Data Processing Addendum

This Data Processing Addendum, including its appendices and the Standard Contractual Clauses (as defined below) attached hereto (collectively, the "DPA") is incorporated by reference to the agreement governing the use of Smartnova's Services ("Agreement) entered by and between the Customer ("Customer", "you") and Smartnova Limited ("Smartnova") and is made as of the effective date of the applicable Customer's acceptance of the Agreement (or an applicable Order Form) or the effective date on which parties otherwise agreed to this DPA ("the Effective Date").

By using the Services, the Customer accepts this DPA that reflects the parties' agreement with regard to the Processing of Customer Personal Data and you warrant and represent that you have full authority to bind the Customer to this DPA. If you cannot, or do not agree to, comply with and be bound by this DPA, or do not have authority to bind the Customer on any other entity, please do not provide Customer Personal Data (as defined below) to us.

1. Definitions

All capitalized terms not otherwise defined in this DPA will have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

"**Customer Personal Data**" means Personal Data under GDPR, contained within the Customer Data Processed by Smartnova for or on behalf of Customer pursuant to or in connection with the Services under the Agreement;

"**Customer Data**" means any and all information, content, communication (commercial or otherwise), data or other materials (including but not limited to Customer Personal Data) inserted, created, shared, generated or otherwise made available, by or for Customer to or through the Services.

"**Data Protection Laws**" means the GDPR, and the UK GDPR that apply to the Processing of Customer Personal Data under the Agreement, where applicable, in each case, as amended from time to time;

"**Data Subject**" means an identified or identifiable natural person whose rights are protected by GDPR;

"**EEA**" means European Economic Area;

"**GDPR**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation);

"**UK GDPR**" means the UK Data Protection Act 2018;

"**Sub-Processor**" means any existing or new person or entity appointed by or on behalf of Smartnova in order to provide parts of the Services (software, tool, components, etc.) and to Process Customer Data on behalf of Customer under the Agreement;

"**Standard Contractual Clauses**" means the Standard Contractual Clauses for the Transfer of Personal Data from EEA to Third Countries approved by the European Commission Decision of 4 June 2021 and attached to, and incorporated into this DPA in Exhibit C ("EU Standard Contractual Clauses (Module 2);

"**UK Addendum**" means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018, as may be amended, superseded or replaced from time to time;

The terms "Commission", "Controller", "Member State", "Personal Data", "Personal Information", "Processing", "Process," "Processed", "Processor", "special categories of personal data", "Sensitive Data" and "Supervisory Authority" shall have the same meaning as in applicable Data Protection Laws and shall be construed accordingly.

2. Processing of Personal Data

2.1 With respect to Customer Personal Data, Smartnova and Customer hereby agree that (i) Customer may act as "Controller" and Smartnova may act as "Processor" under the GDPR or (ii) Customer may act as "Data Exporter" and Smartnova may act as " Data Importer" as defined under the Standard Contractual Clauses or (iii) Customer as a "Exporter" and Smartnova as an "Importer" under UK GDPR.

2.2 Subject to the terms of the Agreement (i) Customer as Controller or Business or Data exporter under Data Protection Laws, hereby appoints Smartnova as Processor or Service Provider or data importer in respect of Processing operations required to be carried out by Smartnova on Customer Personal Data in accordance with the terms of the Agreement, (ii) Customer agrees to comply with its obligations as Controller or Business or data exporter under Data Protection Laws and declares that it has been instructed by and obtained the authorization of the relevant Controller or Business or data exporter to enter into this DPA in the name and on behalf of such Controller or Business or data exporter, (iii) Customer is responsible for obtaining all of the necessary authorizations and approvals and all consents and rights necessary under Data Protection Laws to enter, use, provide, store, and Process Customer Data, including Customer Personal Data in the Services to enable Smartnova's fulfillment of its obligations pursuant to the Agreement.

2.3 Smartnova shall (i) process Customer Personal Data only in accordance with Customer's lawful instructions consistent with the terms of the Data Protection Laws and (ii) Process all Customer Personal Data as Processor or Services Provider or data importer under the applicable Data Protection Laws to fulfill its obligations under the Agreement for or on Customer's behalf, and for no other purposes than in connection with the Services, unless required to do so by Data Protection Laws or other applicable data privacy laws to which Smartnova (or Sub-Processor(s)) is subject. In such a case Smartnova shall to the extent permitted by the Data Protection Laws inform Customer of that legal requirement before the relevant Processing of the Customer Personal Data. Each party will comply in all respects with the provisions of this DPA and the applicable Data Protection Laws

in any country where the Services are used, provided or delivered. Customer hereby agrees and understands that the processing of personal data by Smartnova is always triggered by the type of Services, or function for which Customer has registered or activated. Consequently, the Parties agree that the moment when Smartnova initiates the processing of personal data is always understood to be at the express instruction of Customer to do so for and on behalf of Customer.

2.3. Customer represents and warrants that (i) it is and will at all relevant times remain duly and effectively authorized to give Smartnova the instruction for the Processing of Customer Personal Data covered by this DPA; (ii) that the Processing, including the onward transfer itself, of the Customer Data has been and will continue to be lawfully carried out in accordance with the relevant provisions of the applicable Data Protection Laws (ii) that it has instructed and will have on continuous basis a legal basis for the Processing by Smartnova and transfer of Customer Data for or on behalf of Customer. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Data and the means by which Customer acquired them.

2.4 This DPA, the Agreement and an applicable Order Form, thereunder contain Customer's sole instructions to Smartnova for the Processing of Customer Personal Data, including without limitation the transfer of Customer Data to any country or territory as defined in this DPA. Additional instructions outside the scope of the Agreement or this DPA will be agreed separately between the parties in writing (also electronically).

2.5 The duration of the Processing, the nature and purpose of the Processing, the types of Customer Data subject to the applicable Data Protection Laws and categories of Data Subjects Processed under this DPA, as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws), are further specified in Exhibit A to this DPA, as may be amended by the parties from time to time.

2.6 Customer acknowledges and agrees that the Services are not intended for the Processing of Customer Personal Data defined as special categories of personal data, Sensitive data, genetic data, biometric data, data concerning health, under applicable Data Protection Laws, and Customer will not provide (or cause to be provided) any such data to Smartnova for Processing under the Agreement and Smartnova will have no liability whatsoever for such data whether in connection with Personal Data Breach or otherwise.

3. Smartnova Personnel

As long as Smartnova is obliged to fulfill its obligations under the Data Protection Laws, Smartnova will ensure that its personnel engaged in the Processing of Customer Personal Data are informed of its confidential nature, have received appropriate training on their responsibilities and role and shall have access to Customer Personal Data to the minimum necessary to provide and maintain the Services.

4. Sub-processors

4.1 For the purpose of the delivery of Services, Customer hereby authorizes appointed Sub-Processors and gives Smartnova a general written consent to engage new Sub-Processors in connection with the provision of the Services, including without limitation for the Processing of Customer Personal Data on behalf of Customer.

4.2 Customer may request Smartnova on the list of the authorized Sub-Processor(s) with access to Customer Personal Data. Subject matter of such request, at least 10 days before Smartnova authorizes new Sub-Processor(s) with access to Customer Personal Data, Smartnova will inform the Customer by giving a reasonable notice. Customer may object in writing (also electronically) to Smartnova's appointment of a Sub-Processor(s) within five (5) calendar days of such authorization, provided that such objection is based on reasonable grounds relating to data protection, otherwise Customer shall be deemed to have accepted the respective Sub-processor(s) to Process Customer Personal Data. If Customer legitimately objects to the appointment of a Sub-Processor(s), the parties will discuss such concerns in good faith with a view to achieving resolution, provided that if this is not possible, Customer may suspend or terminate the Agreement without prejudice to any fees incurred by Customer prior to suspension or termination.

4.3 Any Sub-Processor(s) utilized by Smartnova (i) will only be given access to the Customer Data as is reasonably necessary to provide the Services and Smartnova will enter and maintain a written agreement with any Sub-Processor providing parts of its Services (software, components, other tools) as long as it has access to Customer Personal Data with a not less protective level of data protection than that provided for in this DPA and (ii) shall provide to Customer for review copies of such agreements with Sub-processor(s) as Customer may reasonably request once annually, provided that all commercial information and clauses unrelated to data privacy and security may be removed by the Smartnova beforehand and (iii) will be liable for the acts and omissions of its Sub-processors to the same extent Smartnova would be liable if performing the services of its Sub-Processors directly under the terms of the Agreement.

5. Security

5.1 Taking into account, the costs of implementation and the nature, scope, context and purposes of Processing Customer Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Smartnova shall, in relation to the Customer Personal Data implement and maintain throughout the term of the Agreement, the technical and organizational measures set forth in Exhibit B of this DPA (the "Security Measures").

5.2. Customer acknowledges and agrees that the Security Measures implemented by Smartnova provide a level of security appropriate to the risk to Customer Personal Data and the nature of the data to be protected under the requirements of the applicable Data Protection Laws, in particular where the Processing involves the onward transmission of data over a network. Smartnova, at its sole discretion, may modify such safeguards from time to time, provided that such modifications will not materially reduce the overall level of protection for Customer Personal Data.

5.3. Notwithstanding the above, Customer agrees that, except as provided by this DPA, Customer acknowledges that the Services will Process Customer Data in accordance with Customer's configurations in the Services, which Smartnova does not monitor. Customer agrees that, except as provided by this DPA, is solely responsible for (i) the data entered into the Services and shall be fully capable to determine correctness and legality of such data and (ii) for its secure use of the Services, including securing its account authentication credentials, systems and devices Customer uses to access the Services (if and as applicable), storage of any copies of Customer Data outside Smartnova, and backing up its Customer Data as appropriate and protecting the security of Customer Personal

Data when in transit to and from the Services. Customer has the full responsibility for the Customer's permitted users use and settings of the features in the administration area of the Services are in accordance with the applicable Data Protection Laws, the Agreement and this DPA. Customer has the full responsibility for managing Permitted users rights and their access to the Customer's account in the Services, including assessing and addressing any issues that may arise in sharing login details. Customer must inform its Permitted users of the obligations that lie with each user under this DPA and the Agreement.

6. Data Subject Rights

Taking into account the nature of the Processing, Smartnova shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws. Smartnova will, to the extent required by Data Protection Laws, promptly notify Customer upon receipt of a request by a Data Subject that relates to Customer Personal Data and identifies Customer, to exercise Data Subject rights under the applicable Data Protection Laws. Smartnova will advise the Data Subject to submit their request to Customer and Customer will be ultimately responsible for responding to such request, including, where necessary and possible, by using the functionality of the Services on its own. Smartnova may reasonably assist Customer with Data Subject Rights as required by Data Protection Laws to the extent Smartnova is legally permitted to do so, is technically capable to do it and has reasonable access to the relevant Customer Data.

7. Personal Data Breach

Smartnova will, without undue delay after discovery of a Customer Personal Data Breach on the Processor's facilities affecting Data Subject of Customer, (i) notify via email Customer of the Customer Personal Data Breach and will provide Customer with reasonable assistance and sufficient information to making any notification to a Supervisory Authority or any communication to affected Data Subject and (ii) take reasonable steps to minimize harm and secure Customer Personal Data and to improve data protection process internally, if applicable.

8. Assistance on Data Protection Impact Assessment and Consultations.

To the extent required under applicable Data Protection Laws, and taking into account the nature of the Processing Customer Personal Data and the information available to Smartnova, Smartnova will provide reasonable cooperation to Customer regarding the Services (at Customer's expense prior demonstrated to Customer, if such reasonable cooperation will require Smartnova to assign significant resources to that effort) to enable Customer to carry out data protection impact assessments or prior consultations with any Supervisory Authorities, as required by such Data Protection Laws.

9. Return or Deletion of Customer Personal Data

9.1 If Customer wishes to delete its Customer Personal Data during or after the end of the subscription, Smartnova, within 30 days of Customer's written request prior to such termination, shall return and delete requested Customer Personal Data to Customer in a standard format accepted by Smartnova and in accordance with Smartnova's data retention policy with a right to keep a copy of it if applicable legislation or proceedings or any claims, or reasonable rightful grounds do not prevent it from doing so. In any such case, Customer agrees that Smartnova and Sub-Processors may

retain Customer Personal Data, or any portion of it, in storage as a backup only to the extent and for such period as needed and always provided that Smartnova shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed and stored as necessary for the legal purpose(s) and for no other purpose. Certification of return/deletion of Customer Personal Data will only be conducted upon Customer's request.

9.2 During the term of the Agreement, Smartnova will make Customer Data available to Customer in a manner consistent with the functionality of the Services and in accordance with the terms of the Agreement. To the extent Customer, in its use and administration of the Services during the term of the Agreement, does not have the ability to migrate Customer Data (as required by Data Protection Laws) to another system or service provider, Smartnova will, at Customer's reasonable expense, prior demonstrated to Customer (if such reasonable cooperation will require Smartnova to assign significant resources to that effort) reasonably assist Customer in facilitating such actions to the extent Smartnova is legally permitted to do so, technically capable to do it and has reasonable access to the relevant Customer Data.

9.3 Customer agrees that after the termination or expiration of the Agreement their data may be stored as a backup for legal and compliance purposes. Notwithstanding the foregoing, Smartnova shall not reduce the Security Measures at any time until such Data is permanently deleted.

10. Audit

10.1 The parties acknowledge that when Smartnova is acting as a processor on behalf of Customer, Customer must be able to assess Smartnova's compliance with its obligations under applicable Data Protection Laws and this DPA. Smartnova shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA.

11. Cross Border Data Transfer Mechanism

11.1 To the extent that Customer's use of the Services requires a transfer of Customer Personal Data outside the EEA or UK, and to the extent that Smartnova is a recipient of Customer Personal Data in a country that is not recognized as providing an adequate level of protection for Customer Personal Data as described in the GDPR, Smartnova and Customer ensure that such transfers are compliant with the Standard Contractual Clauses and UK Addendum as follow:

11.2 i) The parties agree that the EU Standard Contractual Clauses (Module 2) attached to this DPA in Exhibit C, will apply to Customer Personal Data that is transferred from the EEA to the Services and via the Services from the EEA, either directly or via onward transfer, to any country or recipient where Smartnova or its Sub-processors maintain data processing operations, as necessary to perform the Services not recognized by the European Commission as providing an adequate level of protection for Customer Personal Data. The parties agree that their obligations under the EU Standard Contractual Clauses (Module 2) will be carried out in accordance with the provisions of this DPA. In addition, the parties hereby agree that if the EU Standard Contractual Clauses (Module 2) set forth at Exhibit C to this DPA, will no longer be a valid basis under the decision of the European Commission for establishing adequate protections in respect of a relevant data transfer of Customer Personal Data, the parties agree to comply with an alternative transfer mechanism instead of the transfer mechanisms described in this DPA in respect of the Processing of such Customer Personal Data. In the event that any provision of the EU Standard Contractual Clauses (Module 2) is held

illegal or unenforceable in a judicial proceeding, such provision shall be severed and shall be inoperative, and the remainder of the EU Standard Contractual Clauses (Module 2) and the terms of this DPA shall remain operative and binding on the parties.

11.2 ii) The parties agree that the UK Addendum will apply to Customer Personal Data that is transferred from the United Kingdom ("UK") to the Service and via the Service from the United Kingdom ("UK"), either directly or via onward transfer, to any country or recipient outside of the UK where Smartnova maintain data processing operations, as necessary to perform the Services not recognized by the competent UK regulatory authority or governmental body for the UK as providing an adequate level of protection for Personal Data. If Customer's Personal Data are transferred to Sub-processors, the applicable transfer mechanism shall apply. The parties agree that their obligations under the UK Addendum will be carried out in accordance with the provisions of this DPA. In addition, if the UK GDPR applies to the transferred Customer Personal Data, the EU Standard Contractual Clauses (Module 2) as incorporated in this DPA shall apply with the following modifications: (i) the EU Standard Contractual Clauses (Module 2) shall be amended as specified by the UK Addendum, which shall be incorporated by reference to this DPA, (ii) Tables 1 to 3 in Part 1 of the UK Addendum shall be populated with the information from Exhibits A (Details of Processing), B (Technical and Organizational Security Measures) and C (Standard Contractual Clauses), and Section 4.1. of this DPA, (iii) Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "importer"; and (iv) any conflict between the the EU Standard Contractual Clauses (Module 2) and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum. Each party's signature to this DPA will be considered a signature to the UK Addendum. The parties hereby agree that if the UK Addendum will no longer be a valid basis under the competent UK regulatory authority or governmental body for the UK for establishing adequate protections in respect of a relevant data transfer of Customer Personal Data, the parties shall comply with an alternative transfer mechanism instead of the transfer mechanisms described in this DPA in respect of the Processing of such Customer Personal Data.

12. Liability

12.1 Smartnova shall be liable toward Customer for any direct damage caused to the Customer due to the non-compliance with this DPA the Processing of Customer Personal Data entrusted to Smartnova by Customer, except where the damage(s) is the result of an action or omission for which Smartnova is not responsible.

12.2 Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA will be subject to the exclusions and limitations of liability set forth in the Agreement.

13. General

13.1 This DPA replaces any previously applicable data processing addendum as from the Effective Date and supersedes and replaces all prior representations, understandings, communications, and agreements by and between the parties in relation to the matters set forth in this DPA.

13.2 In the event of a conflict between the Agreement and this DPA in relation to data protection, the terms of this DPA will take precedence to the extent of the conflict.

13.3 This DPA will terminate upon the earliest of: (i) termination of the Agreement as permitted hereunder (and without prejudice to the survival of accrued rights and liabilities of the parties and any obligations of the parties which either expressly or by implication survive termination); (ii) as earlier terminated pursuant to the terms of this DPA or (iii) as agreed by the parties in writing.

EXHIBIT A TO DPA: DETAILS OF PROCESSING

1. Duration of the Processing:

We keep Personal Data for only as long as it is needed to complete the purpose for which it was collected as defined by the Agreement or processed as required by law, complying with our legal obligations (legal, tax, or regulatory reasons), resolving disputes, and enforcing our agreements, provided that we ensure the Security Measures for all retained data.

2. Nature and Purpose of the Processing:

The scope and purpose of Processing of the Customer Personal Data is:

- to provide, maintain and facilitate the Smartnova's Services as well as to ensure safeguards of Services performance, upgrade and improve the functionality of the Services;

- to provide Customer with access to its Customer Personal Data (including chat content) and maintain this access via standard API methods for the duration of paid subscription to the Services (active subscription) in accordance with the Agreement and this DPA;

- to secure Customer's as well as Smartnova's claims that may arise due to the Services

- in order to comply with our legal obligations (i.e. legal, tax or regulatory reasons), and essential purpose (legitimate interest, resolving disputes and enforcing our agreements).

3. Categories of Data Subjects:

Data subjects include Customer's employees, and individuals authorized by Customer to access Customer's account in the Services, and Customer's end-users communicating/interacting with Customer via Services. Data Subjects may also include individuals attempting to communicate or transfer personal information to users of Smartnova's Services. Data Subjects exclusively determine the content of data submitted to Smartnova. Due to a full autonomy of Data Subjects regarding data entered to the Services, Smartnova shall not be liable for any data in the Services regardless if it constitutes Personal Data or not.

4. Sensitive Data or Special Categories of Data (if appropriate):

Smartnova and Customer do not want to, nor do it intentionally, collect or Process any Sensitive Data, special categories of data, genetic data, biometric data, data concerning health in connection with the provision of the Services. Customer is solely responsible for ensuring that suitable safeguards are in place prior to transmitting or processing any Customer's Personal Data to transmit

or process any Sensitive Data, special categories of data, genetic data, biometric data, data concerning health via the Services.

5. Types of Personal Data of Customer:

Customer Personal Data may include but is not limited to email, first name and last name, address, title, contact details, username, chat history, financial information (credit card details, account details, payment information); employment details (employer, job title) and other data in an electronic form provided in the context of Smartnova's Services (specified in the Agreement).

EXHIBIT B TO DPA: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES
Description of the technical and organisational measures implemented by the data importer (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. Access Control. Personnel. Smartnova's personnel will not process Customer Personal Data without authorization and shall have access to Customer Personal Data to the minimum necessary to provide and maintain the Services.

2. Data Privacy Contact

Smartnova Limited

Avlonos, 1 Maria House 1075, Nicosia, Cyprus

Email: support@novatalks.ai

3. Technical and Organization Measures. Smartnova has implemented and will maintain, for the entire term of the Agreement with Customer, appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Personal Data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

3.1 Risk Management.

(a) Risk Assessment is carried out annually;

(b) Smartnova implements measures, as needed, to address discovered risks in a timely manner.

3.2 Storage. Smartnova's database servers are hosted in a data center operated by a third party vendor. Smartnova maintains complete administrative control over the virtual servers, and no third-party vendors have logical access to Customer Personal Data.

3.3 Asset Management:

(a) Asset Inventory. Smartnova maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to authorized personnel;

(b) Asset Handling. Smartnova's employees are required to utilize encryption to store data in a secure manner and is required to use two-factor authentication whenever is reasonable and applicable.

3.4 Software Development and Acquisition: Software developed by Smartnova has secure coding standards and procedures as set out in its standard operating procedures.

3.5 Change Management: Smartnova implements change management that provide a consistent approach for controlling, implementing, and documenting changes (including emergency changes) for Smartnova's software, information systems or network architecture.

3.6 Third Party Provider Management: In selecting third party providers who may gain access to, store, transmit or use Customer Personal Data, Smartnova conducts a quality and security assessment pursuant to the provisions of its standard operating procedures.

3.7 Human Resources Security. Smartnova informs its personnel about relevant security procedures and their respective roles, as well as of possible consequences of breaching the security rules and procedures. Such consequences include disciplinary and/or legal action.

3.8 Physical and Environmental Security:.

(a) Physical Access to Facilities. Smartnova limits access to facilities where information systems that process Customer Data are located to identify authorized individuals who require such access for the performance of their job function. Smartnova terminates the physical access of individuals promptly following the date of the termination of their employment or services or their transfer to a role no longer requiring access to Customer Personal Data;

(b) Protection from Disruptions. Smartnova uses commercially reasonable systems and measures to protect against loss of data due to power supply failure or line interference.

3.9 Communications and Operations Management:

(a) Security Documents. Smartnova maintains security documents describing its security measures and the relevant procedures;

(b) Data Recovery Procedures:

(i) On an ongoing basis, Smartnova maintains multiple copies of Customer Personal Data from which it can be recovered;.

(ii) Smartnova stores copies of CustomerData and data recovery procedures in a different place from where the primary computer equipment processing Customer Personal Data is located;

(iii) Smartnova has procedures in place governing access to copies of Customer Personal Data;

(iv) Smartnova implements anti-malware controls, based on the risk assessment, to help avoid malicious software gaining unauthorized access to Customer Personal Data;

(c) Encryption; Mobile Media. Smartnova uses HTTPS encryption on all data connections. Smartnova restricts access to Customer Personal Data in media leaving its facilities. Smartnova further has a destruction policy for hardware in the data center that stores Customer Personal Data;

(d) Event Logging. Smartnova logs the use of data-processing systems. Logs are maintained for at least 10 days.

3.10 Access Control.

(a) Records of Access Rights. Smartnova maintains a record of security privileges of individuals having access to Customer Personal data;

(b) Access Authorization:

(i) Smartnova maintains and updates a record of personnel authorized to access systems that contain Customer Personal Data;

(ii) Smartnova deactivates authentication credentials of its personnel immediately upon the termination of their services;

(c) Least Privilege:

(i) Smartnova restricts access to Customer Personal Data to only those individuals who require such access to perform their role and responsibilities;

(d) Integrity and Confidentiality;

(i) Smartnova instructs its personnel to disable administrative sessions when leaving the Smartnova's premises or when computers are unattended;

(ii) Smartnova's stores passwords in a way that makes them unintelligible while they are in force;

(e) Authentication;

(i) Smartnova uses commercially reasonable practices to identify and authenticate users who attempt to access information systems;

(ii) Where authentication mechanisms are based on passwords, Smartnova requires the password to be at least 6 or at least 8 characters long (depending on the Services);

(iii) Smartnova allows using double authorization (2-factor authentication) of access to the Services.

(iv) Smartnova ensures that de-activated or expired identifiers are not granted to other individuals;

(v) Network Design. Smartnova has controls to avoid individuals assuming access rights they have not been assigned to gain access to customer data they are not authorized to access.

3.11 Network Security:

(a) Network Security Controls. Smartnova's information systems have security controls designed to detect and mitigate attacks by using logs and alerting;

(b) Antivirus. Smartnova's implements endpoint protection, whenever it is reasonable due to the potential attack surface and technically applicable, on its hosting environments, including antivirus; which are continuously updated with critical patches or security releases.

3.12 Information Security Incident Management.

(a) Record of Breaches. Smartnova maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and the procedure for recovering data;

(b) Record of Disclosure. Smartnova tracks disclosures of Customer Personal Data, including what data has been disclosed, to whom, and at what time, unless prohibited by law.

3.13 Technical and organizational measures to be taken by the sub-processor to provide assistance to the controller and for transfers from a processor to a sub-processor to the Customer. When Smartnova engages a Sub-Processor under this DPA, Smartnova and a Sub-Processor enter into an agreement with data protection obligations substantially similar to those contained in this DPA. Smartnova will restrict Sub-Processor's access to Customer Personal Data only to what is strictly necessary to provide the Services, and Smartnova will prohibit the Sub-Processor from Processing the Customer Data for any other purpose.

3.14 Safeguards Control

Smartnova conducts regular testing and monitoring of the effectiveness of its safeguards and controls.

EXHIBIT C TO DPA: STANDARD CONTRACTUAL CLAUSES
MODULE 2 (TRANSFER CONTROLLER TO PROCESSOR)
SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Not applicable

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf

and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent

supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's

request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([5]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Poland.]

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Poland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts. Court of Poland

ANNEX I
A. LIST OF PARTIES

Data exporter:

Name: Customer as defined in the Data Processing Addendum to the Agreement or Order Form, if any

Address: As specified in the Agreement or Order Form, if any

Contact person's name, position and contact details: As specified in the Agreement Order Form, if applicable

Activities relevant to the data transferred under these Clauses: As described under Section B

Signature and date: The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of these Clauses by both parties on the Effective Date of the Agreement.

Role: Controller

Data importer:

Name: Smartnova, Inc.

Address: 101 Arch Street, 8th Floor Boston, MA 02110 United States of America

Contact person's name, position and contact details: Maciej Malesa, DPO support@Smartnova.com

Activities relevant to the data transferred under these Clauses: As described under Section B.

Signature and date: The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of these Clauses by both parties on the Effective Date of the Agreement.

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: as described in Exhibit A to this DPA

Categories of personal data transferred: data exporter may submit personal data to the Service to the extent that, under data exporter's sole discretion and control, may concern the data as identified in Exhibit A of this DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: as described in Exhibit A to this DPA

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): The frequency of transferring the personal data is continuous, until the Agreement or Order Form (if any) comes to an end

Nature of the processing: as described in the Exhibit A to this DPA

Purpose(s) of the data transfer and further processing: the purpose of processing the personal data is to provide the Service to Customer in accordance with the Agreement and will be subject to the processing activities described in this DPA and Exhibit A.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: we retain and process the personal data on behalf of the data exporter for as long as they remain a Customer. When the data exporter terminates its use of the Services, we delete their user/Customer data within 30 days of the account/subscription termination.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: we appoint sub-processors in order to facilitate the delivery of our products/Services and to help us to maintain Services effectively and efficiently. The subject matter pertains mainly to new features/tools that we add to our Services in order to develop its functionality. The nature of the processing relates to facilitating usage of our Services, such as but not limited to facilitating document storage, email services, community forum platform.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Supervisory of Polish Office of Personal Data Protection (Urząd Ochrony Danych Osobowych)

ANNEX II
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The technical and organisational security measures implemented by data importer are as described in Exhibit B of this DPA.