DATA PROTECTION TERMS

The company – partner agreeing to these terms ("Company"), and Avast Software s.r.o., having its registered office at Pikrtova 1737/1a, Prague 4, Nusle, 140 00, Czech Republic, company ID No.: 021 76 475 , registered in the Commercial Register administered by the Municipal court in Prague, Section C, File No. 216540 ("Vendor") and its subsidiaries and/or affiliates (Vendor together with such subsidiaries and affiliates, collectively, "Vendor Affiliates" or individually "Vendor Affiliate") have entered into an agreement under which Vendor has agreed to provide Software or Service (collectively the "Services" or "Solutions") and related technical support to Company as a reseller and supplier of the Services (the "Agreement").

If you are accepting these Data Protection Terms on behalf of Company, you warrant that: (a) you have full legal authority to bind Company to these Data Protection Terms; (b) you have read and understand these Data Protection Terms; and (c) you agree, on behalf of Company, to these Data Protection Terms. If you do not have the legal authority to bind Company, please do not accept these Data Protection Terms.

These Data Protection Terms, including its appendices (the "Terms") will be effective and replace any previously applicable data processing terms as from the Terms Effective Date (as defined below). These Terms supplement the Agreement, while, at the same time, as regards the area of collection, processing and other use of personal data (as this term is defined in Section 2 hereof) within the Services, the provisions of these Terms shall prevail over the provisions of the Agreement or, as the case may be, shall supersede those provisions of the Agreement which concern the processing of personal data. Other provisions of the Agreement shall remain unaffected hereby. No provision hereof may be interpreted as limiting the rights of Vendor under the Agreement in any manner.

1. Introduction

1.1. These Terms govern the processing and security of personal data processed within the Services under the Agreement between Vendor and Company.

1.2. Taking into account the complexity of the relationship between Vendor, Company and End Users (as defined by General Conditions of the Agreement) during the provision of Services the purpose of these Terms is to determine clearly the responsibilities and duties of Vendor and Company and to cover all aspects of personal data processing based on the Agreement.

1.3. To avoid any doubts Company is a controller of Company's End Users' data processed on the basis of Company's relationship with End User, especially regarding the purchase of and payment for the Services, as well as personal data processed for Company's own marketing and other commercial purposes.

2. Definitions

2.1. **Agreement** – means the agreement to provide Services and related technical support to Company as a reseller and supplier of Services including (if not explicitly stated otherwise) under Partner Agreement Special Conditions (the "Special Conditions") and the Partner Agreement General Conditions (the "General Conditions") provided by Vendor to Company or published on the Vendor Portal www.avast.com/partner (as they may be amended from time to time in accordance with their terms);

2.2. **Company** – means a natural or legal person purchasing or distributing Vendor's Services subject to conditions of the Agreement (referred to as Company, Partner, Participant or other as may be in the Agreement, General Conditions or Special Conditions).

2.3. **Company's End Users** – means natural persons who have purchased a Services from the Company;

2.4. **Data subjects** – has the meaning given thereto in the GDPR (as defined below);

2.5. **EEA** – means the European Economic Area.

2.6. **Effective date** – means the date on which the Company agreed to these Terms;

2.7. **End User Personal Data** – means the personal data of Company's End Users or Company's client's End Users, such as name, email address, physical address, phone number, and credit card number, being collected and processed by the Company; this does not include Services Data.

GDPR and other European Data Protection Legislation – means (i) prior to May 25, 2018, the Directive 95/46/EC of the European Parliament and of the Council, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as amended, (ii) on and after May 25, 2018, the Regulation (EU) 2016/679 of the European Parliament and of the Council, the General Data Protection Regulation (the "GDPR"), (iii) Directive 2002/58/EC of the European Parliament and of the Council, concerning the processing of personal data and the protection of privacy in the electronic communications

sector (the ePrivacy Directive), as amended, (iv) all national data protection legislation implementing or supplementing the legal instruments listed under (i) through (iii) above, and (v) any and all legal instruments amending or replacing the legal instruments listed under (i) through (iv) above.

2.8. **Non-European Data Protection Legislation** – means legal regulation governing the area of protection of privacy and/or personal data applicable to the Parties other than the GDPR and other European Data Protection Legislation.

2.9. **Notice** – has the meaning given thereto in the Partner Agreement General Conditions;

2.10. **Parties or, individually, Party** – means parties or party hereto, i.e., Vendor, any Vendor Affiliate and Company;

2.11. **Personal data** – has the meaning given thereto in the GDPR (as defined above).

2.12. **Services Data** – product data such as that connected with the functionality and performance of the Services which cannot be used to identify an individual and device data such as RAM, screen size and resolution, CPU(s), operating system, firewalls, network connection which cannot be used to identify an individual, and collective product and device data that are processed by Vendor in order to provide Services in accordance with the Agreement.

2.13. Capitalized terms not defined by these Terms have the meanings given by the Partner Agreement General Conditions, Special Conditions or the Orders.

3. Scope of European data protection legislation

3.1. The parties acknowledge and agree that the GDPR will apply to the processing of End User Personal Data if, for example:

3.1.1. the processing is carried out in the context of the activities of an establishment of Company or End Users in the territory of the EEA; and/or

3.1.2. the End User Personal Data is personal data relating to data subjects who are in the EEA and the processing relates to the offering to them of goods or services in the EEA or the monitoring of their behavior in the EEA.

3.2. The parties acknowledge and agree that Non-European Data Protection Legislation may also apply to the processing of End User Personal Data.

3.3. Except to the extent these Terms state otherwise, the Terms will apply irrespective of whether the GDPR or Non-European Data Protection Legislation applies to the processing of Personal Data.

4. Scope of processing

4.1. Subject matter, nature and purpose of the processing under these Terms:

- Based on the Orders made by Company, Vendor provides and makes available the Services to the Company pursuant to the Agreement, so that the Company may provide the Services to the End Users. Company will process End User Personal Data to the extent necessary to make available and provide the Services to End Users.

4.2. Categories of data:

- End User Personal Data related to the End Users provided to the Company in connection with the order, purchase and use of the Services by the End Users.
- Services Data

Company processes End Users' Personal Data (e.g. identification, contact, and billing). Vendor processes Services Data.

4.3. Categories of data subjects:

- End Users.

4.4. Vendor will process Services Data as specified by EULA (End User License Agreement) and Company's or Company's End Users' use of Services.

4.5. Vendor is fully responsible for the processing of Services Data and Company is fully responsible for the processing of End User Personal Data.

4.6. If Company acts as a processor of a third-party controller, Company warrants to Vendor that Company's actions with respect to processing personal data, including its appointment of Vendor as provider of the Services, have been authorized by the relevant controller.

4.7. If Non-European Data Protection Legislation applies to either party's processing of personal data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that personal data.

5. Third Party Contractors

5.1. Both Parties mutually authorize each other to engage other third parties to carry out processing operations on their behalf ("Contractors"). Company specifically authorizes Vendor's engagement of Vendor Affiliates as Contractors. Other Vendor's Contractors comprise providers of e-commerce solutions, cloud solutions, technical support, and analytics tools, and other providers of services consisting in processing of data, including, as the case may be, personal data.

5.2. Both Parties will inform each other of any intended changes concerning the addition or replacement of Contractors that may have a substantial impact on the processing of End User Personal Data. Parties are entitled to object to such changes if there are serious and documented doubts about the Contractor's ability to provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

5.3. Contractors are obliged to confidentiality by a contract (NDA) as well as all persons authorized to process the personal data on their behalf.

5.4. Where Vendor or Company engage another contractor for carrying out specific processing activities relating to End User Personal Data on its behalf, the same obligations as set out in these Terms shall be imposed on that other contractor by way of a contract. Vendor or Company remain fully liable for all obligations subcontracted to, and all acts and omissions of, their contractors.

6. Data Subject Rights; Data Export

6.1. Information duty. Company will provide End Users with appropriate information about the processing of personal data collected and processed by Company. Vendor requires Companies to inform End Users about the processing of Services Data (incl. accepting EULA and Privacy Policy).

6.2. Access; Rectification; Restricted Processing; Portability. Company will ensure compliance with the rights to access, rectify, portability, and restrict processing of personal data and to export personal data as regards End User Personal Data collected and processed by Company. During the effectiveness of the Agreement, Vendor will, in a manner consistent with the functionality of the Services, assist Company in ensuring compliance with the rights to access, rectify, portability, and restrict processing of personal data and to export personal data.

6.3. Data Subject Requests. During the effectiveness of the Agreement, if Vendor receives any request from a Company's End User in relation to his/her personal data, Vendor will advise the data subject to submit their request to Company and Company will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

6.4. Vendor Data Subject Request Assistance. Company agrees that Vendor will (taking into account the nature of the processing of End User's personal data) assist Company in fulfilling any obligation to respond to requests by End Users, including if applicable Company's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, especially by providing necessary information and support as regards the functionality of Services.

7. Impact Assessments and Consultations

7.1. Vendor and Company will (taking into account the nature of the processing and the information available to each of them within the scope of the Agreement and these Terms) help and assist each other in ensuring compliance with any obligations in respect of data protection impact assessments and prior consultation pursuant to Articles 35 and 36 of the GDPR, by:

7.1.1. providing the security safeguards (as defined in Appendix 1 of these Terms); and

7.1.2. providing the information and assistance contained in the Agreement and these Terms.

8. Data transfers and location

8.1. Vendor will not transfer any End User Personal Data (if available to Vendor) to any third party but Vendor Affiliates and Contractors as defined in Section 5. This does not affect Vendor's right to process and transfer Services Data – at its own discretion – in compliance with applicable law.

8.2. Vendor may, subject to applicable law and as applicable in accordance with Section 3, store and process the relevant Services Data anywhere Vendor, its Affiliates or its Contractors maintain facilities provided that appropriate safeguards under Articles 45-49 of the GDPR are in place.

8.3. If the storage and/or processing of End User Personal Data involves transfers of End User Personal Data out of the EEA ("Third Countries"), and the European Data Protection Legislation applies to the transfers of such data, Parties will ensure compliance with any obligations in respect of transfers to Third Countries and will provide appropriate safeguards pursuant to Articles 45-49 of the GDPR.

9. Data retention

9.1. Vendor and Company process personal data for the duration of provisioning Services to End Users, and further for the time necessary to comply with contractual and legal obligations or to protect legitimate interests of any of the Parties or the End Users (esp. when personal data is necessary for billing or defense of rights during the statutes of limitation).

9.2. Should these Terms cease to exist for any reason and/or the provision of services relating to processing ends, the Parties undertake to agree on the transition of processing and services related to processing being carried out on the basis of or in connection with these Terms. This does not apply if Vendor and/or Company has legitimate grounds to further process personal data due to contractual obligations, legal obligations or legitimate interests (esp. when personal data is necessary for billing or defense of rights during the statutes of limitation).

10. Security incidents

10.1. Security Incident means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, End User Personal Data on systems managed by or otherwise controlled by Vendor and/or Company. "Security Incidents" will not include unsuccessful attempts or activities that do not compromise the security of personal data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other similar network attacks on firewalls or networked systems which do not compromise the safety and security of personal data.

10.2. Incident Notification. If Vendor and/or Company become aware of a Security Incident, they will: (a) notify the other contracting party of the Security Incident promptly and without undue delay after becoming aware of the Security Incident; and (b) promptly take reasonable steps to minimize harm and secure personal data.

10.3. Details of Data Incident. Notices made pursuant to this section will describe, to the extent possible, details of the Security Incident, including steps taken to mitigate the potential risks and steps Vendor or Company recommend to take to address the Security Incident.

10.4. Delivery of Notices. Notice(s) of any Security Incident(s) will be delivered to infosec@avast.com or, at Vendor and/or Company discretion, by direct communication (for example, by phone call or an in-person meeting). Company is solely responsible for ensuring that the contact details are current and valid.

10.5. Notices of Third Parties. Company is solely responsible for: (a) complying with incident notification laws applicable to Company and fulfilling any third-party notification obligations related to any Security Incident(s); and

(b) notifying each End User affected by a Security Incident without undue delay.

10.6. No Acknowledgement of Fault by Vendor. Vendor notification of or response to a Security Incident under this section will not be construed as an acknowledgement by Vendor of any fault or liability with respect to the Security Incident.

11. Use of Services

11.1. Company is solely responsible for its and End Users' use of the Services, including:

11.1.1. making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of End User Personal Data;

11.1.2. securing the account authentication credentials, systems and devices Company and End Users use to access the Services; and

11.1.3. backing up End User Personal Data.

12. Security of personal data

12.1. Vendor security measures

12.1.1. Vendor will implement and maintain within its Services technical and organizational measures to protect data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 1 (the "Security Measures").

12.2. Company security measures

12.2.1. Company agrees that, without prejudice to Vendor's obligations under Section 12.1 (Vendor security measures) and Section 10 (Security incidents) as between Company and Vendor:

- Vendor has no obligation to protect End User Personal Data that Company, or its End Users elect to store or transfer outside of Vendor's and its Contractors' systems (for example, offline or on-premise storage).

13. Audits and compliance reviews

13.1. Audit Rights.

13.1.1. If the European Data Protection Legislation applies to the processing of End User Personal Data, Parties will ensure ongoing compliance with obligations set by the GDPR, including monitoring, regular reviews and improvements of the security safeguards and documentation.

13.1.2. In order to document their compliance, Parties may conduct internal or third-party audits (including inspections). As regards processing of End User Personal Data subject to the European Data Protection Legislation which requires one of the Parties in particular situations to allow for and contribute to audits, Parties will assist each other and contribute to such audits by providing necessary documentation.

13.1.3. Parties may also conduct an audit to verify compliance with obligations under these Terms by reviewing available security documentation (which may also reflect the outcome of audits conducted by third party auditors).

13.2. Terms for audits and reviews.

13.2.1. In case the European Data Protection Legislation applies to the processing of End User Personal Data and requires one of the Parties in specific situations to allow for and contribute to audits, the Party requesting an audit must send any requests for audits or reviews of documentation in advance to authorized contact email, for Vendor it is: legal@avast.com.

13.2.2. Following the receipt of the request according to section 13.2.1, Parties will discuss and agree in advance on: (i) the reasonable date(s) of and security and confidentiality controls applicable to any review of the safeguards and/or security documentation; and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under this Section.

13.2.3. Party requested to conduct an audit may charge a fee (based on Party's reasonable costs) for any review of the documentation and/or audit under this Section. Parties will provide each other with further details of any applicable fee, and the basis of its calculation, in advance of any such review or audit. Party requesting an audit will be responsible for any fees charged by any auditor appointed by that Party to execute any such audits.

13.2.4. Party requested to conduct an audit may object in writing to an auditor appointed by Party requesting an audit to conduct any audit under this Section if the auditor is, in Party's reasonable opinion, not suitably qualified or independent, a competitor of Party requested to conduct an audit, or otherwise manifestly unsuitable. Any such objection will require the other Party to appoint another auditor or conduct the audit itself.

14. Third Party Beneficiary

14.1. Vendor – Avast Software s.r.o. Notwithstanding anything to the contrary in the Agreement, where Vendor is not a party to the Agreement, Vendor will be a third party beneficiary of relevant rights under these Terms, including without limitation, Section 5.2 (Objection to Contractor Engagement), Section 7 (Impact assessments and Consultations) and Section 13 (Audits and Compliance Reviews).

14.2. Other Third Parties. Except as expressly provided herein and subject to Section 14.1, no one other than a party to the Agreement shall have any right to enforce any of these Terms. For the avoidance of doubt, this includes End Users, who shall not have any right to enforce these Terms.

15. Effect of these Terms

15.1. Notwithstanding anything to the contrary in the Agreement, to the extent of any conflict or inconsistency between these Terms and the remaining terms of the Agreement, these Terms shall prevail.

Appendix 1: Security Measures

As from the Terms Effective Date, Vendor will implement and maintain the Security Measures set out in this Appendix 1. Vendor may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

1. Data Transmission and Threat Management

Data Transmission. Individual Vendor Affiliates are typically connected via high-speed private links to provide secure and fast data transfer between them. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Vendor transfers data via Internet standard protocols.

External Attack Surface. Vendor employs multiple layers of network devices and intrusion detection to protect its external attack surface. Vendor considers potential attack vectors and incorporates appropriate purpose-built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Vendor's intrusion detection involves:

1. tightly controlling the size and make-up of Vendor'sattack surface through preventative measures;
2. employing intelligent detection controls at data entry points; and
3. employing technologies that automatically remedy certain dangerous situations.

Vulnerability management. Vendor conducts regular scanning of entire infrastructure to ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches.

Incident Response. Vendor monitors a variety of communication channels for security incidents, and Vendor's security personnel will react promptly to known incidents.

Encryption Technologies. Vendor uses HTTPS encryption (also referred to as SSL or TLS connection).

2. Site and Access Controls

(a) Site Controls.

On-site Data Center Security Operation. Vendor maintains an on-site security operation responsible for all physical security functions.

Access Procedures for Vendor Premises. Vendor maintains formal access procedures for allowing physical access to its premises. The entrance into the premises requires electronic card key access. All entrants to the premises are required to identify themselves as well as show proof of identity. Only authorized employees, contractors and visitors are allowed entry.

On-site Security. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations is restricted based on the individual's job responsibilities. CCTV cameras are in operation both inside and outside the premises. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the building, and elevator access. On-site personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.

(b) Access Control.

Infrastructure Security Personnel. Vendor has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Vendor's security personnel are responsible for the ongoing monitoring of Vendor's security infrastructure and responding to security incidents.

Access Control and Privilege Management. Company's administrators must authenticate themselves via a central authentication system or via a single sign on system in order to administer the Services.

Internal Data Access Processes and Practices - Vendor's internal data access processes are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Vendor designs its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Vendor employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. Vendor requires the use of strong authentication to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the

authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis.

3. Data Storage, Isolation and Logging

Vendor stores data in a multi-tenant environment on Vendor-owned or Vendor-leased servers. The data and file system architecture are replicated between multiple geographically dispersed data centers. Vendor also logically isolates the Company's data. Company will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Company to determine the product sharing settings applicable to Company End Users for specific purposes. Company may choose to make use of certain logging capability that Vendor may make available via the Services.

4. Personnel Security

Vendor personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.
Personnel are required to execute a confidentiality agreement. Personnel are provided with security and data protection training.

5. Contractor Security

Before onboarding contractors, Vendor conducts an assessment of the security and privacy practices of contractors to ensure contractors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Vendor has assessed the risks presented by the contractor, the contractor is required to enter into appropriate security, confidentiality and privacy contract terms.