KASPERSKY SECURITY FOR MICROSOFT OFFICE 365 AGREEMENT

This agreement ("**Agreement**") contains the terms and conditions that govern your access to and use of the Kaspersky Security for Microsoft Office 365 ("**Product**") and is an agreement between AO Kaspersky Lab ("**Kaspersky Lab**" or "**Kaspersky**") and you ("**User**" or "**You**"), as the organization have authorized the natural person accepting this Agreement to enter into this Agreement for and on behalf of You. This Agreement takes effect when you click the "I Accept" button or check the box indicating Your agreement to these terms.

If there is a separate agreement entered into between Kaspersky Lab and the You, or between You and the corresponding authorized partner of Kaspersky Lab ("**Partner**"), to the extent the separate agreement ("**Separate Agreement"**) between Kaspersky Lab or Partner and the You conflicts with any provisions of this Agreement, such Separate Agreement shall prevail.

SECTION A: GENERAL TERMS

1. Overview of the Product

Kaspersky Security for Microsoft Office 365 is a software solution designed for protection of Exchange Online mailboxes managed through Office 365. Email messages are scanned for viruses, Trojans, and other types of malware that can be transmitted via email, as well as spam and phishing.

Kaspersky Security for Microsoft Office 365 can perform the following operations:

- scan email messages in user mailboxes for malware;
- filter unsolicited mail (spam) from user mailboxes;
- scan email messages for phishing and malicious links;
- filter attachments in email messages;
- move messages to backup to prevent infection;
- provide the common view for items located in Kaspersky Security backup and Exchange Online quarantine, thus allowing the Administrator to review all the security violations and, if necessary, to locate and release selected items;
- notify about messages that contain malicious objects, filtered attachments and/or phishing;
- display statistics and generate reports on Product activity.

Kaspersky Security for Microsoft Office 365 is deployed in the Kaspersky Lab infrastructure. The functionality of the Kaspersky Security for Microsoft Office 365 is provided in the online help ("**Online Help**").

2. Grant and Limitations of License

2.1. **License**. Kaspersky Lab grants the User a non-exclusive, non-transferable limited license to access and use the Product in accordance with this Agreement and solely for the User's internal business purposes. User must comply with all technical requirements provided in the Online Help. Additional conditions and restrictions on use of the Product shall be specified in the applicable License Certificate (as defined below) and/or in the Separate Agreement.

2.2. **License Certificate**. License Certificate is the separate file generated by Kaspersky Lab upon execution of an order by the User. License Certificate contains the main information with a description of the license to Product(s).

2.3. **Access to Product**. Product is provided by means of granting to User access to the web-based portal at cloud.kaspersky.com ("**Portal**"). User will identify the username and password that are used for access to User's account on Portal. User will not share its username or password with any third party and will be responsible and liable for the acts or omissions of any person who accesses Product using passwords or access procedures provided to User. Kaspersky Lab reserves the right to refuse registration of, or to suspend or cancel, login IDs used by User to access the Product for any reason, including if User violates the terms and conditions set forth in this Agreement.

2.4. Kaspersky Lab reserves the right at any time to change the Product and/or its components including but not limited to Online Help.

2.5. With the exception of the DPA (as defined in the section "DATA PROCESSING AND PRIVACY TERMS"), Kaspersky Lab reserves the right at any time to modify this Agreement and to impose new or additional terms or conditions on the use of the Product. Such modifications will be effective immediately when incorporated into the Agreement. Continued use of the Product by You will be deemed acceptance thereof.

3. User Obligations

3.1. User must comply with, and may not work around, any technical limitations in the Product as specified in the Online Help.

3.2. User must comply with all laws and regulations applicable to its use of the Product, including but not limited to all applicable laws related to privacy, personal data, data protection and confidentiality of communications. User is responsible for responding to any request from a third party regarding User's use of the Product.

3.3. User shall not sell, rent, lease, or lend the Product to any third party or use the Product to create own products or services used for detection, blocking, or treating threats or any other purpose.

3.4. User may not remove or alter any copyright notices or other proprietary notices of the Product, related documentation or materials.

3.5. User may not probe, scan or test the vulnerability of the Product or Portal or any related system or networks, or violate any safety measures or verification checks used in connection with the Product and Portal and such systems and networks.

3.6. If the User violates any of its obligations hereunder or license limitations stipulated in this Agreement or other legally binding document entered into between User and Kaspersky Lab and/or Partner(s), Kaspersky Lab may revoke the license and disable use of the Product.

4. Term and Termination

4.1. **Term**. The initial expiration date of the license is specified in the License Certificate. User has the option to renew the license to the Product for one or more additional time period upon execution of an additional order of the Product. In that case User has the license to use the Product during the renewal term. This Agreement shall remain in effect for the entire term of the license ("**License Term**").

4.2. **Termination**. In the event of material breach of this Agreement by User, Kaspersky Lab may immediately terminate this Agreement and the License to use Product by without written notice to User. For any other breach of this Agreement, Kaspersky Lab may provide User with fifteen (15) days written notice of such breach and if User does not cure the breach within the fifteen (15) day notice period, Kaspersky Lab may immediately terminate this Agreement. Upon any termination, User's right to use and access the Product shall be terminated.

5. Payment

5.1. **Payment**. License fees and all applicable taxes payable are due within the period specified in the invoice provided to User by Kaspersky Lab or Partner.

6. Trial Use

6.1. User may order a version of the Product for trial use. Upon Kaspersky Lab’s acceptance of the order, User may access and use the Product for evaluation purposes and non-production purposes only. User has thirty (30) days to use the Product as specified in this Clause. If Kaspersky Lab sets another duration for the applicable trial period, User will be informed prior to User providing credentials for access and use. Kaspersky Lab does not provide technical support during trial use of the Product.

7. Technical Support

7.1. During the License Term of this Agreement, Kaspersky Lab provides User with technical support service for the Product (except during trial use of the Product) in accordance with technical support rules. Technical support service and its rules are located at: https://support.kaspersky.com.

8. Electronic Notices

8.1. Kaspersky Lab may provide User with important information and notices about the Product electronically, including via email and the Portal. For such aims Kaspersky Lab may use all necessary information about You, including information about User's account on the Portal.

9. Limited Warranty and Disclaimer

9.1. Product may contain or show links to third-party websites or resources in relation to the Product. Kaspersky Lab provides these links for convenience only and is not responsible for the content, resources, or links to products or services that they provide. You accept sole responsibility and assume all risk when using third-party websites or resources.

9.2. Kaspersky Lab and/or Partners are not responsible for any delays in, failures of, and access denial to the Products which may be caused by Your Internet or mobile service provider.

9.3. EXCEPT FOR KASPERSKY LAB OBLIGATIONS STATED HEREBY THE PRODUCT IS PROVIDED "AS IS" AND 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. KASPERSKY LAB 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, NON-INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. USER ASSUMES ALL RESPONSIBILITY, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE PRODUCT TO ACHIEVE USER INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE PRODUCT. WITHOUT LIMITING THE FOREGOING PROVISIONS, KASPERSKY LAB MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE PRODUCT WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE PRODUCT WILL MEET ANY OR ALL OF USER REQUIREMENTS WHETHER OR NOT DISCLOSED TO KASPERSKY LAB.

10. Exclusion and Limitation of Liability

10.1. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL KASPERSKY LAB 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 PRODUCT, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER PRODUCTS, INFORMATON, SERVICE AND RELATED CONTENT THROUGH THE

PRODUCT OR OTHERWISE ARISING OUT OF THE USE OF THE PRODUCT, 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 KASPERSKY LAB, EVEN IF KASPERSKY LAB HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

11. Intellectual Property Ownership

11.1. You agree that the Product and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Product are proprietary intellectual property and/or the valuable trade secrets of the Kaspersky Lab or its Partners and that the Kaspersky Lab and its Partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patents of the Russian Federation, European Union and the United States, as well as other countries and international treaties.
This Agreement does not grant You any rights to the intellectual property, including any Trademarks or Service Marks of the Kaspersky Lab and/or its Partners ("**Trademarks**"). You may use the Trademarks only insofar as to identify printed output produced by the Product 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 Kaspersky Lab and/or its Partners own and retain all right, title, and interest in and to the Product, including without limitation any error corrections, enhancements, updates or other modifications to the Product, whether made by the Kaspersky Lab 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 Product does not transfer to you any title to the intellectual property in the Processor, and you will not acquire any rights to the Product except as expressly set forth in this Agreement. All copies of the Product made hereunder must contain the same proprietary notices that appear on and in the Product. Except as stated herein, this Agreement does not grant You any intellectual property rights in the Product 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. Kaspersky Lab reserves all rights not expressly granted to you in this Agreement.

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

12. Governing Law

12.1. Except as provided in Clauses 12.2 and 12.3 below, this Agreement shall be governed by and construed in accordance the laws specified below for the country or territory in which You obtained the License Certificate, without reference to or application of conflicts of laws principles:
a. **Russia**. If you obtained the License Certificate in Russia, the laws of the Russian Federation.

b. **United States, Puerto Rico, American Samoa, Guam, and U.S. Virgin Islands**. If you obtained the License Certificate in the United States, Puerto Rico, American Samoa, Guam or the U.S. Virgin Islands, the laws of the Commonwealth of Massachusetts, USA, provided, however, that the laws of the U.S. state where you live will govern claims under state consumer protection, unfair competition, or similar laws. To the fullest extent permitted by law, the Kaspersky Lab and you expressly agree hereby to waive any right to a trial by jury.
c. **Canada**. If you obtained the License Certificate in Canada, the laws of the Province of Ontario.
d. **Mexico**. If you obtained the License Certificate in Mexico, the federal laws of the Republic of Mexico.
e. **European Union (EU)**. If you obtained the License Certificate in a member country of the EU, the laws of Germany.
f. **Australia**. If you obtained the License Certificate in Australia, the laws of the State or Territory in which you obtained the license.
g. **Hong Kong Special Administrative Region (SAR) and Macau SAR**. If you obtained the License Certificate in Hong Kong SAR or Macau SAR, the laws of Hong Kong SAR.
h. **Taiwan**. If you obtained the License Certificate in Taiwan, the laws of Taiwan.
i. **Japan**. If you obtained the License Certificate in Japan, the laws of Japan.
j. Any Other Country or Territory. If you choose to obtain the License Certificate in another country, the substantive laws of the country where the purchase took place will be in effect.

12.2. Notwithstanding the foregoing, if the mandatory laws or public policy of any country or territory in which this Agreement is enforced or construed prohibit the application of the law specified herein, then the laws of such country or territory shall instead apply to the extent required by such mandatory laws or public policy. Similarly, if you are an individual consumer, the provisions of clause 12.1 shall not affect any mandatory right you may have to take action in your country of residence under the laws of that country.

12.3. 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.

12.4. User is responsible for contacting only the Kaspersky Lab or their Partners directly if having any problems with the product.

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. 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 Kaspersky Lab provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Kaspersky Lab'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.

SECTION B: DATA PROCESSING AND PRIVACY TERMS

1. Data Processing on behalf of the User

1.1. Product is used by the User to protect Exchange Online mailboxes under the control of the User, during which the User collects, stores, and processes data, which may include personal data ("**User Data**").

1.2. User Data, including Personal Data as so defined under the EU General Data Protection Regulation 2016/679 ("**GDPR**"), provided to Kaspersky Lab on User's behalf, if any, and the processing thereof, shall be governed under the terms and conditions set forth in the Kaspersky Security for Microsoft Office 365 Data Processing Agreement ("**DPA**"). Kaspersky Lab shall provide prior notification to the User upon any material change to the DPA.

1.3. The DPA is an integral part of this Agreement. Unless otherwise explicitly agreed in writing between the User and Kaspersky Lab and/or Partner, it is agreed and acknowledged that the User is the **Controller** and Kaspersky Lab is the **Processor** (as defined under the GDPR and the DPA), in particular with respect to any Personal Data included in the User Data. The list of data and purposes of processing data are specified in the DPA.

1.4. User will have the ability to access User Data stored in the Product in the Kaspersky Lab infrastructure and systems. Kaspersky Lab will retain User Data in the User account in restricted mode for the duration specified in the Online Help following the expiration or termination of User license so that User may extract the User Data. Upon conclusion of the retention period, Kaspersky Lab will delete the User Data. Kaspersky Lab has no liability for the deletion of User Data as described in this Clause.

1.5. User is solely responsible for acquainting itself with the Online Help, in particular, the DPA and the Section "Data Processing and Privacy Terms" of this Agreement. The User is solely responsible for independently determining whether the foregoing documents and documents referenced therein comply with the User's requirements.

1.6. During use of the Product, the User is fully responsible for ensuring that the processing of Personal Data included in the User Data is lawful, particularly, within the meaning of Article 6 (1)

(a) to (f) of GDPR (if the administrated computer or mobile device is in the European Union) or applicable laws on confidential information, personal data, data protection, or similar thereto.

1.7. User shall be fully liable in relation to Kaspersky Lab for any damage resulting from a breach of this Agreement, especially in relation to the Section "Data Processing and Privacy Terms", or DPA.

1.8. User shall indemnify Kaspersky Lab in relation to third parties from any claim arising from the failure of the User to fulfill obligations under the Section "Data Processing and Privacy Terms" of this Agreement which third parties, especially data protection authorities, assert against Kaspersky Lab.

2. Data Processing for the Product

2.1. **Purposes of Processing Data**. During use of the Product, processing data is necessary to protect the User from known threats to information security, as described in the Online Help and to ensure uninterrupted performance of the Product. Such information may be considered personal according to applicable laws of certain countries. The Controller is Kaspersky Lab in relation to data described in the Subsection 2 "Data Processing for the Product".

Processed Data.

The following data will be processed by Kaspersky Lab on a regular basis to protect the User from known threats to information security:
- IP address belonging to the sender of the scanned message.
- The checksums (MD5, SHA2-256, SHA1) of the scanned object.
- URL address for which the reputation is being requested.
- Top-level domain names used in web addresses in the scanned messages.
- Checksum (MD5) of the names of files attached to the message.
- The number of IP addresses (v4 and v6) in the message header and a flag indicating the address belonging to the local or external network.
- Irreversible hash function of domain names in the header of the scanned message.
- Message scan result and spam rating.
- Checksum (MD5) of the scanned message sender's email address.
- URL addresses from scanned messages with deleted passwords.
- Checksums (MD5) of graphic objects included in the message.
- Short text signatures composed from message text (irreversible text digests that cannot be used to recover the original text, the text itself is not transmitted) used for filtering known spam mailings and product decisions about them.
- IP addresses of the message sender and intermediate mail servers, sender’s mail client version, message ID, information about the completion of message fields, the checksum (CRC32) of message fragments defined by markup language, sender domain names taken from the SMTP session and MIME-header, checksums (CRC23) of the sender name taken from the SMTP-session

and MIME-header, checksums (CRC32) of the sender's name and domain taken from the SMTP session.

The following data will be processed by Kaspersky Lab on a regular basis to ensure uninterrupted performance of the Product:
- Message size
- Scanned object size and type
- Message subject
- Message ID
- EWS object ID
- Mailbox name and primary SMTP address
- Name of Exchange Online organization
- Message timestamp
- Message sender
- Message recipients
- Message scan result
- IP address and anonymized email address of the administrator who has modified Product settings
- The list of settings that have been modified, without indicating the actual parameter values
- Kaspersky Security for Microsoft Office 365 organization ID, date of organization setup, IP-address of the computer used to set up the organization
- License type
- Number of detections with the following statuses assigned: Clean / Infected / Spam / Mass mail / Phishing / Attachment filtering
- Number of objects in Kaspersky Security for Microsoft Office 365 backup and Exchange Online quarantine
- Total number of mailboxes in the organization, number of mailboxes covered by the license, number of mailboxes selected for protection
- Protection status (module disabled / module enabled) for each application module (Anti-Virus, Anti-Phishing, Anti-Spam, Attachment Filtering by file format, file mask, Microsoft Office files containing macros), selected action to take on detected objects
- Number of users (Active Directory user objects) in the organization

2.2. **Data Protection and Processing**. Kaspersky Lab handles the data it receives from the User under provisions of this Subsection 2 “Data Processing for the Product” in accordance with Kaspersky Lab’s Privacy Policy published at: https://www.kaspersky.com/Products-and-Services-Privacy-Policy.

2.3. During use of the Product, the 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 GDPR (if data subject is in the European Union) or applicable laws on confidential information, personal data, data protection, or similar thereto.

2.4. In case that the User wants to base the lawfulness of the processing on the consent of its data subjects, the 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 User prior to using the Product. The User guarantees that consent of each data subject of the User was obtained prior to the processing of Personal Data.

2.5. It is agreed between the Kaspersky Lab and User that, in case of item 2.4 of this Subsection, the 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 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 Kaspersky Lab within 5 business days starting with the request of the Kaspersky Lab.

2.6. Furthermore, in case of item 2.4 of this Subsection, the 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 the processing of Personal Data. In particular, the User is obliged to provide each data subject in the European Union, or where applicable law requires, with the Kaspersky Lab's Privacy Policy (https://www.kaspersky.com/Products-and-Services-Privacy-Policy) prior to the processing of Personal Data.

2.7. The User shall be fully liable in relation to the Kaspersky Lab for any damage resulting from a breach of this Agreement, in particular the 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.

2.8. The User shall indemnify the Kaspersky Lab in relation to third parties from the claims arising from the failure of User to fulfill obligations under Subsection 2 "Data Processing for the Product" which third parties, especially the supervisory data protection authorities, assert against the Kaspersky Lab.

Kaspersky Security for Microsoft Office 365 Agreement version 1.0

This version of the Agreement is effective as of May 25, 2018.

The latest version of this Agreement is available at https://cloud.kaspersky.com/Home/LegalDocuments

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 effective immediately upon being posted to our website: www.kaspersky.com/Products-and-Services-Privacy-Policy

This version of the policy is effective as of February 1, 2018

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 ALL OBLIGATIONS UNDER THE CONTRACT;**
- **KASPERSKY SECURITY NETWORK STATEMENT, WHICH DESCRIBES THE DATA NECESSARY FOR INCREASING THE EFFECTIVENESS OF YOUR PROTECTION;**
- **MARKETING STATEMENT, WHICH DESCRIBES THE DATA NECESSARY FOR IMPROVING APPLICATION PERFORMANCE AND TO HELP US ANALYZE USER SATISFACTION;**
- **FEATURE-RELATED STATEMENTS, WHICH DESCRIBE DATA PROCESSING IN RELATION TO SOME FEATURES OF THE PRODUCT, LIKE ANTI-SPAM. YOU CAN FAMILIARIZE YOURSELF WITH THESE STATEMENTS WHEN YOU DECIDE TO TURN ON THE FEATURES IN THE PRODUCT.**

FOR BUSINESS USERS (B2B):

- **KASPERSKY SECURITY NETWORK STATEMENT, WHICH DESCRIBES THE DATA NECESSARY FOR INCREASING THE EFFECTIVENESS OF YOUR PROTECTION. FOR SOME PRODUCTS, THE IT-ADMINISTRATOR OR ANY OTHER EMPLOYER RESPONSIBLE FOR SETTING UP THE PRODUCT WILL BE ABLE TO 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. We filter out information regarding logins and passwords from transmitted URLs, even if they are stored in the initial browser request from the user.

- 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 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 and how we share it

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
- Switzerland

Outside of the EU or EEA:

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

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

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 links to products of third parties whose privacy practices differ from Kaspersky Lab's. If you provide personal data to any of those products, your data is governed by their 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, update and correct inaccuracies in your personal data, object to the processing of your personal data, and have the information blocked, anonymized or deleted, as appropriate. The right to access personal data may be limited in some circumstances by the requirements of local law. To exercise these rights, 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, contact us electronically via: https://support.kaspersky.com/privacy; or send us a letter to the Kaspersky Lab Privacy Office: AO Kaspersky Lab, Bldg. 3, 39A, Leningradskoe Shosse, Moscow, 125212, Russian Federation.

KASPERSKY SECURITY FOR MICROSOFT OFFICE 365 DATA PROCESSING AGREEMENT

This data processing agreement ("**DPA**") forms an integral part of the Kaspersky Security for Microsoft Office 365 Agreement ("**Agreement**") on provision of the Kaspersky Security for Microsoft Office 365 ("**Product**") between Kaspersky Lab and User. The attached annex(es) and appendices supplement the terms of this DPA. If the parties previously entered into a data processing agreement for Product, this DPA shall now supersede the foregoing.

All terms used in this DPA have the same meaning as in the Agreement. Terms used here with reference to the EU General Data Protection Regulation (2016/679), such as "personal data breach," "processing," "controller," "processor," and "data subject," will have the same meaning as set forth in Article 4 of the GDPR.

This DPA specifies the terms and conditions for activities of commissioned processing of User Data, especially in relation to the processing of personal data ("Personal Data") included in User Data, in connection with the Agreement.

1. Scope and Roles

1.1. This DPA applies to the processing of User Data by Kaspersky Lab on behalf of User.

1.2. User and Kaspersky Lab agree that User is the controller ("**Controller**") of User Data and Kaspersky Lab is the processor ("**Processor**") of such data.

1.3. This DPA does not limit or reduce any data protection commitments Kaspersky Lab makes to User in the Agreement or other agreement between User and Kaspersky Lab and/or its Partners.

1.4. User Data will be used only for the purpose of providing User with the Product, including purposes necessary to and consistent with providing the Product, as specified in the Annex 1 of this DPA. User retains all rights, title, and interest in and to User Data. Kaspersky Lab does not acquire any rights in User Data other than the rights necessary to provide the Product to the User.

1.5. DPA will remain in full force and effect until all of the User Data is deleted or extracted from Kaspersky Lab's systems in accordance with the Agreement and Annex 1 of this DPA.

1.6. This DPA does not apply where Kaspersky Lab is a controller processed data.

1.7. Before using the Product, the User must specify the location of its organization. The specified location of the organization will determine where the User Data will be processed according to the Online Help by Kaspersky Lab or its affiliates or sub-contractors. In accordance with this instruction User appoints Kaspersky Lab to perform transfer of User Data to the chosen location and to store and process User Data in order to provide the Product. Kaspersky Lab does not control or limit the regions from which User or User's end users may access or move User Data.

1.8. When providing technical support service to User, Kaspersky Lab will have access to the User Data from Russia.

1.9. Annex 2 to this DPA is the Standard Contractual Clauses (processors), which are based on the Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of Personal Data to processors established in third countries, under Directive 95/46/EC). Standard Contractual Clauses apply to the transfer and processing of Personal Data outside of the EEA to a third country which does not otherwise provide adequate protection for personal data, in the course of providing the Product. Standard Contractual Clauses shall prevail over any conflicting section of the DPA and/or the Agreement.

2. Kaspersky Lab Obligations

2.1. Kaspersky Lab shall not engage another processor without prior specific or general written authorization of User. In the case of general written authorization, Kaspersky Lab shall inform User of any intended changes concerning the addition or replacement of other processors, thereby giving User the opportunity to object to such changes.

2.2. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of User Data, the categories of data subjects and the obligations and rights of the User are set forth in the Agreement, including this DPA. In particular, Kaspersky Lab shall:

- process User Data, including with regard to transfers of User Data to a third country or an international organization, only in accordance with User's instructions within the scope of and for purposes of Product as described in the Agreement and this DPA. The Agreement including this DPA, along with User's use and configuration of features in the Product, are User's complete instructions to Kaspersky Lab for the processing of User Data.
- ensure that persons authorized to process the User Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- take all measures required pursuant to Article 32 of the GDPR;
- respect the conditions for engaging another processor;
- taking into account the nature of the processing, assist User by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the User's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;
- assist User in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to Kaspersky Lab;
- at the choice of User, delete or return all the User Data to User after the end of the provision of Product, and delete existing copies;
- make available to User all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by User or another auditor mandated by User.

2.3. Kaspersky Lab shall notify User without undue delay after becoming aware of a personal data breach in a form required by the law. Notification(s) will be delivered to one or more of User's administrators by any means Kaspersky Lab selects, including via email. It is User's sole responsibility to ensure User's administrators maintain accurate contact information. Obligation to report or respond about a personal data breach is not an acknowledgement by Kaspersky Lab of any fault or liability with respect to that a personal data breach.

2.4. Kaspersky Lab shall implement and maintain appropriate technical and organizational measures intended to protect User Data as described in Annex 1 Subsection 2 of this DPA against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction. The technical and organizational measures are subject to technical progress and development. Kaspersky Lab may implement adequate alternative measures that provide at least the same level of security as the specified measures.

2.5. User and Kaspersky Lab shall take steps to ensure that any person acting under the authority of User or Kaspersky Lab who has access to User Data does not process them except on instructions from User.

3. User Obligations

3.1. User shall be responsible for compliance with applicable data protection regulations and laws including but not limited to all transfer of User Data to Kaspersky Lab.

3.2. User may notify Kaspersky Lab in written form and within thirty (30) days after expiration or termination of the User license extract User Data by reasonable measures or delete the stored User Data. User shall notify Kaspersky Lab without undue delay, if User is unable to retrieve User Data within this time period. After the time period has elapsed without notification by User, Kaspersky Lab shall delete all stored User Data, unless Kaspersky Lab is legally prohibited to do so.

4. User Audit

4.1. User shall be allowed to audit Kaspersky Lab's compliance with Kaspersky Lab's obligations under this DPA as required by applicable data protection laws. For this purpose, Kaspersky Lab shall reasonably support User and upon written request by User provide the necessary information.

4.2. After notifying Kaspersky Lab at least five weeks in advance, User may also conduct the audit by an on-site inspection of Kaspersky Lab's data processing facilities and activities during regular business hours and without serious interruption of Kaspersky Lab's daily operations. To conduct the audit on its behalf, User may also select a sufficiently qualified independent third party auditor, who has been obligated to confidentiality and shall not be a competitor of Kaspersky Lab.

4.3. User shall document the audit process and provide Kaspersky Lab with a report on all determined breaches of Kaspersky Lab's obligations under this DPA, if applicable. User and Kaspersky Lab will agree on reasonable measures to ensure future compliance.

4.4. User shall bear all costs for conducting audits and will reimburse Kaspersky Lab for any personal resources expended to support the audit at Kaspersky Lab's then current professional services rates.

5. Sub-processing

5.1. User authorizes Kaspersky Lab to engage sub-processors for the processing of User Data in accordance with this DPA. A list of current sub-processors is available under the following URL https://help.kaspersky.com/Cloud/1.0/en-US/172033.htm. At least fourteen (14) days before authorizing any new sub-processor to access User Data, Kaspersky Lab will provide the notice to User about it.

5.2. Kaspersky Lab will ensure that sub-processors are bound by written agreements that require them to provide at least the level of data protection required of Kaspersky Lab by this DPA.

6. Severability

6.1. The term of this DPA follows the term of the Agreement. Where individual provisions of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

ANNEX 1. ADDITIONAL TERMS OF DATA PROCESSING AND SECURITY

1. Additional Terms of Data Processing

1.1. **Duration of data processing**. The duration of data processing shall be for the duration of License Term. After expiration or termination of User license, Kaspersky Lab will delete or return User Data in accordance with the terms and timelines set forth in the Agreement.

1.2. **Reason for data processing**. The reason for data processing is to provide the Product to User, to provide technical support to the User, to fulfill other obligation under the Agreement.

1.3. **Category of data subjects**. The categories of data subjects are User's representatives and end users, such as employees, contractors, collaborators, and customers.

1.4. **Scope and purposes of processing personal data**. Product is used by the User for the purpose of protecting Exchange Online mailboxes under the control of the User. For such purposes, Processor may receive, store, and process the following types of data:

1) Office 365 Global Administrator credentials required for authorizing the creation of a Service Account with the necessary permissions in Exchange Online. The Product does not depend on the Global Administrator account after the Service Account has been created, and does not store its credentials for future use.
2) Service Account credentials used to connect the Product to Office 365.
3) A list of all mailboxes of the protected Exchange Online organization.
4) A list of all accepted domains in the protected Exchange Online organization.
5) Email messages and appointments, message attachments and X-headers.
The Product receives these items for scanning and processes them according to the protection settings. Email messages and items are not stored in the Kaspersky Security for Microsoft Office 365 infrastructure.
6) The metadata of email messages (sender, recipient, subject, primary SMTP address of the related mailbox).
7) The email address specified during registration and the corresponding IP address.
8) Product settings available at Portal.
9) Email addresses excluded from scanning.
10) Email addresses specified in notification settings.
11) Statistics on Product operations (senders, recipients, subjects and scan results of email messages).
12) Active Directory group names, group IDs and information about group membership.

1.5. **Technical support**. Kaspersky Lab will have access to and process the User Data to provide technical support service. User Data will be used only for the purpose of providing support, including purposes necessary to and consistent with providing support, such as troubleshooting recurring issues and making improvements to support and/or to the Product. Technical support service and its rules are located at: https://support.kaspersky.com

2. Security

2.1. Kaspersky Lab has implemented and will maintain and adhere to the following security measures for the Product, which are Kaspersky Lab's only responsibility with respect to the security of User Data:

Organization of Information Security
1. There have been appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures
2. Personnel with access to User Data are subject to confidentiality obligations.
3. There has been performed a risk assessment before processing the User Data or launching the services.

Asset Management
4. Inventory of all assets (which User Data is stored) is maintained. Access to inventories of such media is restricted to personnel authorized to have such access.
5. User Data is classified to help identify it and to allow for access to it to be appropriately restricted.
6. It is required to obtain special authorization prior to storing User Data on portable devices, remotely accessing User Data, or processing User Data outside company facilities.

Human Resources Security
7. Kaspersky Lab informs its personnel about relevant security procedures and their respective roles.
8. Kaspersky Lab also informs its personnel of possible consequences of breaching the security rules and procedures.
9. Kaspersky Lab performs training about personal data security.

Physical and Environmental Security
10. Kaspersky Lab limits access to facilities where information systems that process User Data are located to identified authorized individuals:

- 7x24 security service is provided by security guards
- Perimeter access is controlled by Electronic Access Card System
- Turnstile is used with proximity card at all entrance points
- Employees must wear the Kaspersky Lab badge
- Visitors are registered and they must wear visitor badges; visitors are accompanied during their visit

- All perimeter access and secure areas are monitored with CCTV, which is monitored by the security guards

11. Kaspersky Lab maintains records of the incoming and outgoing media, including the kind of media, the authorized sender/recipients, date and time, the number of media.
12. A variety of industry standard systems to protect against loss of data due to power supply failure or line interference is used.
13. Industry standard processes to delete User Data when it is no longer needed are used.

Communications and Operations Management
14. Kaspersky Lab maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to User Data.
15. Copies of User Data and data recovery procedures are stored in a different place from where the primary computer equipment processing the User Data is located.
16. Antimalware controls to help prevent against malicious software from gaining unauthorized access to User Data, including malicious software originating from public networks, are used.
17. User Data, which is transmitted over public networks, is encrypted.
18. Kaspersky Lab logs access and use of information systems containing User Data, registering the access ID, time, authorization granted or denied, and relevant activity.

Access Control
19. Kaspersky Lab maintains and updates a record of personnel authorized to access systems that contain User Data.
20. Kaspersky Lab identifies those personnel who may grant, alter or cancel authorized access to data and resources.
21. Kaspersky Lab ensures that where more than one individual has access to systems containing User Data, the individuals have separate identifiers/log-ins.
22. Technical support personnel are only permitted to have access to User Data when needed.
23. Kaspersky Lab restricts access to User Data to only those individuals who require such access to perform their job function.
24. Kaspersky Lab implements role based access control
25. Personnel have been instructed to disable administrative sessions when leaving premises controls or when computers are otherwise left unattended.
26. Passwords are stored in a way that makes them unintelligible while they are in force.
27. Kaspersky Lab uses industry standard practices to identify and authenticate users who attempt to access information systems.
28. Kaspersky Lab has established a password policy that prohibits the sharing of passwords, governs what to do if a password is disclosed, requires passwords to be changed on a regular basis and default passwords to be altered;
29. Kaspersky Lab password policy defines password complexity requirements;
30. All passwords are stored using a one-way hashing algorithm and are never transmitted unencrypted.
31. Kaspersky Lab has controls to prevent individuals from assuming access rights they have not been assigned to gain access to User Data they are not authorized to access.

32. Kaspersky Lab internal network channel is protected by implementing firewalls.
33. All data transfers between the Kaspersky Lab, legal, entities and partners and customers are protected with TLS/SSL protocol.

Information Security Incident Management

34. Kaspersky Lab maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

Vulnerabilities Management

35. Kaspersky Lab's information resources are regularly checked by vulnerability scanners. Kaspersky Lab conducts penetration testing information resources and security audits.

ANNEX 2

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The User, as defined in the Data Processing Agreement (the "data exporter") and
AO Kaspersky Lab, 39A/2 Leningradskoye Shosse, Moscow, 125212 Russian Federation (the "data importer")
each a 'party'; together 'the parties',
HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:
(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
(b) 'the data exporter' means the controller who transfers the personal data;
(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system

ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
(e) that it will ensure compliance with the security measures;
(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
(d) that it will promptly notify the data exporter about:
i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
ii. any accidental or unauthorised access; and
iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
(b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data

importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9
Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses . Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter: The User as defined in the DPA is the data exporter.

Data importer: The data importer is AO Kaspersky Lab, 39A/2 Leningradskoye Shosse, Moscow, 125212 Russian Federation, an international developer of software security solutions and provider of the Kaspersky Endpoint Security Cloud ("Product").

Data subjects: The personal data transferred concern the end users of Software, as defined in the Subsection 1 of Annex 1 in this DPA.

Categories of data: The scope and categories of data are specified in the Subsection 1 of Annex 1 in this DPA.

Special categories of data (if appropriate): The transfer of special categories of data is not anticipated.

Processing operations The personal data transferred will be subject to the processing activities as described in the Agreement and DPA, especially in the Subsection 1 of Annex 1 in this DPA.

Appendix 2 to the Standard Contractual Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. **Technical and Organization Measures**. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect User Data, as defined in the Subsection 2 of the Annex 1 in this DPA, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.

2. **Contacts**. For any questions regarding the processing of User Data, please contact Kaspersky Lab EU representative via e-mail or phone: Kaspersky Labs GmbH, Ingolstadt, Germany, info@kaspersky.de, +49 (0) 841 98 18 90.