Amendment Agreement to the Avanan Terms of Service

Regarding the Processing of Personal Data of EU Customers

(hereinafter referred to as "**Avanan DPA**")
by and between

1. Avanan, Inc., hereinafter referred to as "**Avanan**"

and

2. _____- hereinafter referred to as "**Customer**" -

- **Avanan** and Customer hereinafter referred to as "**Parties**" and each as "**Party**" -

PREAMBLE

Avanan performs malware protection and data security services for Customer ("**Services**") as agreed between the Parties in the Avanan Terms of Service Agreement between Customer and Avanan entered into on _____, _____ ("the **Agreement**"). In the course of providing the Services, Avanan will process personal data for which, pursuant to EU data privacy laws, Customer, Customer's affiliates located in the European Union and/or European Economic Area or Customer's Customers located in the European Union and/or European Economic Area ("**Customer's Customers**") are responsible as provided under Art. 4 no 7 GDPR ("**Customer's personal data**"). Customer's Customers are companies that render services to their end-customers and who engage Avanan as sub-processor.

This Avanan DPA regulates the data protection obligations of the Parties when processing Customer's or Customer's Customers personal data is done under the [Agreement and will reasonably ensure that such processing will only be rendered on behalf of and under the Instructions of Customer or Customer's Customers and in accordance with the EU Standard Contractual Clauses for Processors pursuant to European Commission Decision of 5 February 2010 ("**SCC**") and Art. 28 et seq. of the General Data Protection Regulation ("**GDPR**").

1. DEFINITIONS

– In addition to the definition in Clause 1 SCC, "**Instruction**" means any documented instruction, submitted by Customer to Avanan, directing Avanan to perform a specific action with regard to personal data, including but not limited to the rectification, erasure or restriction of personal data. Instructions shall initially be specified in the **Avanan Cloud Services Agreement** and may, from time to time thereafter, be amended, supplemented or replaced by Customer by separate written or text form Instructions provided that such instructions still fall within the scope of the Services. Instructions issued for the purpose of complying with statutory claims under the GDPR such as rectification, erasure or restriction of personal data fall within the scope of the Services.

– Terms used but not defined in this Section, including but not limited to “personal data”, “personal data breach”, “processing”, “controller”, “processor” and “data subject”, will have the same meaning as set forth in Art. 4 GDPR.

– “**Applicable Law**” means all laws, rules and regulations applicable to either party’s performance under this Data Processing Agreement, including but not limited to those applicable to the processing of personal data. This means in particular the GDPR and all national laws validly amending the applicable rules for the processing of personal data.

2. SUBJECT, DURATION, PURPOSE, AND SPECIFICATION OF PROCESSING

2.1 Avanan will, in the course of providing Services due under the **Avanan Cloud Services Agreement**, process Customer’s personal data which shall be subject to the following provisions contained in this Avanan DPA.

2.2 When performing the Services, Avanan will act either as processor or sub-processor. Avanan’s function as processor or sub-processor will be determined by the function of Avanan’s Customer. If the Customer is the data controller, then Avanan shall be the processor. If the Customer is processor on behalf of its Customer’s Customers, then Avanan shall be the sub-processor and Customer and any of Customer’s Customers shall be entitled to issue Instructions under this Avanan DPA.

2.3 The subject matter, duration, nature and purpose of the processing are described in the **Avanan Cloud Services Agreement**, the appendices of the SCC and Sect. 9 of this Avanan DPA.

2.4 The categories of data and data subjects which may be concerned by the processing are listed in Exhibit, Appendix 1.

2.5 This Avanan DPA amends the **Avanan Cloud Services Agreement** with respect to any processing of personal data provided by Customer and/or its affiliates (each affiliate is hereinafter referred to as: "**EU Customer Affiliate**"), or Customer’s Customers as amended from time to time by written agreement between both Parties.

2.6 Customer enters into this Avanan DPA on its own behalf, on behalf of each of the EU Customer Affiliates and Customer’s Customers and confirms of being authorized to do so. Alternatively, EU Customer Affiliate, or Customer’s Customer can co-sign this Avanan DPA.

2.7 This Avanan DPA is by way of reference an integral part of any agreement entered into between Avanan, Avanan’s EU Customer Affiliate and Avanan’s Customers.

3. STANDARD CONTRACTUAL CLAUSES

Any processing operation as described in Sect. 2 shall also be subject to the SCC as contained in the **Exhibit** which shall prevail over any conflicting clauses in the **Avanan Cloud Services Agreement** or the Avanan DPA. The Parties agree that the SCC shall be directly binding between Avanan as Data Importer (as defined therein), Customer and each EU Customer Affiliate or Customer’s Customers, each acting as

Data Exporter (as defined therein) in relation to the personal data provided by Customer or the respective EU Customer Affiliate or Customer's Customer.

4. AVANAN'S OBLIGATIONS

4.1 In addition to Clause 5 (a) SCC, Avanan shall in the course of providing Services, including with regard to transfers of personal data to a third country, process Customer's personal data only on behalf of and under the documented Instructions of Customer unless required to do so otherwise by the law applicable to Avanan; in such a case, Avanan shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

4.2 Avanan shall take all steps reasonably necessary to ensure that any natural person acting under its authority who has access to personal data does not process such personal data except on Instructions from the Customer, unless Avanan, he or she is otherwise required to do so by applicable law.

4.3 Avanan ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that the obligation will remain after termination of this Avanan DPA.

4.4 Technical and Organizational Data Security Measures

4.4.1 In addition to Clause 5 (c) SCC, the measures specified in Exhibit, Appendix 2 are subject to technical advancements and development.

4.4.2 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Avanan shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as required by Art. 32 GDPR. This includes but is not limited to (as appropriate)

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

4.4.3 When assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

4.4.4 If Avanan significantly modifies measures specified in Exhibit, Appendix 2, such modifications have to meet the obligations pursuant to Sect. 4.4.2 and 4.4.3. Avanan shall make available to Customer a description of such measures which enables Customer to assess compliance with Art. 32 GDPR and allow for and contribute to audits, including

inspections, conducted by the Customer or another auditor mandated by the Customer as permitted by Clause 5 (f) SCC. Avanan and Customer shall agree on such significant modifications by signing the modified Exhibit, Appendix 2 after every amendment. Customer shall not refuse to accept any modification that meets the requirements pursuant to Sect. 4.4.2 and 4.4.3 of this Avanan DPA.

4.4.5 Avanan shall implement a data protection management procedure according to Art. 32 para 1 lit. d) GDPR, for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to appropriately ensure the security of the processing. Avanan will further, by way of regular self-audits, reasonably ensure that the processing of Customer's personal data conforms with the provisions as agreed with Customer or to Customer's Instructions.

4.5 Avanan shall, while taking into account the nature of the processing, assist Customer through appropriate technical and organizational measures, with the fulfilment of Customer's obligations to respond to requests for exercising rights of data subjects in accordance with Applicable Law, in particular Art. 15 through 18 and 21 GDPR.

4.6 Taking into account the nature of the processing and the information available to Avanan, Avanan shall assist Customer with ensuring compliance with the obligations pursuant to Art. 33 through 36 GDPR (Data Security Breach Notification, Data Protection Impact Assessment, Consultation with Data Protection Supervisory Authorities).

4.7 Documentation and Audit Rights

4.7.1 Avanan may, in its discretion provide data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, by a publically certified auditing company or by another customer of Avanan.

4.7.2 If Customer has justifiable reason to believe that Avanan is not complying with the terms and conditions under this agreement, in particular with the obligation to implement and maintain the agreed technical and organizational data security measures, and only once per year, Customer is entitled to audit Avanan. This audit right can be exercised by (i) requesting additional information, (ii) accessing the databases which process Customer's personal data or (iii) by inspecting Avanan's working premises whereby in each case no access to personal data of other customers or Avanan's confidential information will be granted. Alternatively, Customer may also engage third party auditors to perform such tasks on its behalf. The costs associated with such audits and/or for providing additional information shall be borne by Customer unless such audit reveals Avanan's material breach with this Avanan DPA.

4.7.3 Customer may, in its discretion and in exchange for the audit, rely on data protection certifications issued by a commonly accepted certification issuer which has been audited by a data security expert or by a publicly certified auditing company.

4.7.4 If Customer intends to conduct an audit at Avanan's working premises, Customer shall give reasonable notice to Avanan and agree with Avanan on the time and duration of the audit.

In the case of a special legitimate interest, such audit can also be conducted without prior notice. Both Parties shall memorialize the results of the audit in writing.

4.8 Notification Duties

4.8.1 In addition to Clause 5 (d) SCC, Avanan shall inform Customer without undue delay in text form (e.g. letter, fax or e-mail) of the events listed in Clause 5 (d) SCC and the following events:

- Requests from third parties including from a data protection supervisory authority regarding Customer's personal data;
- Threats to Customer's personal data in possession of Avanan by garnishment, confiscation, insolvency and settlement proceedings or other incidents or measures by third parties. In such case, Avanan shall immediately inform the respective responsible person/entity that Customer holds the sovereignty and ownership of the personal data.

4.8.2 For the purpose of complying with Clause 5 (d) SCC and for enabling Customer to comply with its own data breach notification obligations pursuant to Art. 33 para 2 GDPR, Avanan shall notify Customer without undue delay after becoming aware of a personal data breach. Such notice will, at a minimum, include the following information:

- a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- information pursuant to Sect. 4.10;
- description of the likely consequences of the personal data breach; and
- description of the measures taken or proposed to be taken by the Customer to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4.8.3 Avanan shall inform Customer immediately if, from its point of view, an Instruction of Customer may lead to a violation of the GDPR or other Union or Member State data protection provisions. Until the Customer either confirms or alternates the Instruction, Avanan may refuse to comply.

4.9 Rectification, Erasure (Deletion), Restriction

4.9.1 If legally required and Customer is unable to perform the applicable task itself or if provided so in the services description contained in the **Avanan Cloud Services Agreement**, Avanan shall rectify, erase (delete) or restrict (block) Customer's personal data upon Customer's request. Any deletion of Customer's personal data pursuant to this Sect. 4.9 shall be executed in such a manner that restoring or recovering such data is rendered impossible.

4.9.2 At Customer's request, Avanan shall conduct a data protection-compliant destruction of data media and other material if so provided by Customer. Alternatively, at the request of

Customer, Avanan shall provide the data media and other material to Customer or store it on Customer's behalf.

4.9.3 Unless Union or Member State law requires a retention of the personal data, Avanan shall, upon completion of the Services in consultation with Customer, either delete or return all Customer's personal data in its possession to Customer.

4.9.4 If a data subject addresses Avanan with claims for rectification, erasure or restriction, Avanan shall refer the data subject to Customer.

4.10 Avanan will inform Customer of the name and the official contact details of its data protection officer if Avanan is, by Applicable Law, required to appoint a data protection officer. If Avanan is not required to appoint a data protection officer, Avanan shall name a person responsible for dealing with questions relating to applicable data protection law and data security in the context of performing this Avanan DPA.

4.11 In the case claims based on Art. 82 GDPR are raised against Customer, Avanan shall reasonably support Customer with its defense.

4.12 Avanan will make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Avanan DPA and Art. 28 GDPR.

4.13 Avanan will on request make available a record of its processing activities based on Art. 30 GDPR unless the exception of Art. 30 para 5 GDPR applies.

5. CUSTOMER'S OBLIGATIONS

5.1 In addition to Clause 4 (b) SCC, Customer shall provide all Instructions pursuant to this Avanan DPA to Avanan in written or electronic form.

5.2 Customer may issue Instructions at any time as to the type, scope and procedures of the processing to the extent this is so provided in the **Avanan Cloud Services Agreement** or necessary for complying with statutorily granted requests of data subjects. Verbal Instructions shall be confirmed in written form immediately thereafter. Customer shall notify Avanan in writing of the names of the persons who are entitled to issue Instructions to Avanan. Any consequential costs incurred resulting from Customer's failure to comply with the preceding sentence shall be borne by Customer. In any event, the managing directors and personnel/human resource management of Customer are entitled to issue Instructions.

5.3 Customer shall inform Avanan immediately if processing by Avanan might lead to a violation of data protection regulations.

5.4 In the case claims based on Art. 82 GDPR are raised against Avanan, Customer shall reasonably support Avanan with its defense.

5.5 Customer shall name a person responsible for dealing with questions relating to applicable data protection law and data security in the context of performing this Avanan DPA.

6. SUBPROCESSING

6.1 In addition to the provisions contained in Clause 11 SCC, any subprocessor is obliged, before initiating the processing, to commit itself in writing, for the benefit of Customer and Customer's Customers to comply with the same data protection obligations as the ones under this Avanan DPA or legal Act within the meaning of Art. 28 para 3, 4 and 6 GDPR vis-à-vis Customer (the sub-processing agreement must provide at least the same level of data protection as required under this Avanan DPA). Where the subprocessor fails to fulfil its data protection obligations, Avanan shall remain fully liable to the Customer for the performance of the subprocessor's obligations.

6.2 Where a subprocessor refuses to be bound by the same data protection obligations as the ones under this Avanan DPA, Customer may consent thereto whereby such consent shall not be unreasonably withheld.

6.3 Avanan may provide for a website or provide another notice that lists all subprocessors, which have access to personal data of its Customer as well as the limited or ancillary services they provide. At least 14 days before authorizing any new subprocessor gains access to personal data, Avanan will update its website, notify Customer and grant the opportunity to object to such change. Upon Customer's request, Avanan will provide all information necessary to demonstrate that the subprocessor will meet all requirements pursuant to Sect. 6.1 and 6.3. In the case Customer objects to the subprocessing, Avanan can choose to either not engage the subprocessor or to terminate the Avanan DPA with two (2) months prior written notice.

6.4 Subject to Avanan complying with the obligations under Clause 11 SCC and Art. 28 para 2 GDPR, Customer herewith agrees to the following subprocessors:

- Amazon AWS
- _____
- _____
- Any additional subprocessors listed in https://www.avanan.com/gdpr_subprocessors

7. LIABILITY

7.1 Customer and Avanan shall be each liable for damages of concerned data subjects according to Art. 82 GDPR (external liability):

7.1.1 Customer and Avanan shall be liable for all the damage caused by processing which infringes the GDPR.

7.1.2 Avanan's liability under Sect. 7.1.1 shall be limited to the damage caused by processing where it has not complied with obligations of the GDPR specifically directed to Avanan or where it has acted outside or contrary to lawful Instructions of the Customer.

7.1.3 Customer and Avanan shall be exempt from liability under Sect. 7.1.1 and 7.1.2 if they prove to not be in any way responsible for the event giving rise to the damage.

7.1.4 Where more than one Customer and Avanan, or both, the Customer and Avanan, are involved in the same processing and under Sect. 7.1.1 and 7.1.2 are responsible for any damage caused by processing, each Customer or Avanan shall be held liable for the entire damage.

7.1.5 Sect. 7.1.1, 7.1.2, 7.1.3 and 7.1.4 shall apply only, where more beneficial for data subjects as compared to Clause 3 and 6 SCC. In any other case, Clauses 3 and 6 SCC shall prevail.

7.1.6 Customer and Avanan shall be entitled to claim back from the other, Avanan or Customer, that part of the compensation corresponding to their part of responsibility for the damage.

7.2 As regards the internal liability and without any effect as regards the external liability towards data subjects, the Parties agree that notwithstanding anything contained hereunder, when providing the Services, Avanan's liability for breach of any terms and conditions under this Avanan DPA shall be subject to the liability limitations agreed in the **Avanan Cloud Services Agreement**. Further, no EU Customer Affiliate shall become beneficiary of the Avanan DPA without being bound by this Avanan DPA and without accepting this liability limitation. Customer will indemnify Avanan from any exceeding claims of its EU Customer Affiliates or data subjects who claim rights based on alleged violation of this Avanan DPA including the SCC.

8. COSTS FOR ADDITIONAL SERVICES

If Customer's Instructions lead to a change from or increase of the agreed Services or in the case of Avanan's compliance with its obligations pursuant to Sects. 4.6, 4.9 or 4.11 to assist Customer with Customer's own statutory obligations, Avanan is entitled to charge reasonable fees for such tasks which are based on the prices agreed for rendering the Services and/or notified to Customer in advance.

9. CONTRACT PERIOD

The rights, benefits and obligations of this Avanan DPA shall commence with the initiation of the Services and shall terminate with termination of the agreed Services under the **Avanan Cloud Services Agreement**.

10. MODIFICATIONS

Avanan may modify or supplement this Avanan DPA, with notice to Customer, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with Applicable Law, (iii) to implement standard contractual clauses laid down by the European Commission or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 of the GDPR.

11. WRITTEN FORM

Any side agreements to this Avanan DPA as well as changes and amendments of this Avanan DPA, including this Sect. 11, shall be in writing (textform being sufficient).

12. CHOICE OF LAW

This Avanan DPA is governed by, and shall be interpreted in accordance with, the law of the EU Member State in which the Customer or, if the Customer is not controller, the Customer's Customer resides, excluding its conflict of law provisions, to the extent not otherwise provided by Clause 7 SCC.

13. MISCELLANEOUS

13.1 For the determination of the data protection obligations, entitlement to provide orders and control, responsibilities, liabilities and consequences of objectives, the Avanan DPA shall prevail over all other agreements between the Parties.

13.2 This Avanan DPA may only be amended, supplemented or changed upon the written agreement of the Parties.

13.3 In the event a clause under the **Avanan Cloud Services Agreement** has been found to violate the GDPR including all other Applicable Laws, the Parties will mutually agree on modifications to the **Avanan Cloud Services Agreement** to the extent necessary to ensure data privacy-law compliant processing.

Signatures:

_____	_____
Customer	Avanan
_____	_____
Name, Title	Name, Title
_____	_____
Date	Date

Exhibit– Standard Contractual Clauses for Processors

Standard Contractual Clauses for 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.

Customer and each of the EU Customer Affiliates and Customer's Customer are hereinafter referred to as the "**Data Exporter**" with respect to the personal data provided by that Data Exporter.

Avanan as defined in the Avanan DPA is hereinafter referred to as the "**Data Importer**".

The Data Exporter(s) and the Data Importer, each a "party" and collectively "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 subprocessor'* means any processor engaged by the Data Importer or by any other subprocessor of the Data Importer who agrees to receive from the Data Importer or from any other subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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 subprocessing, 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 subprocessing, it has previously informed the Data Exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor 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 subprocessor, 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor 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 subprocessor, 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 subprocessor preventing the conduct of an audit of the Data Importer, or any subprocessor, 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

Subprocessing

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 subprocessor which imposes the same obligations on the

subprocessor as are imposed on the Data Importer under the Clauses (This requirement may be satisfied by the subprocessor co-signing the contract entered into between the Data Exporter and the Data Importer which is based on the terms and conditions of this Agreement.). Where the subprocessor 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 subprocessor's obligations under such agreement.

2. The prior written contract between the Data Importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing 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 subprocessing 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 subprocessor 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 subprocessor 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.

On behalf of the Data Exporter(s):		**On behalf of the Data Importer:**	
		AVANAN	
Signature:		Signature:	
Print Name:		Print Name:	
Print Title:		Print Title:	
Date:		Date:	

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
Customer

Data Importer
AVANAN is engaged in providing cloud security services.

Data subjects
The Data subjects will depend upon how the Customer has configured the Avanan Service and the type of data the Service has visibility into. The Service may process data potentially coming from Customer employees, vendors, or downstream customers, depending upon the types and source of data that the Service inspects and the content the Customer submits to the Service for analysis.

Categories of data
The personal data transferred concern the can include the following categories of data:
- *Unencrypted files being uploaded, downloaded or stored in the cloud,*
- *Names, usernames and IP Addresses of Customer employees using the cloud service,*
- *Email Sender, Recipient and body of Email if so configured and any attachments or URLs in the body of an Email the system inspects.*

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:
Not to be expected but cannot be excluded.

Processing operations
The personal data transferred will be subject to the following basic processing activities:
Depending upon the configuration of the system, Service will monitor and scan
- *Plain text files and unencrypted documents present within the Customer cloud accounts*
- *All email messages and attached files*

This monitoring is done for the purpose of identifying potentially malicious content such as phishing, ransomware, Trojans, botnets, or other malicious content. No orginal data is stored after the scan. The Bundled Product will store meta-data about the malicious content and make such information about malicious content available to the Customer to defend from threats without revealing the original source(s) of the data or the original data itself.
Authorized employees within the organization will have availability to original malicious content and metadata based upon permissions granted within the system.

Retention

At all times during the term of Avanan subscription, Avanan will have the ability to access and extract Customer's Personal Data stored by the Service. The Service will retain Customers' Personal Data stored in a limited function account for 90 days after expiration or termination of the Customer's subscription so that the Customer may extract the data. After the 14-day retention period ends, Avanan will disable the Customer's account and delete the Customer's Personal Data.
The Services may not support retention or extraction of software provided by Avanan. Avanan has no liability for the deletion of personal data as described in this section.

On behalf of the Data Exporter(s):		**On behalf of the Data Importer:**	
[_____]		**AVANAN**	
Signature:	_____	Signature:	_____
Print Name:	_____	Print Name:	_____
Print Title:	_____	Print Title:	_____
Date:	_____	Date:	_____

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

Description of the technical and organizational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Sub-Processors will be bound to adhere to similar but not identical organizational security measures which shall not fall below the level of data security as agreed herein. Any organizational security measures are subject to change as technical standards evolve and such changes can be implemented by Data Importer. If so requested, data importer will provide data exporter with a description of the then current measures.

1. Separation Control:

The customer information within the Avanan environment consists of a.) the meta-data database about every malware event and b.) the files and emails that are currenly being scanned for malware.

a.) Each customer meta-data database is maintained within a separate database instance which is independently accessible with a per-customer credentials. The database itself is stored on encrypted storage infrastructure that is inaccessbile except witin the context of the customer database. All data classified as confidential or higher stored in a database that is encrypted by the application performing the storage operation and not by the database itself or by the file system.

b.) The files and emails that are currently being scanned are temporarily held in a context-independent environment and sent to the malware scanners within that context. The filesystem on which the file is temporarily stored is encrypted. The result of the scan is returned within the same customer context and added to the database. Once scanned, the file or email is permanently and irretrievably deleted. All data classified as confidential or higher stored on file systems that are encrypted by the application performing the storage operation and located in an encrypted file system.

Temporary storage of unencrypted files for necessary for processing is allowable, provided that:

- The file system is encrypted
- A background process regularly deletes unprocessed files
- Foreground processes delete temporary files after processing

2. Pseudonymization

The meta-data databases are inaccessible outside the customer-specific context and completely innaccessible to the outside world so there is no pseudonymization of the meta-data.

3. Encryption

All data considered confidential or higher is stored on Avanan systems in encrypted form. Encryption shall be performed as follows:

- All data classified as confidential or higher are encrypted using a strong algorithm.
- All data classified as confidential or higher are encrypted using a strong key that is customer specific.
- All data classified as confidential or higher are kept in encrypted form unless decryption is absolutely required.
- In no case is data classified as confidential or higher be transferred in unencrypted state.
- In no case is data classified as confidential or higher be stored permanently in unencrypted state.

All databases and temporary file storage are maintained within encrypted file systems accessible only within the context of the customer environment.

4 Measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

Avanan's Information Security Practice, in part, is based off of the principles in ISO27002/27001. Avanan leadership has established controls that uphold these principles. Controls help identify and prevent the compromise of information security and the misuse of company data, applications, networks and computer systems by which all employees must adhere when handling information.

- The network and servers are all located in the Amazon Web Services (AWS) environment, which is, built on a highly redundant environment. In case of a failure, restoration of the entire system can be resumed within 4 hours.
- Each server configuration and software packages are stored on Assembla and can be redeployed in the event of a failure. The network layer redundancy is covered by AWS infrastructure. Utilizing he AWS environment allows high redundancy and availability for the entire system. Additional backups of installation software and scripts are resident on the developer's laptops and desktops.
- All customer data is backed up on within one or more EU-based Amazon AWS data centers.
- All customer data is backed up once a day. Backups are rotated based on a first in first out schedule and limiting the data kept up to 14 days. All backups are encrypted.
- In case of failure of the platform, Avanan has the capability to recover quickly through running installation scripts and to rebuild the systems and repopulate the systems with the client data.

Only the meta-data databases are maintained over time. Customer files and emails are deleted as soon as they are scanned and are not backed up or stored for any reason. All backups and redundant systems are separated using the same customer-specific context of the live system.

5. Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The Avanan infrastructure and protocols have been audited for security and integrity by. Ongoing testing, assessing and evaluation is performed on a regular schedule and with each software version that affects the processing infrastructure or security architecture.

On behalf of the Data Exporter(s):		**On behalf of the Data Importer:**	
[_____]		**Avanan**	
Signature:	_____	Signature:	_____
Print Name:	_____	Print Name:	_____
Print Title:	_____	Print Title:	_____
Date:	_____	Date:	_____

[Remainder of Page Intentionally Left Blank]