EU GDPR
DATA PROCESSING ADDENDUM (DPA)
DATA PROCESSING STATEMENT FOR BITNINJA
CUSTOMERS

WHO SHALL EXECUTE THIS DPA:

If it has been determined that you qualify as a data controller under the GDPR and need a data processing statement in place with companies that process personal data on your behalf. This Data Processing Addendum is used to make enforcing your rights easy.

This GDPR compliant Data Processing Addendum is attached in a form to sign it, when accepted, in accordance with the instructions below.

HOW TO EXECUTE THIS DPA:

1   This DPA consists of two parts: the DPA main body and Annexes 1, 2 and 3 (including Appendices 1 to 2).

2   This DPA has been pre-signed on behalf of BitNinja. The Standard Contractual Clauses in Annex 2 (including Appendix 1 thereto) and the Security Measures in Annex 3 have been pre-signed by BitNinja as the data importer.

3   To execute this DPA, Customer must complete the information in the appropriate spaces and sign on Pages 6, 13, 15 and 19.

4   Send the completed and signed Data Processing Statement to BitNinja by email, indicating the Customer's Legal Name (as set out on the applicable BitNinja Order Form or invoice, if applicable), to info@bitninja.io.

Upon receipt of the validly completed Data Processing Statement by BitNinja at this email address, the terms and conditions therein will become legally binding to the parties on the strength of the law.

EU GDPR

DATA PROCESSING ADDENDUM

This Data Processing Addendum("**DPA**"), forms part of the Agreement, BitNinja General Contract Terms And Conditions (available at https://bitninja.io/terms-and-services or any other written or electronic agreement, by and between BitNinja Kft.("**BitNinja**") and the undersigned customer of BitNinja ("**Customer**") for certain security, and/or other website services (collectively, the "**Service**") provided by BitNinja (the "**Main Agreement**"). All Terms not defined herein shall have the meanings set forth in the Main Agreement. Hereinafter each of Customer and BitNinja may be referred to as a "**party**" and together as the "**parties**."

In connection with the Service, the parties anticipate that BitNinja may process in accordance with EU regulations related to data protection, in respect of which the Customer or any member of the Customer Group may be a data controller or data processor, as applicable, under applicable EU legislation.

The parties have agreed to enter into this DPA in order to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data as required by EU regulations.

HOW SHALL THIS DPA APPLY

This DPA is an addendum to and forms part of the Main Agreement. The Customer/entity signing this DPA must be the same as the Customer/entity party to the Main Agreement.

If the Customer/entity signing this DPA does not comply with the Main Agreement and is not directly related to BitNinja, but is instead indirectly related to BitNinja Service Provider, the content of this DPA will not valid and legally binding between them. Such entity should notify the competent party by itself whether any amendment to its agreement between them may be required.

DATA PROCESSING TERMS

In the course of providing the Service to Customer pursuant to the Main Agreement, BitNinja may Process such Personal Data on behalf of Customer. BitNinja agrees to comply with the following provisions with respect to any Personal Data submitted by or for Customer to BitNinja or collected and processed by or for Customer using BitNinja's services.

1. Definitions

1.1   The following definitions are used in this DPA:

   a)   "**Adequate Country**" means a country or territory that provides adequate protection for Personal Data under EU Data Protection Regulations;

   b)   "**BitNinja Group**" means BitNinja and any of its Affiliates;

   c)   "**Customer Group**" means Customer and any of its Affiliates doing business in the EEA or the European Union;

   d)   "**EU Legal Provisions**" mean all laws and regulations of the European Union and the European Economic Area, their member states, applicable to the processing of Personal Data under the Main Agreement, including (where applicable) the GDPR;

   e)   "**GDPR**" means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data);

   f)   "**Personal Data**" means all data which is defined as '*personal data*' under EU Legal Provisions and to which EU Legal Provisions apply and which is provided by the Customer to BitNinja, and accessed, stored or otherwise processed by BitNinja as a data processor as part of its provision of the Service to Customer; and

   g)   "**processing**", "**data controller**", "**data subject**", "**supervisory authority**" and "**data processor**" shall have the meanings ascribed to them in EU Data Protection Regulations.

1.2   An entity "**Controls**" another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract; and two entities are treated as being in "**Common Control**" if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

2. Status of the parties

2.1   The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, shall be recognised as described in Annex 1.

2.2   In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby acknowledge and agree that the Customer is the data controller or processor, and BitNinja is the data processor or sub-processor, as applicable, and accordingly BitNinja agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA.

2.3   Each party warrants in relation to Personal Data that it will comply (and will procure that any of its personnel comply and use commercially reasonable efforts to procure that its sub-processors comply), with EU Data Protection Regulations. As between the parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data.

2.4   If Customer is a data processor, Customer warrants to BitNinja that Customer's instructions and actions with respect to the Personal Data, including its appointment of BitNinja as another processor and concluding the standard contractual clauses (Annex 2), have been authorised by the relevant controller.

2.5   Where and to the extent that BitNinja processes data which is defined as '*personal data*' under the applicable EU legal provisions, as a data controller, as set out in BitNinja Privacy Policy (available at https://bitninja.io/privacy-policy, BitNinja will comply with the provisions of the applicable EU Regulation in respect of that processing.

2.6   Each party shall appoint an individual within its organization authorized to respond from time to time to enquiries regarding the Personal Data and each party shall deal with such enquiries promptly.

2.7   Upon Customer's request the data controller shall - without undue delay - rectify the incorrect personal data with respect to the requestor.

Data processor admits and states that in case of any incident relating to Personal Data it shall promptly meet its obligations to Hungarian National Authority for Data Protection and Freedom of Information within 72 hours.

3.   BitNinja obligations

3.1   With respect to all Personal Data, BitNinja warrants that it shall:

(a)   only process Personal Data in order to provide the Service, and shall act only in accordance with: (i) this DPA, (ii) the Customer's written instructions as represented by the Main Agreement and this DPA, and (iii) as required by applicable laws;

(b)   upon becoming aware, inform the Customer if, in BitNinja's opinion, any instructions provided by the Customer under clause 3.1(a) infringe the GDPR;

(c)   implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. Such measures shall include, without limitation, the security measures set out in Annex 3;

(d)   take reasonable steps to ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under obligations of confidentiality;

(e)   without undue delay after becoming aware, notify the Customer of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by BitNinja, its sub- processors, or any other identified or unidentified third party (a "**Security Breach**");

(f)   promptly provide the Customer with reasonable cooperation and assistance in respect of a Security Breach and all reasonable information in BitNinja's possession concerning such Security Breach insofar as it affects the Customer, including the following to the extent then known:

(i)   the possible cause and consequences for the Data Subjects of the Security Breach;

(ii)   the categories of Personal Data involved;

(iii)   a summary of the possible consequences for the relevant data subjects;

(iv)   a summary of the unauthorised recipients of the Personal Data; and

(v)   the measures taken by BitNinja to mitigate any damage;

(g)   not make any public announcement about a Security Breach (a "**Breach Notice**") without the prior written consent of the Customer, unless required by applicable law;

(h)   promptly notify the Customer if it receives a request from a data subject to access, rectify or erase that individual's Personal Data, or if a data subject objects to the processing of, or makes a data portability request in respect of, such Personal Data (each a "**Data Subject Request**"). BitNinja shall not respond to such request without the Customer's prior written consent except to confirm that such request relates to the Customer, to which the Customer hereby agrees. To the extent that the Customer does not have the ability to address a Data Subject Request, then upon Customer's request BitNinja shall provide reasonable assistance to the Customer to facilitate such Data Subject Request to the extent able and in line with applicable law. Customer shall cover all costs incurred by BitNinja in connection with its provision of such assistance;

(i) other than to the extent required to comply with applicable law, following termination or expiry of the Main Agreement or completion of the Service, BitNinja will delete all Personal Data (including copies thereof) processed pursuant to this DPA;

(j) taking into account the nature of processing and the information available to BitNinja, provide such assistance to the Customer as the Customer reasonably requests in relation to BitNinja's obligations under EU Data Protection Regulations with respect to:

(i) data protection impact assessments (as such term is defined in the GDPR);

(ii) notifications to the supervisory authority under EU Data Protection Regulations and/or communications to data subjects by the Customer in response to any Security Breach; and

(iii) the Customer's compliance with its obligations under the GDPR with respect to the security of processing;

provided that the Customer shall cover all costs incurred by BitNinja in connection with its provision of such assistance.

4. Sub-processing

4.1 The Customer grants a general authorization: (a) to BitNinja to appoint other members of the BitNinja Group as sub-processors, and (b) to BitNinja and other members of the BitNinja Group to appoint third party data centre operators, and outsourced marketing, business, engineering and customer support providers as sub-processors to support the performance of the Service.

4.2 BitNinja will maintain a list of sub-processors on the www.bitninja.io website and will add the names of new and replacement sub-processors to the list prior to them starting sub-processing of Personal Data. If the Customer has a reasonable objection to any new or replacement sub-processor, it shall notify BitNinja of such objections in writing within ten (10) days of the notification and the parties will seek to resolve the matter in good faith. If BitNinja is reasonably able to provide the Service to the Customer in accordance with the Main Agreement without using the sub-processor and decides in its discretion to do so, then the Customer will have no further rights under this clause 4.2 in respect of the proposed use of the sub-processor. If BitNinja requires use of the sub-processor in its discretion and is unable to satisfy the Customer as to the suitability of the sub-processor or the documentation and protections in place between BitNinja and the sub-processor within ninety (90) days from the Customer's notification of objections, the Customer may within thirty (30) days following the end of the ninety (90) day period referred to above, terminate the applicable Order Form and/or Insertion Orders with at least thirty (30) days written notice, solely with respect to the service(s) to which the proposed new sub-processor's processing of Personal Data relates. If the Customer does not provide a timely objection to any new or replacement sub-processor in accordance with this clause 4.2, the Customer will be deemed to have consented to the sub-processor and waived its right to object. BitNinja may use a new or replacement sub-processor whilst the objection procedure in this clause 4.2 is in process.

4.3 BitNinja will ensure that any sub-processor it engages to provide an aspect of the Service on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Personal Data than those imposed on BitNinja in this DPA (the "**Relevant Terms**"). BitNinja shall procure the performance by such sub-processor of the Terms set out in this document and shall be liable to the Customer for any breach by such person of any of the Terms.

5. Audit and records

5.1 BitNinja shall, in accordance with EU Data Protection Regulations, make available to the Customer such information in BitNinja's possession or control as the Customer may reasonably request with a view to demonstrating BitNinja's compliance with the obligations of data processors under EU Data Protection Regulations in relation to its processing of Personal Data.

5.2   Customer may exercise its right of access under EU Data Protection Regulations in relation to Personal Data, as follows:

      (a) an audit report not older than eighteen (18) months, prepared by an independent external auditor (inspector) demonstrating that BitNinja's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard; and

      (b) additional information in BitNinja's possession or control to an EU supervisory authority when it requests or requires additional information in relation to the processing of Personal Data carried out by BitNinja under this DPA.

      (c) it may request and control Personal Data that BitNinja stores and information relating to their processor at any time. In case of a typical data request, Controller is not allowed to add any extra charge for the information.

6.   Data transfers

6.1   To the extent any processing of Personal Data by BitNinja takes place in any country outside the EEA (except if in an Adequate Country), the parties agree that the standard contractual clauses approved by the EU authorities under EU Data Protection Regulations and set out in Annex 2 will apply in respect of that processing, and BitNinja will comply with the obligations of the 'data importer' in the standard contractual clauses and the Customer will comply with the obligations of the 'data exporter'.

6.2   The Customer acknowledges and accepts that the provision of the Service under the Main Agreement may require the processing of Personal Data by sub-processors in countries outside the EEA.

6.3   If, in the performance of this DPA, BitNinja transfers any Personal Data to a sub-processor located outside of the EEA (without prejudice to clause 4), BitNinja shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place, such as:

      (a)   the requirement for BitNinja to procure that the sub-processor execute to the benefit of the Customer standard contractual clauses approved by the EU authorities under EU Legal Provisions and set out in Annex 2;

      (b)   the requirement for the sub-processor to be certified under the EU-U.S. Privacy Shield Framework; or

      (c)   the existence of any other specifically approved safeguard for data transfers (as recognised under EU Data Protection regulations) and/or a European Commission finding of adequacy.

6.4   The following terms shall apply to the standard contractual clauses set out in Annex 2:

      (a)   The Customer may exercise its right of audit under clause 5.1(f) of the standard contractual clauses as set out in, and subject to the requirements of, clause 5.2 of this DPA; and

      (b)   BitNinja may appoint sub-processors as set out, and subject to the requirements of, clauses 4 and 6.3 of this DPA.

7.   General

7.1   This DPA is without prejudice to the rights and obligations of the parties under the Main Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

7.2   BitNinja's liability under or in connection with this DPA (including under the standard contractual clauses set out in Annex 3) is subject to the limitations on liability contained in the Main Agreement.

7.3   This DPA does not confer any third-party beneficiary rights. It is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

7.4   This DPA and any action related thereto shall be governed by and construed in accordance with the laws of the State of California, without giving effect to any conflicts of laws principles. The parties consent to the personal jurisdiction of the court of registered office of BitNinja Kft.

7.5   This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA. No modification of, amendment to, or waiver of any rights under the DPA will be effective unless in writing and signed by an authorized signatory of each party. This DPA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. Each person signing below represents and warrants that he or she is duly authorized and has legal capacity to execute and deliver this DPA. Each party represents and warrants to the other that the execution and delivery of this DPA, and the performance of such party's obligations hereunder, have been duly authorized and that this DPA is a valid and legally binding agreement on each such party, enforceable in accordance with its terms.

(*Signature page follows*)

IN WITNESS WHEREOF, the parties have each caused this DPA to be signed and delivered by its duly authorized representative.

CUSTOMER:		BITNINJA KFT.:	
BY		BY	
NAME		NAME	
TITLE		TITLE	
ADDRESS		ADDRESS	
DATE		DATE	

<u>**Annex 1**</u>

Details of the Personal Data and processing activities

(a) The personal data comprises: in relation to visitors of the Customer's online properties identification data, professional life data, personal life data, connection data, or localization data (including IP addresses). Customer, its online visitors and/or other partners may also upload content to Customer's online properties which may include personal data and special categories of data, the extent of which is determined and controlled by the Customer in its sole discretion. Such special categories of data include, but may not be limited to, information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sex life.

(b) The duration of the processing will be: until the earliest of (i) expiry/termination of the Main Agreement, or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Main Agreement (to the extent applicable);

(c) The processing will comprise: Processing necessary to provide the Service to Customer, pursuant to the Main Agreement;

(d) The purpose(s) of the processing is/ are: necessary for the provision of the Service;

(e) Personal data may concern the following data subjects:

- Prospective customers, customers, resellers, referrers, business partners, and vendors of the Customer (who are natural persons);

- Employees or contact persons of the Customer's prospective customers, customers, resellers, referrers, sub-processors, business partners, and vendors (who are natural persons);

- Employees, agents, advisors and freelancers of the Customer (who are natural persons); and/or

- Natural persons authorized by the Customer to use the Service.

2010 EU Model clauses extracted from 2010/87/EU Annex EU Standard Contractual Clauses for the transfer of personal data to data processors established in third countries which do not ensure an adequate level of data protection

INTRODUCTION

Both 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.

AGREED TERMS

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 EU Data Protection Laws 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 entity 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 EU Data Protection Laws 95/46/EC;

d)   the "**sub-processor**" means any processor engaged by the data importer or by any other sub- processor of the data importer who agrees to receive from the data importer or from any other sub- processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

e)   the "**applicable data protection law**" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established; and

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.

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.

3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this Clause, Clause 4.1(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.

3.2 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.

3.3 The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub- processor shall be limited to its own processing operations under the Clauses.

3.4 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.

4. Obligations of the data exporter

4.1 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;

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 EU legal provisions 95/46/EC;

g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

j) that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer

5.1 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 implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

c) 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;

d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6.   Liability

6.1   The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2   If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 3, 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 or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3   If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7.   Mediation and jurisdiction

7.1   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.

7.2   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.

8.   Co-operation with supervisory authorities

8.1   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.

8.2   The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3   The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9.   Governing law

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

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.

11.   Sub-processing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third- party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5.1(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

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

12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

This agreement has been entered into on the date shown at the beginning of the first page of this agreement.

CUSTOMER (DATA EXPORTER):		BITNINJA KFT. (DATA IMPORTER):	
BY		**BY**	
NAME		**NAME**	
TITLE		**TITLE**	
ADDRESS		**ADDRESS**	
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
The data exporter is (please specify briefly your activities relevant to the transfer):
The (i) legal entity that has created an account with BitNinja Kft. ("**BitNinja**") for provision of the Service and executed the Clauses as a data exporter.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
BitNinja , which processes Personal Data upon the instruction of the data exporter in accordance with the terms of the agreement between the data exporter and BitNinja.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
The data exporter may submit Personal Data to BitNinja and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospective customers, customers, resellers, referrers, business partners, and vendors of the data exporter (who are natural persons);

- Employees or contact persons of the data exporter's prospective customers, customers, resellers, referrers, subcontractors, business partners, and vendors (who are natural persons);

- Employees, agents and advisors of the data exporter; and/or

- Natural persons authorized by the data exporter to use the services provided by BitNinja Kft. to the data exporter.

Categories of data
The personal data transferred concern the following categories of data (please specify):
The data exporter may submit Personal Data to BitNinja, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:

- Names, titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, professional life data, personal life data, connection data, or localization data (including IP addresses).

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

The data exporter may submit special categories of data to BitNinja and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion. Such special categories of data include, but may not be limited to, Personal Data with information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sex life.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):
The objective of the processing of Personal Data by BitNinja is to provide the Service, pursuant to the Main Agreement.

CUSTOMER (DATA EXPORTER):		BITNINJA KFT. (DATA IMPORTER):	
BY		**BY**	
NAME		**NAME**	
TITLE		**TITLE**	
ADDRESS		**ADDRESS**	
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 organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

See Annex 3 to the DPA.

<u>**Annex 3**</u>

Safety measures

A. Data importer/sub-processor has implemented and shall maintain a security program in accordance with industry standards, laws and the GDPR.

B. More specifically, data importer/sub-processor's security program shall include:

Access Control of Processing Areas

Data importer/sub-processor implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the personal data are processed or used, including:

- establishing security areas;

- protection and restriction of access paths;

- establishing access authorizations for employees and third parties, including the respective documentation;

- the data centre where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

- all access to the data centre where personal data are hosted is logged, monitored, and tracked; and

  the data centre where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

Access Control to Data Processing Systems

Data importer/sub-processor implements suitable measures to prevent their data processing systems from being used by unauthorized persons, including:

- use of adequate encryption technologies;

- identification of the terminal and/or the terminal user to the data importer/sub-processor and processing systems;

- automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;

- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and

- all access to data content is logged, monitored, and tracked.

Access Control to Use Specific Areas of Data Processing Systems

Data importer/sub-processor commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the personal data;

- release of data only to authorized persons, including allocation of differentiated access rights and roles;

- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;

- monitoring capability in respect of individuals who delete, add or modify the personal data;

release of data only to authorized persons, including allocation of differentiated access rights and roles;

- use of adequate encryption technologies; and

- control of files, controlled and documented destruction of data.

Availability Control

Data importer/sub-processor implements suitable measures to ensure that personal data are protected from accidental destruction or loss, including:

- infrastructure redundancy; and

- backup is stored at an alternative site and available for restore in case of failure of the primary system.

Transmission Control

Data importer/sub-processor implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;

- certain highly confidential employee data (e.g., personally identifiable information such as National ID numbers, credit or debit card numbers) is also encrypted within the system; and

- providing user alert upon incomplete transfer of data (end to end check); and

- as far as possible, all data transmissions are logged, monitored and tracked.

Input Control

Data importer/sub-processor implements suitable input control measures, including:

- an authorization policy for the input, reading, alteration and deletion of data;

- authentication of the authorized personnel;

- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;

- utilization of unique authentication credentials or codes (passwords);

- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;

- automatic log-off of user ID's that have not been used for a substantial period of time; and

- proof established within data importer/sub-processor's organization of the input authorization; and

- electronic recording of entries.

Separation of Processing for different Purposes

Data importer/sub-processor implements suitable measures to ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users;

- modules within the data importer/sub-processor's data base separate which data is used for which purpose, i.e. by functionality and function;

- at the database level, data is stored in different normalized tables, separated per module, per Controller Customer or function they support; and

- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Documentation

Data importer/sub-processor will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data importer/sub-processor shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Appendix 2.

Monitoring

Data importer/sub-processor shall implement suitable measures to monitor access restrictions to data importer/sub-processor's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- individual appointment of system administrators;

- adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;

- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the data importer/sub-processor and applicable laws;

- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to data exporter upon request.

CUSTOMER (DATA EXPORTER):		BITNINJA KFT. (DATA IMPORTER):	
BY		**BY**	
NAME		**NAME**	
TITLE		**TITLE**	
ADDRESS		**ADDRESS**	
DATE		**DATE**	