

KASPERSKY DIGITAL FOOTPRINT INTELLIGENCE

PRODUCT TERMS AND CONDITIONS

These Product terms and conditions ("Product T&C") set out the special terms and conditions applicable to Kaspersky Digital Footprint Intelligence and is to be read in conjunction with the [Kaspersky Threat Intelligence Agreement](#) ("Agreement"), that apply to these Product T&C.

These Product T&C are legally binding and govern Customer's and Partner's use of Kaspersky Digital Footprint Intelligence ("Product" or "DFI"), accordingly Kaspersky advises to read them carefully.

By purchasing, accessing and/or using the Product, and/or by clicking the appropriate acceptance button if required by Kaspersky (which shall, to the maximum extent permitted by applicable law, constitute conclusive acceptance thereof), Customer or Partner accepts and agrees to be bound by these Product T&C and shall ensure that all individuals or legal bodies involved in purchasing, accepting and using the Product are aware of the terms of these Product T&C and should comply with the same.

By accepting the Product T&C on behalf of Customer or Partner, You represent and warrant that,

- (i) You have full legal authority to bind Customer or Partner to the Product T&C accordingly;
- (ii) You have read and understand these Product T&C;
- (iii) You agree, on behalf of Customer or Partner accordingly, to these Product T&C.

In the event of any conflict between the provisions of these Product T&C and any separate agreement entered into between Kaspersky and the Customer or Partner, the terms of such separate agreement shall prevail to the extent of the conflict.

1. DESCRIPTION

Kaspersky Digital Footprint Intelligence explores the ways to mount an attack against Customer's organization that would be most attractive to cybercriminals, identifying routes and information available to an attacker specifically targeting the Customer, and more. Kaspersky experts piece together a comprehensive picture of the current attack status, identifying weak points ripe for exploitation, and revealing evidence of past, present and planned attacks targeting the Customer.

The Product provides:

► Network Reconnaissance and Vulnerability Analysis

Open-source intelligence (OSINT) semi-passive methods that closely resemble normal internet traffic and behavior, including but not limited to:

- WHOIS;
- Inactive analysis of public Internet sites;
- requests to search engines;
- DNS requests.

Among other techniques, centralized resources are used to detect available network services and their versions, based on port scanning periodically performed by these services (such as Shodan, censys.io, scans.io). Kaspersky experts will also use specialized tools - like Maltego - for massive information gathering, identifying services versions and analyzing potential vulnerabilities based on publicly available information.

The analysis focuses on network inventory, including cloud services specified by the Customer with the following scope:

- Available services
- Service fingerprinting
- Identification of vulnerabilities

- Exploit analysis
- Scoring and risk analysis
- Misconfigured network services
- Defaced or compromised resources

► **Malware and Cyber-Attack Tracking Analysis**

Multiple Kaspersky internal resources are harnessed to monitor and track the actions of different types of malware (including malware used by cybercriminals for sophisticated fraud), together with cybercriminal and cyber-espionage campaigns. Resources used include:

- Kaspersky Security Network (KSN) containing about a petabyte of malicious and potentially malicious samples,
- Passive DNS records,
- Web crawlers,
- C&C sinkholes for specific malware.

Records on IP addresses and the domain names of past, current and potential victims of sophisticated Advanced Persistent Threat (APT) malware will be analyzed separately, to detect any indication that Customer's organization may be being targeted. Using these technologies, it is possible to uncover:

- Phishing attacks
- Targeted attacks
- APT campaigns
- Attacks aimed at Customer's company.

► **Data Leakage and Underground Activities Analysis**

Kaspersky will analyze dumps of compromised accounts as they become publicly available as a result of various breaches, as well as compromised data available on various hacker forums to which Kaspersky has gained covert access. Information on deals taking place on underground forums will be checked for the presence of any indication that Customer's data and resources, or those of Customers' clients or employees, is being traded or discussed. In particular, Kaspersky will uncover:

- Any attempts to hire insiders to attack you from within
- The activities of any malicious insiders trying to sell your access or data
- And discussions about plans to attack you
- Any open bounties offered as reward to those ready and able to help compromise your corporate security.
- Corporate documents being made publicly accessible
- Employee activity on social networks
- E-mail leaks
- Compromised credentials

► **Analysis of identified Threat by Kaspersky Experts**

At this stage, Kaspersky will analyze those threats specific to the Customer fully describing Kaspersky threat intelligence findings and giving recommendations for further remediation.

The Product is conducted with no negative impact on or disruption to the integrity and availability of Customer network resources. The Product is based on non-intrusive network reconnaissance methods, and on the analysis of information available in open sources and resources of limited access.

► **Assets**

In order to continuously monitor and analyze Customer organization's digital footprint, and to identify cybersecurity vulnerabilities and threats, Kaspersky experts work with assets. These Assets are the indicators associated with the Customer organization's infrastructure – and can take a number of forms, including:

- Organization and brand names,
- Domains or subdomain names,
- IP addresses,
- Email addresses,
- The names of employees.

Customer **is NOT ALLOWED** to add assets that are not legally owned (controlled) by Customer, or Customer does not have the related rights to analyze such assets.

MP Partner, being permitted by its End-User(s), **is ALLOWED** to add assets on behalf of such End-user(s) only.

► **Dashboard**

The **Digital Footprint** → **Dashboard** page displays a summary for Digital Footprint Intelligence objects: assets and threat notifications that were found in the organization's infrastructure:

- **Threats** — Summary for threat notifications:
- **Assets** — Summary for assets:

► **Threat notifications**

Threat notifications provide information about detected threats that may reduce the level of protection of the Customer's organization.

For each notification, the following data is displayed:

- **Date**. Date and time when the threat was detected.
- **Risk**. Danger level of the detected threat (Critical, High, Medium, Low, Info).
- **Category**. Category of the threat, for example:
 - APT victim
 - Compromised account
 - Compromised resource
 - Dark web
 - Defacement
 - Employee email address
 - External perimeter
 - Leakage
 - Malware
 - Pastebin entries
 - pDNS record
 - Person
 - Surface web
 - Vulnerability

► **Dark Web search**

Kaspersky TIP allows to run a full-text search against a range of Dark web or other hidden publications and against a number of publications in various social media. (It's not possible, for reasons of victim confidentiality among other legally reasonable things, to provide Kaspersky customers with access to every source of covert intelligence that Kaspersky works with).

Kaspersky TIP searches Forums, Messengers, Ransomware blogs, News, and Pastes categories.

► **Threat Lookup**

Kaspersky Threat Lookup delivers all the knowledge acquired by Kaspersky about cyber-threats and their relationships, brought together into a single, powerful web service. The goal is to provide your security teams with as much data as possible, preventing cyber-attacks before they affect your organization. The platform retrieves the latest detailed threat intelligence about URLs, domains, IP addresses, file hashes, threat names,

statistical/behavior data, WHOIS/DNS data, etc. The result is global visibility of new and emerging threats, helping you secure your organization and boosting your incident response performance.

Product Options

The type and prices of the Product are indicated in the Proposal, and/or in the Kaspersky's price list in effect at the time of Order placement, which Customer or Partner declares to know and accept; and the current price list shall supersede all previous price lists.

License or MP License (as defined below) may be purchased for the different Subscription Periods. In addition Kaspersky provides access to Kaspersky Threat Lookup, limited by fifty (50) searches per day, as a part of the Product.

Digital Footprint Intelligence Analytical Reports (Add-on license)

In addition to notifications, Kaspersky can provide a report containing descriptions of actual noteworthy threats specific to its organization, as well as additional detailed information on the results of Kaspersky technical analyses. Reports are delivered via Kaspersky TIP, and each report may include the following information:

- **Identification of threat vectors.** Identification and status analysis of externally available critical components of Customer's network, including ATMs, video surveillance, and other systems using mobile technologies, as well as employees' social network profiles and personal email accounts, all of which are potential targets for attack.
- **Malware and cyberattack tracking analysis.** Identification, monitoring, and analysis of any active or inactive malware samples targeting Customer's organization, any past or present botnet activity, and any suspicious network-based activity.
- **Third-party attacks.** Evidence of threats and botnet activity specifically targeting Customers' clients, partners, and subscribers, whose infected systems could then be used to attack Customer's organization.
- **Information leakage.** Through discreet monitoring of underground online forums and communities, Kaspersky experts discover whether hackers are discussing attack plans with Customer's organization in mind. Or, for example, if an unscrupulous employee is trading information.
- **Current attack status.** APT attacks can continue undetected for many years. If a current attack affecting Customer's infrastructure is detected, Kaspersky experts provide advice on effective remediation.

Kaspersky Threat Intelligence Bundles

The Product is included into the Theat Intelligence Bundles, available for purchase.

Kaspersky Threat Intelligence Bundles Composition

PRODUCTS AND SCOPE	BASIC	ESSENTIAL	ADVANCED	EXPERT	MAXIMUM
Digital Footprint Intelligence — External perimeter analysis — Dark web monitoring — Discovery of data leaks — Threats detection	-	+	+	+	+
APT Reporting	All reports and Actor profiles available				

— Reports — Actors profiles — IoC and Yara	10 reports to download	15 reports to download	20 reports to download	50 reports to download	Unlimited downloads
Crimeware Reporting — Reports — Actors profiles — IoC and Yara	All reports and Actor profiles available				
	10 reports to download	15 reports to download	20 reports to download	50 reports to download	Unlimited downloads
Threat Infrastructure Tracking	-	-	Country level	Full access	Full access
Kaspersky Threat Lookup — Access to database of threat indicators — Research graph — WHOIS Hinting Rules — 10 saved searches	1 000 requests	2 000 requests	3 000 requests	10 000 requests	50 000 requests
	per 1 year				
Threat Analysis — Cloud Sandbox — Cloud Threat Attribution Engine — Similarity	100 requests	150 requests	200 requests	1 000 requests	3 000 requests
	per 1 year for each technology				

MSSP Bundles Composition

There are different Kaspersky Threat Intelligence Bundles – MSSP, created particularly for MP Partners.

License is available for one (1) year of Subscription Period.

PRODUCTS AND SCOPE	BASIC MSSP	ESSENTIAL MSSP	ADVANCED MSSP	EXPERT MSSP	MAXIMUM MSSP
Digital Footprint Intelligence — External perimeter analysis — Dark web monitoring — Discovery of data leaks — Threats detection	-	5 End-Users	5 End-Users	5 End-Users	5 End-Users
APT Reporting — Reports — Actors profiles — IoC and Yara	All reports and Actor profiles available				
	10 reports to download	15 reports to download	20 reports to download	50 reports to download	Unlimited downloads
Crimeware Reporting — Reports — Actors profiles — IoC and Yara	All reports and Actor profiles available				
	10 reports to download	15 reports to download	20 reports to download	50 reports to download	Unlimited downloads
ICS Reporting	All reports and Actor profiles available				
	-	15 reports to download	20 reports to download	50 reports to download	Unlimited downloads
Kaspersky Threat Lookup — Access to database of threat indicators — Research graph — WHOIS Hinting Rules — 10 saved searches	1 000 requests	2 000 requests	3 000 requests	10 000 requests	50 000 requests
	per 1 year				

Dark Web search — Forums — IT Forums — Messengers — Ransomware blogs — News	-	+	+	+	+
Cloud Sandbox	100 requests	150 requests	200 requests	1 000 requests	3 000 requests
	per 1 year				
Threat Analysis — Cloud Sandbox — Cloud Threat Attribution Engine — Similarity	100 requests	150 requests	200 requests	1000 requests	3000 requests
	per 1 year				
Threat Infrastructure Tracking	-	-	Country level	Full access	Full access

Kaspersky reserves the right at any time to change the composition of the Threat Intelligence Bundles and/or its components in order to improve its value to the Customer or Partner. Actual composition of the bundles is available in the Proposal and/or in the Kaspersky's price list in effect at the time of Order placement, or by request before the Order placement.

Kaspersky provides Product option(s) in accordance with the Order, Certificate and these Product T&C.

2. DELIVERY

2.1. License. Kaspersky grants Customer or Partner a non-exclusive, non-transferable limited license to access to the Kaspersky threat intelligence database and software allowing to see related threats, as well as receive instant notifications about new findings, related to Assets specified by Customer for analysis by Kaspersky solely for Customer's or Partner's internal business purposes, in accordance with the Order, these Product T&C, and the Agreement. The Customer or Partner acknowledges and accepts this License.

2.2. MP License. Kaspersky hereby grants MP Partner a non-exclusive, non-refundable, non-transferable, limited, revocable license during the Period to:

- Where(if) applicable install, integrate, execute, reproduce, display, copy for archival purposes, transmit internally, use the Product and its components on the MP Partner's server/computer system(s) for the purpose of creating, maintaining, providing and supporting MP's products and services;
- provide End-User(s) with access and the right to use the Product solely as part of MP Partner products and services managed by MP Partner in accordance with the Order, conditions of Trial use, and the Product T&C;
- permit End-User(s) to access and use the Product solely as a part of MP products and services subject to the terms of a MP End-User Agreements. MP End-user agreement means an agreement that must be executed between MP Partner and the MP End-User for the provision of MP Partner products and services which is no less restrictive and as protective of Kaspersky's rights, as stated in these Product T&C.

2.3. Trial Use License. Kaspersky grants Customer or Partner a non-exclusive, non-transferable trial license to store, load, install, and use the Product or its components for its internal evaluation business purposes for a period of up to thirty (30) calendar days from the Effective date with no charge. Kaspersky may upon mutual written agreement (including via email), extend the Period of this Trial Use License.

Trial Use License is a time-limited and/or functionality-limited license to use the Product in accordance with these Product T&C. Trial use is available in a full format, with a limited Period, and in format of Demo use, or Pilot project mode. Parameters and limitations, Trial use format is previously agreed by Parties in written (including via email), or stated in the Proposal, or in the Order. Usage of Trial Use License indicates Customer's or Partner's acceptance of any such parameters and limitations.

Kaspersky reserves all rights to provide Pilot projects on a royalty-free and/or commercial basis. All conditions of Trial use, including but not limited to terms of subscription, functionality, scope of the extended support of Kaspersky team, etc. are previously agreed by Parties in written including via email.

Demo use can be limited by functionality, provided at the time of Customer's or Partner's access.

- 2.4.** Access to Product. The Product is provided by means of granting access to Kaspersky TIP. Customer credentials and digital certificate or TOTP code for Kaspersky TIP access are delivered via encrypted email communication to the email address specified by Customer. Customer is not allowed to share credentials and/or digital certificates/TOTP code to anyone. Reports and real-time threat notifications will be delivered to Kaspersky TIP. Customer will be able to obtain information from the Kaspersky TIP itself or using restfulAPI.
- 2.5.** Compensation. The License fee and payment procedure and details shall be stipulated in the Order and/or in the Direct agreement. Obligations of Kaspersky hereunder shall be subject to and conditioned upon the confirmation from Customer or Partner that the payment terms for the Product have been fully accepted and acknowledged by Customer or Partner and Kaspersky received a valid Order in respect of these Product. Customer or Partner hereby agrees to pay License fee in due order. Unless otherwise agreed in writing, all amounts are exclusive of value added tax, sales tax, or other applicable taxes, which shall be payable by Customer or Partner in addition to license fees. In the event of delayed payment beyond ten (10) Business days after the due date, Kaspersky may suspend the provision of Product until full payment is received, without prejudice to any other rights or remedies available. Kaspersky may charge interest on overdue amounts at a rate of fifteen (15) % per annum or the maximum rate permitted by applicable law, calculated from the due date until payment is received.
- 2.6.** Term. The Product T&C shall commence on (i) the Effective Date, (ii) the date of Customer or Partner acceptance of these Product T&C, by clicking the appropriate buttons if required by Kaspersky. The Product T&C becomes not applicable as soon as the Period is expired unless the initial Period is extended or renewed by a new Order, or otherwise agreed by Parties in written, including via email..
- 2.7.** Cooperation. Customer or Partner shall provide the access to its information and property as may be reasonably required in order to permit Kaspersky to perform its obligations hereunder. Kaspersky will not be liable if information or materials provided to Kaspersky by the Customer or Partner are unavailable, inaccurate, and/or inadequate for the Product delivery. Kaspersky will use commercially reasonable efforts to work with the Customer or Partner to correct or clarify any inaccuracies in the Customer's or Partner's information or materials.
- 2.8.** Technical Support. During the term of license purchased Kaspersky provides Customer or Partner with Technical Support, which includes resolution of Customer or Partner problems related to the Product use and being utilized properly according to its intended use and in compliance with the documentation and technical specifications, and these Product T&C.

Kaspersky Technical Support/Customer Service specialists make every commercially reasonable efforts to provide quality support within reasonable time, depending on the nature of the request.

Obligations to respond within a fixed period of time can only be offered as part of [paid services](#).

Customer can ask Kaspersky via [the contact page](#) or use a dedicated "Contact support" button in Kaspersky TIP, if technical support is needed.

2.8.1. Standard Support does not include the following:

- Development of new Product functionality at the request of a User;
- Performance improvement and configuring of User's devices;
- Onsite Support and Remote Support sessions (can be bought as an additional service within Kaspersky Professional Services);
- Assisting a User on the phone or via web chat while collecting data for analysis and/or application of recommendations;
- Consultations regarding third-party applications and/or operating systems;
- Use of third-party patches for operating systems and applications to fix vulnerabilities
- Integration of Kaspersky Software with third-party software (can be bought as an additional service within Kaspersky Professional Services);
- Configuring and checking the Software performance by Technical Support/Customer Service specialists and advice on configuring network security (can be bought as an additional service within Kaspersky Professional Services);
- Software training;
- Demonstration, deployment, and configuration of Software (can be bought as an additional service within Kaspersky Professional Services);
- Analysis and provision of an official opinion on causes of a technical error;
- Analysis and investigation of the causes of incidents resulting from malware infection (can be bought as an additional service within Kaspersky Incident Response).

2.8.2. Kaspersky does not provide Support in the following cases:

- Hardware and/or platform-specific software does not meet the minimum system requirements for the Product;
- Product version is no longer supported (support renewal can be bought upon request).

2.8.3. Kaspersky does not guarantee successful installation, stable Product operation, and resolution of problems in the following cases:

- Installation is performed on an infected device.
- Kaspersky Software is installed in a mixed environment together with other incompatible applications.
- Software interruptions are caused by hardware issues.
- Software interruptions are caused by incompatible versions of platform-specific software.
- The User is unable or refuses to provide Kaspersky Technical Support/Customer Service specialists with the information that is required to reproduce, analyze, and fix the specific problem.
- The problem arose due to incorrect use or disregard of instructions provided by Kaspersky Technical Support/Customer Service specialists or Kaspersky documentation.

2.8.4. Kaspersky provides Support under the following conditions:

- All commercial and trial versions are supported regardless of the license status.
- A valid license is required for support of all commercial versions of Product.

Some services that are not included in Standard Support may be offered as part of [paid services](#).

2.8.5. Kaspersky guarantees the provision of Technical Support/Customer Service for the Product in accordance with these Product T&C.

2.8.6. Kaspersky Technical Support/Customer Service specialists may ask the User to execute additional Kaspersky utilities (software tools) if this is deemed necessary for handling a request.

2.8.7. After processing a request and on a periodic basis, Kaspersky has the right to ask the User for feedback on the quality of service.

2.8.8. When communicating with Technical Support/Customer Service specialists, the User must provide Kaspersky with timely responses, information about the purchased License, and any information reasonably necessary to properly process the request.

3. DATA PROCESSING AND PROTECTION TERMS

3.1. Data processing and protection terms set up in the Threat Intelligence Agreement are relevant to the Product.

3.2. During use of the functionality related to data processing for the Product, Customers or Partners may periodically provide Kaspersky the information, as stated below, for the following purposes:

- ▶ Processing of User's requests to Kaspersky TIP in accordance with these Product T&C;
- ▶ Investigating issues that arise during processing of Users' requests to ensure quality of Kaspersky TIP and the Product.

3.3. Specific goals of the information collection are authentication in Kaspersky TIP, show the recent requests, Input Hint Generation, detection service improvement, history of User's requests, notification about next events in Kaspersky TIP, Products and Services; (i) New / updated Kaspersky Threat Intelligence Reporting; (ii) WHOIS tracking rules; (iii) License expiration.

▶ **Digital Footprint Intelligence**

For purposes of investigating issues and verification of compliance with the current License, on any user's action during the access to the Product the following information is processed:

- ☐ IPs
- ☐ IP Range
- ☐ CIDR
- ☐ e-mail
- ☐ Employee name
- ☐ brand name
- ☐ domains/hosts
- ☐ Free form additional info
- ☐ User Full Name
- ☐ User Name (Login)
- ☐ Organization vulnerabilities

3.4. Kaspersky undertakes the processing of all data received from Customer or Partner in accordance with the Customer or Partner instructions. These Data Provision along with the Product T&C and End User License Agreement for Software (when applicable), as well as use of the functionality of Kaspersky TIP and these Product and its configuration are complete instructions issued by Customer to Kaspersky regarding data processing unless otherwise specified in a separate written agreement.

3.5. Customer or Partner must comply with laws that apply when the Product is used, including laws on confidential information, personal data, and data protection.

3.6. During use of the Product Customer or Partner 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.

3.7. Customer or Partner shall be fully liable in relation to Kaspersky for any damage resulting from a breach of this Data processing and protection terms, in particular the failure to ensure that the processing of personal data is lawful, and/or from any other violation of an obligation under the statements of the clause 3.6 of these Product T&C.

3.8. Customer or Partner shall indemnify Kaspersky in relation to third parties from the claims arising from Customer's or Partner's failure to fulfill obligations under the Product T&C, which third parties, especially the supervisory data protection authorities, assert against Kaspersky.

For any questions or comments regarding the processing of personal data and Kaspersky's privacy practices please contact [Kaspersky data protection officer](#).

3.9. In accordance with all applicable EU Data Protection Laws, BRAZILIAN GENERAL DATA PROTECTION LAW (LGPD) and other applicable laws, by using Kaspersky TIP, Products and Services Customer shall be the data Controller and Kaspersky shall be the data processor, processing data on Customer's behalf.

3.10. Kaspersky is not allowed to sell any Personal Data.

3.11. Kaspersky can use anonymized data to improve the quality of the Product provided.

4. MISCELLANEOUS

4.1. Customers shall guarantee, that they are authorized by their third parties, including but not limited to their partners and/or suppliers, and have all necessary agreements with such third parties in accordance with their local laws, where applicable, to request Kaspersky to provide a security assessment of such third parties based on the Digital Footprint Intelligence scope. This includes the collection, storage, and analysis of data from passive scanning services covering their Internet-facing hosts. Customers shall provide any agreements, powers of attorney, or other documents confirming their rights to request such services upon Kaspersky's request.

4.2. MP Partners shall guarantee, that they are authorized by End-User(s) and have all necessary agreements with its End-User(s) in accordance with its local law, where applicable, and all necessary rights and permissions to use the Product on End-User(s) behalf.

4.3. Kaspersky reserves the right at any time to improve the Product and/or its components (including without limitation content, format, delivery, update details, number of records, sources of intelligence and internal manuals). Content of the Product, its features and/or its format is subject to change and not all their features are available at all times.

4.4. If Customer or Partner violates any of its obligations hereof or License limitations stipulated in these Product T&C or other legally binding document concluded between Kaspersky and Customer or Partner related to the Product, Kaspersky may stop or suspend its delivery. No refund is due in such event.

4.5. Customer may provide Kaspersky with IP addresses, networks, domains, brands or keywords relevant to Customer's organization as a part of the scope of analysis. This information can be provided on the relevant tab of Kaspersky Threat Intelligence Portal. Kaspersky reserves the right to evaluate the provided resources specified by Customer as inappropriate for analysis within the Product.

4.6. Kaspersky does not covenant, guarantee or warrant that Customer will not be attacked during the Product use, as a goal of the Product is to analyze threats specific to the Customer, and notify the Customer about threat intelligence finding and give recommendation for further remediation.

- 4.7.** Customer may not remove or alter any copyright notices or other proprietary notices of the Product, related documentation or materials. All rights not expressly granted herein are reserved by Kaspersky and its licensors.
- 4.8.** Kaspersky reserves the right at any time to modify (by posting on its website or via email to the contact provided by Customer/Partner) these Product T&C and to impose new or additional terms or conditions on the Product use. Such modifications will be effective immediately when incorporated into the Product T&C. Continued use of the Product by Customer or Partner will be deemed acceptance thereof.
- 4.9.** Neither party shall assign or transfer its rights nor delegate its obligations under these Product T&C without the prior written consent of the other party, save that Kaspersky may assign these Product T&C to an affiliate or in the context of a merger or acquisition without restriction.
- 4.10.** Unless otherwise is stated in the Agreement, these Product T&C are governed by the material laws of Germany. Any disputes arising out of or in connection with these Product T&C shall be subject to the exclusive jurisdiction of the courts of country where Kaspersy entity rendering the services is located.
- 4.11.** To the extent Kaspersky processes any personal data on behalf of the Customer/Partner, such processing shall be in accordance with the Data Processing Addendum, available upon request or as set forth in the Agreement.
- 4.12.** Unless otherwise is stated in the Agreement, and to the maximum extent permitted by applicable law, in no event shall Kaspersky, its affiliates, or licensors be liable for any indirect, incidental, special, consequential or punitive damages, or for any loss of profits or revenues, whether incurred directly or indirectly, or any loss of data, use, goodwill, or other intangible losses, resulting from Customer's use of or inability to use the Product, even if Kaspersky has been advised of the possibility of such damages. The aggregate liability of Kaspersky under these Product T&C shall not exceed the fees paid or payable by Customer for the Product in the twelve (12) months preceding the event giving rise to the liability.
- 4.13.** No delay or omission by either party in exercising any right under these Product T&C shall operate as a waiver of that or any other right. A waiver or consent given by a party on any one occasion shall be effective only in that instance and shall not be construed as a bar or waiver of any right on any other occasion. In the event that any provision of the Product T&C shall be invalid, illegal or otherwise unenforceable, the validity, legality and enforceability of the remaining provisions shall in no way be affected or impaired. This Agreement may also be amended or modified by a written instrument executed by both the Customer or Partner and Kaspersky or by Kaspersky only as stipulated in clause 4.9.

THESE PRODUCT T&C SHALL BE BINDING UPON, AND INURE TO THE BENEFIT OF, BOTH PARTIES AND THEIR RESPECTIVE SUCCESSORS AND ASSIGNS