODUCTS AND WILL ENABLE AN ASSESSMENT OF USER SATISFACTION REGARDING PRODUCT USE;
- . SEPARATE STATEMENTS RELATING TO SPECIFIC PRODUCT FEATURES, WHICH DESCRIBE THE DATA PROCESSED DURING THEIR USE, FOR EXAMPLE, ANTI-SPAM. YOU CAN FAMILIARIZE YOURSELF WITH SUCH STATEMENTS WHEN YOU TURN ON THE FEATURES IN THE PRODUCT.

FOR BUSINESS USERS (B2B):

- . SECTION "CONDITIONS REGARDING DATA PROCESSING" OF THE EULA, WHICH DESCRIBES THE DATA THAT NEED TO BE PROCESSED IN ORDER TO PERFORM OBLIGATIONS UNDER THE CONTRACT;
- . KASPERSKY SECURITY NETWORK STATEMENT, WHICH DESCRIBES THE DATA THE PROCESSING OF WHICH MAY INCREASE THE REACTION SPEED OF PRODUCTS AND SERVICES IN THE EVENT OF THREATS TO INFORMATION SECURITY. FOR SOME PRODUCTS, THE IT ADMINISTRATOR OR ANY OTHER EMPLOYEE RESPONSIBLE FOR SETTING UP THE PRODUCT CAN CHOOSE THE VOLUME OF DATA TO BE PROCESSED.

The data obtained for processing depends on the product or service, and it is recommended that users carefully read the agreements and related statements accepted during installation or usage of software or service.

Some data are non-personal, according to laws of certain countries. Regardless of the type of data and territory where data was received or processed, we use the highest standards of data protection and apply various legal, organizational, and technical measures in order to protect user data, guarantee safety and confidentiality, as well as ensure users' rights guaranteed under applicable law.

The data depends on the products and services you use, and could include the following:

- . License/ subscription information  
It is processed in order to recognize legitimate users. This data is needed to maintain communication between the product and Kaspersky Lab services - sending and receiving product databases, updates, etc.
- . Product information  
Data on the product's operation and its interaction with the user is also analyzed. For example, how long does threat scanning take? Which features are used more often than others? Answers to these and other questions help developers to improve products, making them faster and easier to use.
- . Device data  
Data such as device type, operating system, etc. may be needed so the user doesn't have to buy a new license for the security product after reinstalling the operating system. This information also helps us to analyze cyberthreats, because it shows how many devices are affected by any specific threat.
- . Threats detected  
If a threat (new or known) is found on a device, information about that threat is sent to Kaspersky Lab. This enables us to analyze threats, their sources, principles of infection, etc., resulting in a higher quality of protection for every user.
- . Information on installed applications  
This information helps to create lists of 'white' or harmless applications and prevents security products from mistakenly identifying such applications as malicious. This data is also used to update and extend program categories for features like Parental Control and

Application Startup Control. In addition, this information helps us to offer users security solutions that best match their needs.

. URLs visited

URLs can be sent to be checked whether they are malicious. This information also helps to create lists of 'white' or harmless websites and prevents security products from mistakenly identifying such websites as malicious. This data is also used to update and extend website categories for solutions like Kaspersky Safe Kids and provide better protection for financial transactions in such products as Kaspersky Fraud Prevention. In addition, this information helps us to offer users security solutions that best match their needs. Information about logins and passwords, if contained in the initial browser request from the user, is removed from the visited URL addresses up to the hostname or IP address. In any case, it is not Kaspersky Lab's purpose to process user logins and passwords, and Kaspersky Lab takes all reasonable and sufficient measures to avoid processing these data.

. Operating System events

New malware can often be identified only by its suspicious behavior. Because of this, the product analyzes data on processes running on the device. This makes it possible to identify early on processes that indicate malicious activity and to prevent any damaging consequences, such as the destruction of user data.

. Suspicious files and files that could be exploited by intruders

If an (as yet) unknown file, exhibiting suspicious behavior is detected on a device, it can be automatically sent for a more thorough analysis by machine learning-based technologies and, in rare cases, by a malware analyst. Personal files (such as photos or documents) are rarely malicious and do not behave suspiciously. As a result, the 'suspicious' category includes mainly executable files (.exe). For the purpose of investigating information security incidents, executable and non-executable "white files" or their parts may be sent.

. Wi-Fi connection data

This information is analyzed in order to warn users of insecure (i.e., poorly protected) Wi-Fi access points, helping to prevent personal data from being inadvertently intercepted.

. User contact data

Email addresses are used for authorization on the Kaspersky Lab web portals (My Kaspersky, Company Account, Kaspersky Endpoint Security Cloud, etc.), which enables users to manage their protection remotely. Email addresses are used to send security messages to (e.g., containing important alerts) to users of Kaspersky Lab products. Users can also choose to specify the names (or nicknames) by which they would like to be addressed on the My Kaspersky portal and in emails. Contact information is provided by users at their own discretion.

. Dump and trace files

By checking the special box in the product settings, users can also share error reports with Kaspersky Lab servers. This information helps (1) during analysis of errors that occurred in the product and to modify it accordingly so that it will function more effectively moving forward, and (2) in the prevention and investigation of information security incidents.

. Content of your emails

During your use of the anti-spam functionality, we may receive and analyze information about emails, including content and senders to protect you from the spam and fraud. This functionality is intended to protect its users from any unwanted emails or spam. The anti-spam functionality analyzes information contained in emails reported by you as spam or as incorrectly identified as spam by the software.

. Data about stolen device

The Anti-theft feature provides certain remote access and control functions designed to protect data on your mobile phone in case of theft, as well allows you to receive



information about the location of the stolen device. Anti-theft has to store data about your phone and approved users for these functions to work.

. Data for child protection feature

If a parent or holder of parental responsibility wants to use the child protection feature like Kaspersky Safe Kids, he or she can receive information about the child's device and information about the child's location. Additionally, the parent or holder of parental responsibility can configure parameters in order to block or permit specific websites and/or allow or prevent certain applications from running on the child's device. Kaspersky Lab does not collect children's data beyond the framework of such feature.

KASPERSKY LAB WILL ONLY PROCESS PERSONAL DATA FOR PARTICULAR, PRE-DETERMINED PURPOSES THAT ARE LEGITIMATE WITH REGARD TO APPLICABLE LAW, AND THAT ARE RELEVANT TO KASPERSKY LAB'S BUSINESS.

. To ensure the performance of a contract with users and to ensure the required performance of products and services for customers.

. To protect the user from known threats to information security.

. To verify that the license is legal.

. To update the anti-virus databases;

. To increase the effectiveness of the protection of your computer, in particular to provide a faster response to new information and network security threats, to increase the effectiveness of the performance of the software's protection component, to decrease the probability of false positive.

. To improve user interaction and experience with our products and services, in particular changing interfaces and providing the desired content and advertisement, related to Marketing purpose.

. To provide technical support of products and services for customers and to improve the quality of products and services.

Kaspersky Lab will retain personal data for as long as necessary to fulfill the purpose for which the data is processed in accordance with the objectives specified in the agreements (KSN statements, EULAs, consents), or to comply with applicable legal requirements.

LIMITATION OR RESTRICTION DATA PROCESSING

IF YOU CHOOSE NOT TO PROVIDE DATA THAT IS NECESSARY IN ORDER FOR A PRODUCT OR FEATURE TO WORK, YOU MAY NOT BE ABLE TO USE THAT PRODUCT OR FEATURE. THIS OBLIGATORY DATA IS LISTED IN THE END USER LICENSE AGREEMENT. THE KASPERSKY SECURITY NETWORK STATEMENT OR MARKETING STATEMENT CONTAINS A LIST OF DATA THAT USERS CAN DECIDE TO PROVIDE TO US AT ANY TIME BY CHECKING THE CORRESPONDING BOX IN THE PRODUCT SETTINGS (THEY CAN ALSO REVERSE THIS DECISION WHENEVER THEY CHOOSE).

What we aren't going to process

Through its products and services, Kaspersky Lab never process "sensitive" personal data such as religion, political views, sexual preference, or health, or other special categories of personal data. We do not wish to receive any such data and will not request it from you.

Kaspersky Lab's products must be installed and used by an adult. Children may use the device where Kaspersky Lab's product was installed only with permission from their parents or holder of parental responsibility. Except for "Data for child protection feature", we do not intend to process personal data of children, nor do we want to receive such personal information of children.

Where we process Information

The personal data provided by users to Kaspersky Lab can be processed in the following countries, including countries outside European Union (EU) or the European Economic Area (EEA):

Within the EU or EEA:

- . Germany
- . Netherlands
- . France
- . United Kingdom

Outside of the EU or EEA:

- . Switzerland
- . Canada
- . Singapore
- . Russia
- . Japan
- . USA
- . Mexico
- . China
- . Azerbaijan

The list of countries where the data provided by the user may be processed can change. You can acquaint yourself with the current list of countries in the version of the Privacy Policy on the website [www.kaspersky.com/Products-and-Services-Privacy-Policy](http://www.kaspersky.com/Products-and-Services-Privacy-Policy).

According to our general business practice, the data received from users in the EU are processed on servers located in the EU and Russia.

The personal data may be processed at destinations outside the European Union (EU) or the European Economic Area (EEA) some of which have not been determined by the European Commission to have an adequate level of data protection. It may also be processed by staff operating outside EU or EEA who work for us or for one of our suppliers.

Whenever data is processed, we use the highest level of standards for data protection and apply a variety of legal measures in order to protect user data, guarantee safety and confidentiality, and ensure users' rights. To learn more about the European Commission's decisions on the adequacy of the protection of personal data in the countries where Kaspersky Lab processes data, please visit: [ec.europa.eu/justice/data-protection/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm)

#### Provision of Information

We never provide data or access to them for state organization or third parties. We may only disclose the Information as follows:

- . Within the Group of Companies Kaspersky Lab. Data can be shared.
- . Service Providers. We also may share your information with vendors that provide services to us, including companies that provide web analytics, data processing, advertising, e-mail distribution, payment processing, order fulfillment, and other services.

Please note that some of our products, for example Kaspersky Secure Connection, include applications of third parties whose privacy practices differ from Kaspersky Lab's. If you provide personal data to any of those applications, your data is governed by their privacy statements. You are responsible for acquainting yourself with the data processing rules and procedures described in the relevant privacy statements.

#### Your Rights and Options

You have certain rights regarding your personal data. We also offer you certain options about what personal data you provide to us, how we use that information, and how we communicate with you.

In most cases you can choose not to provide personal data to us when you use Kaspersky Lab's products, services, and websites. You may also refrain from submitting information directly to us. However, if you do not provide personal data when requested, you may not be able to benefit from the full range of Kaspersky Lab products and services and we may not be able to provide you with information about products, services, and promotions.

You can at any time choose not to receive marketing communications by e-mail by clicking on the unsubscribe link within the marketing e-mails you receive from us.

If your employer provides your personal data to Kaspersky Lab, you may have certain options with respect to Kaspersky Lab's use or disclosure of the information. Please contact your employer to learn about and to exercise your options.

To the extent provided by applicable law, you may withdraw any consent you previously provided to us, or object at any time on legitimate grounds, to the processing of your personal data. We will apply your preferences going forward. In some circumstances, withdrawing your consent to Kaspersky Lab's use or disclosure of your personal data will mean that you cannot take advantage of certain Kaspersky Lab products or services.

Subject to applicable law, you may have the right to: obtain confirmation that we hold personal data about you, request access to and receive information about your personal data, receive copies of your personal data that you provided to us, also in a machine-

readable format and have it sent to another data controller, where technically possible, update and correct inaccuracies in your personal data, object to the processing of your personal data, have the information blocked, anonymized or deleted, as appropriate, as well as lodge a complaint with a supervisory authority. The right to access personal data may be limited in some circumstances by the requirements of local law. To exercise rights that depend on action from Kaspersky Lab, please contact us as set forth below.

If you provide us with any information or material relating to another individual, you should make sure that this sharing with us and our further use as described to you from time to time is in line with applicable laws; thus, for example, you should duly inform that individual about the processing of her/his personal data and obtain her/his consent, as may be necessary under applicable laws.

If we fall short of your expectations in processing your personal data or you wish to make a complaint about our privacy practices, please relate this to us, as it gives us an opportunity to fix the problem. You may contact us by using the contact details provided in the "How to Contact Us" section below. To assist us in responding to your request, please give full details of the issue. We attempt to review and respond to all complaints within a reasonable time.

#### The Privacy Principles

Personal data processing at Kaspersky Lab is based on the following principles:

##### Consent and choice

- . Presenting to the users the choice whether or not to allow the processing of their personal data except where the users cannot freely withhold consent or where applicable law specifically allows the processing of personal data without the natural person's consent. The user's election must be freely given, specific and made on a knowledgeable basis;

- . Informing users, before obtaining consent, about their rights under the individual participation and access principle;

- . Providing users, before obtaining consent, with the information indicated by the openness, transparency and notice principle; and

- . Explaining to users the implications of granting or withholding consent.

##### Purpose legitimacy and specification

- . Ensuring that the purpose(s) complies with applicable law and relies on a permissible legal basis;

- . Communicating the purpose(s) to users before the information is used for the first time for a new purpose;

- . Using language for this specification which is both clear and appropriately adapted to the circumstances;

##### Data processing limitation

- . Limiting the gathering of personal data to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s).

- . Deleting and disposing of personal data whenever the purpose for personal data processing has expired, there are no legal requirements to keep the personal data, or whenever it is practical to do so.

##### Use, retention and disclosure limitation

- . Limiting the use, retention and disclosure of personal data to that which is necessary in order to fulfil specific, explicit and legitimate purposes;

- . Limiting the use of personal data to the purposes specified by Kaspersky Lab prior to receiving the data, unless a different purpose is explicitly required by applicable law;

- . Retaining personal data only as long as necessary to fulfill the stated purposes, and thereafter securely destroying or anonymizing it; and

- . Locking (i.e. archiving, securing and exempting the personal data from further processing) any personal data when and for as long as the stated purposes have expired, but where retention is required by applicable laws.

##### Accuracy and quality

- . Ensuring that the personal data processed is accurate, complete, up-to-date (unless there is a legitimate basis for keeping outdated data), adequate and relevant for the purpose of use;

- . Ensuring the reliability of personal data provided from a source other than from users before it is processed;
- . Verifying, through appropriate means, the validity and correctness of the claims made by the user prior to making any changes to the personal data (in order to ensure that the changes are properly authorized), where it is appropriate to do so;
- . Establishing personal data processing procedures to help ensure accuracy and quality; and
- . Establishing control mechanisms to periodically check the accuracy and quality of personal data processing.

#### Openness, transparency and notice

- . Providing users with clear and easily accessible information about Kaspersky Lab's policies;
- . Establishing procedures and practices with respect to the processing of personal data;
- . Including in notices the fact that personal data is being processed, the purpose for which this is done, the types of privacy stakeholders to whom the personal data might be disclosed, and the identity of the entity which determines the above and on how to contact;
- . Disclosing the options and means offered by Kaspersky Lab to users for the purposes of limiting the processing of, and for accessing, correcting and removing their information;
- . Giving notice to users when major changes in the personal data handling procedures occur.

#### Individual participation and access

- . Giving users the ability to contact us (by using the contact details provided in the "How to Contact Us") and review their personal data, provided their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law;
- . Allowing users (by using the contact details provided in the "How to Contact Us" or by using interface of our products and services) to challenge the accuracy and completeness of the personal data and have it amended, corrected or removed as appropriate and possible in the specific context;
- . Providing any amendment, correction or removal to personal data processors and third parties to whom personal data had been disclosed, where they are known; and
- . Establishing procedures to enable users to exercise these rights in a simple, fast and efficient way, which does not entail undue delay or cost.

#### Information Security: How We Protect Your Privacy

Information security is Kaspersky Lab's core business. All data and all information provided by you is confidential by default. Kaspersky Lab will therefore always apply technical and organizational data security measures for the protection of personal data that are adequate and appropriate, taking into account the concrete risks resulting from the processing of personal data as well as up-to-date security standards and procedures. In order to, among other reasons, identify and fulfill the appropriate level of protection, Kaspersky Lab classifies processing systems with personal data and implements cascading sets of protective measures.

Kaspersky Lab also maintains physical, electronic and procedural safeguards to protect the information against loss, misuse, damage or modification and unauthorized access or disclosure. Some of the other central features of our information security program are:

- . The Information Security Department, which designs, implements and provides oversight to our information security program;
- . A determination of personal data safety hazards in the course of processing in a Kaspersky Lab processing system;
- . Application of appropriate information security tools;
- . Performance evaluation of applied personal data security measures before commissioning processing systems;
- . Implementing controls to identify, authenticate and authorize access to various services or websites;
- . Discovering the facts surrounding unauthorized access to personal data and adopting corresponding measures;
- . Recovery of personal data that was modified or destructed;

- . Establishing access rules to personal data processed in Kaspersky Lab processing systems and also recording and accounting for all actions undertaken with personal data in these systems;
- . Encryption between our clients and servers (and between our various data centers);
- . We restrict access of our employees and contractors who need to know the information in order to process it for us and who are subject to strict contractual confidentiality obligations, to personal information. They may be disciplined or their contract terminated if they fail to meet these obligations;
- . Monitoring of our systems infrastructure to detect weaknesses and potential intrusions;
- . Monitoring measures taken to ensure the security of personal data;
- . Providing Kaspersky Lab personnel with relevant training and continually updating our security practices in light of new risks and developments in technology.

#### How to Contact Us

If you have any questions or comments about this Privacy Policy, Kaspersky Lab's privacy practices or if you would like us to update or remove information or preferences you provided to us, please visit <https://www.kaspersky.com/global-privacy-policy>, or, according to point (a) of Article 13 (1) and Article 27 (1) of Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR"), you may contact our Kaspersky Lab EU representative via e-mail or phone: Kaspersky Labs GmbH, Ingolstadt, Germany, [info@kaspersky.de](mailto:info@kaspersky.de), +49 (0) 841 98 18 90.

#### MICROSOFT SOFTWARE LICENSE TERMS MICROSOFT SQL SERVER 2017 EXPRESS

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- . updates,
- . supplements,
- . Internet-based services, and
- . support services

for this software, unless other terms accompany those items. If so, those terms apply.

BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.

We collect data about how you interact with this software. This includes data about the performance of the services, any problems you experience with them, and the features you use. This also includes data about your device and the network you use to connect to our services, including IP address, device identifiers, regional and language settings. It includes information about the operating systems and other software installed on your device, including product keys. By using this software, you consent to Microsoft's collection of usage and performance data related to your use of the software.

If you comply with these license terms, you have the rights below.

1. INSTALLATION AND USE RIGHTS. You may install and use any number of copies of the software on any device including third party shared devices.
2. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.
  - a. Distributable Code.
    - i. Right to Use and Distribute. If you comply with the terms below:
      - . You may copy and distribute the object code form of the software ("Distributable Code") in programs you develop;
      - . You may combine the object code form of the Distributable Code with your programs to develop a unified web solution and permit others via online methods to access and use that unified web solution, provided that the Distributable Code is only used as part of and in conjunction with your programs; and
      - . You may permit distributors of your programs to copy and distribute the Distributable Code as part of those programs.
    - ii. Distribution Requirements. For any Distributable Code you distribute, you must
      - . add significant primary functionality to it in your programs;
      - . for any Distributable Code having a filename extension of .lib, distribute only the results of running such Distributable Code through a linker with your program;

- . distribute Distributable Code included in a setup program only as part of that setup program without modification;
- . require distributors and external end users to agree to terms that protect it at least as much as this agreement;
- . display your valid copyright notice on your programs; and
- . indemnify, defend, and hold harmless Microsoft from any claims, including attorneys' fees, related to the distribution or use of your programs.

iii. Distribution Restrictions. You may not

- . alter any copyright, trademark or patent notice in the Distributable Code;
- . use Microsoft's trademarks in your programs' names or in a way that suggests your programs come from or are endorsed by Microsoft;
- . distribute Distributable Code to run on a platform other than the Windows platform;
- . include Distributable Code in malicious, deceptive or unlawful programs; or
- . modify or distribute the source code of any Distributable Code so that any part of it becomes subject to an Excluded License. An Excluded License is one that requires, as a condition of use, modification or distribution, that
  - . the code be disclosed or distributed in source code form; or
  - . others have the right to modify it.

b. Hosting. You may use the software for commercial software hosting services, subject to the following terms:

i. You are Fully Responsible. If you use the software for commercial hosting purposes, you will be legally responsible for all usage of the software by your end users.

i. Indemnity. You must defend, indemnify and hold Microsoft harmless from any claim arising as a result of (1) your improper installation of the software; (2) any software virus introduced by you; (3) your violation of the terms of this agreement; and (4) unauthorized installation, use, access, copying, reproduction, and/or distribution of any portion of the software by an end user (or any third party providing services to the end user).

ii. No High Risk Use. The software is not fault-tolerant and is not guaranteed to be error free or to operate uninterrupted. You must not grant the right to use the software in any application or situation where the software failure could lead to death or serious bodily injury of any person, or to severe physical or environmental damage ("High Risk Use"). Examples of High Risk Use include, but are not limited to: aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles, or weaponry systems. High Risk Use does not include utilization of software for administrative purposes, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control, but must not be directly or indirectly responsible for the control function. You agree to indemnify and hold harmless Microsoft from any third-party claim arising out of end users' use of the software in connection with any High Risk Use.

iii. Compliance with license requirements. You must (1) inform the individuals who have access to the software that the software is licensed by Microsoft, and (2) bind individuals who have access to the software to terms that protect the software at least as much as the terms of this agreement. You will use commercially reasonable efforts to prevent any unauthorized distribution, copying, use, or pirating of the software.

3. SCOPE OF LICENSE. The software is licensed, not sold. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not

- . disclose the results of any benchmark tests of the software to any third party without Microsoft's prior written approval;
- . work around any technical limitations in the software;
- . reverse engineer, decompile or disassemble the software, or otherwise attempt to derive the source code for the software except, and only to the extent: (i) permitted by applicable law, despite this limitation or (ii) required to debug changes to any libraries licensed under the GNU Lesser Public License that are included with and linked to by the software;

. make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;

. publish the software for others to copy;

. rent, lease or lend the software except as permitted under Section 2.b.

("Hosting") of this agreement.

4. THIRD PARTY NOTICES. The software may include third party components with separate legal notices or governed by other agreements, as may be described in the ThirdPartyNotices file accompanying the software. Even if such components are governed by other agreements, the disclaimers and the limitations on and exclusions of damages below also apply.

5. BACKUP COPY. You may make one backup copy of the software. You may use it only to reinstall the software.

6. DOCUMENTATION. Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.

7. TRANSFER TO A THIRD PARTY. The first user of the software may transfer it and this agreement directly to a third party. Before the transfer, that party must agree that this agreement applies to the transfer and use of the software. The first user must uninstall the software before transferring it separately from the device. The first user may not retain any copies.

The provisions of this section do not apply if you acquired the software as a consumer in Germany or in any of the countries listed on this site (aka.ms/transfer), in which case any transfer of the software to a third party, and the right to use it, must comply with applicable law.

8. EXPORT RESTRICTIONS. The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see [www.microsoft.com/exporting](http://www.microsoft.com/exporting).

9. SUPPORT SERVICES. Because this software is "as is," we may not provide support services for it.

10. ENTIRE AGREEMENT. This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.

11. APPLICABLE LAW.

a. United States. If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

b. Outside the United States. If you acquired the software in any other country, the laws of that country apply.

12. LEGAL EFFECT. This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.

13. DISCLAIMER OF WARRANTY. THE SOFTWARE IS LICENSED "AS-IS." YOU BEAR THE RISK OF USING IT. MICROSOFT GIVES NO EXPRESS WARRANTIES, GUARANTEES OR CONDITIONS. YOU MAY HAVE ADDITIONAL CONSUMER RIGHTS UNDER YOUR LOCAL LAWS WHICH THIS AGREEMENT CANNOT CHANGE. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAWS, MICROSOFT EXCLUDES THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

FOR AUSTRALIA - you have statutory guarantees under the Australian Consumer Law and nothing in these terms is intended to affect those rights.

14. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. \$5.00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES.

This limitation applies to

. anything related to the software, services, content (including code) on third party Internet sites, or third party programs, and

. claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may

not allow the exclusion or limitation of incidental, consequential or other damages.

15. CANADA.Â You may stop receiving updates by turning off the automatic update feature or by turning off Internet access. Refer to the product documentation to learn how to turn off updates for your specific device or software.