STATEMENT ABOUT DATA PROVISION

The Statement about Data Provision (hereinafter "Statement") relates to all Services and Software described below.

This Statement along with the corresponding Terms and Conditions for Service and End User License Agreement for Software described below specifies the conditions, responsibilities, and procedures relating to transmission and processing of the data indicated in this Statement. Carefully read the terms of this Statement, as well as all documents referred to in this Statement, before accepting it.

1. Under this Statement the following definitions are introduced:

Customer – means the organization for which Service and Software are 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.

Data Subject – means a natural person who is a representative of the Customer and/or who uses Service and Software directly or indirectly, including a worker, contractor, employee, or client of the Customer in respect of whom the data is transmitted and processed in the context of the Customer'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 Customer.

2. During use of the functionality related to data processing for Service and Software, the Customer agrees to periodically provide Kaspersky Lab the following information for the following purposes:

- Processing Customer's requests to Kaspersky Threat Intelligence Portal services in accordance with Terms and Conditions described below.
- Investigating issues that arise during processing of user requests to ensure quality of the services provided.

Specific purposes of data processing are described below.

General User Actions

For purposes of investigating issues and verification of compliance with the current license, on any user action during work with Kaspersky Threat Intelligence Portal, the following information are processed:

- Date and time when an action was performed
- IP address (also used for blocking accounts that make frequent attempts to sign in to Kaspersky Threat Intelligence Portal)
- User agent string
- Username (login)

Signing in to Kaspersky Threat Intelligence Portal

For purposes of user authentication and verifying compliance with the current license, on signing in to Kaspersky Threat Intelligence Portal, the following information are processed:

- Certificate
- Password (salt and hash)
- User name (login)
- Session identifier (ID), also stored in the local storage of the user's browser
- API Key (Token)

Digital Footprint Intelligence service

In order to detect immediate threats to the organization and provide the user with information about them, to perform text searches from the user and to filter the results thereof, Kaspersky Threat Intelligence Portal receives the following data when you use the digital footprint intelligence service:

- Information about the organization
- Information about the vulnerabilities found for this organization
- Search queries from the user

APT Intelligence Reporting, Financial Threat Intelligence Reporting and ICS Threat Intelligence Reporting services

For purposes of generating user input hints and searching for requested text (full text search), the requests to the Reporting service are received, stored, and processed.

Kaspersky Threat Lookup Service

For purposes of investigating issues, verifying compliance with the current license, and notifying the user, when the WHOIS hunting functionality is used in the Kaspersky Threat Lookup Service, the following information are processed:

- Requested object
- Username (login)

Accounts management

For the purpose of verifying compliance with the current license, the following information is provided when a new account is created:

- Role (administrator or user)
- Type (type of access to the Kaspersky Threat Intelligence Portal)
- Username (login)

By using Service and Software, the Customer gives its consent to automatically transmit the data specified in this Clause. In case the Customer does not agree to provide this information to Kaspersky Lab, the Customer must not use Service and Software.

3. Kaspersky Lab undertakes the processing of all data received from the Customer in accordance with the instructions of the Customer. This Statement along with corresponding Terms and Conditions for Service and End User License Agreement for Software described below, as well as use of the functionality of Service and Software and its configuration by the Customer are complete instructions issued by the Customer to Kaspersky Lab regarding data

processing unless otherwise specified in a separate written agreement between the Customer and Kaspersky Lab.

4. The Customer is solely responsible for acquainting itself with the user manual for Service and Software, particularly in regards to data processing, with Kaspersky Lab's Privacy Policy, which describes data handling, and independently determining whether they comply with the Customer's requirements.

5. The Customer must comply with laws that apply when Service and Software are used, including laws on confidential information, personal data, data protection.

6. During use of Service and Software the Customer 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.

7. In case that the Customer wants to base the lawfulness of the processing on the consent of its Data Subjects, the Customer 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 Customer prior to using Service and Software. The Customer guarantees that consent of each Data Subject of the Customer was obtained prior to the processing of personal data.

8. It is agreed between Kaspersky Lab and the Customer that, in case of Clause 7 of this Statement, the Customer 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 Customer guarantees that it is able to and will prove the existence of each Data Subject's consent at any time upon request by Kaspersky Lab within 5 business days starting with the request of Kaspersky Lab.

9. Furthermore, in case of Clause 7 of this Statement, the Customer 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 Service and Software. In particular, the Customer is obliged to provide each Data Subject in the European Union, or where applicable law requires, with Kaspersky Lab's Privacy Policy prior to using Service and Software.

10. The Customer shall be fully liable in relation to Kaspersky Lab for any damage resulting from a breach of this Statement, in particular the Customer'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 Statement.

11. The Customer shall indemnify Kaspersky Lab in relation to third parties from the claims arising from the failure of the Customer to fulfill obligations under this Statement which third parties, especially the supervisory data protection authorities, assert against Kaspersky Lab.