Appendix D - Data Processing Agreement

1. BACKGROUND AND PURPOSE

1.1 The Parties have entered into a service agreement under which the Processor shall provide the Controller with certain services (the "Main Agreement"). The performance of the Main Agreement will entail processing of personal data by the Processor on behalf of Controller and the Parties have therefore entered into this Data Processing Agreement (the "DPA").

1.2 The nature and purpose of the processing under the DPA, as well as the type of personal data and categories of data subjects and other instructions regarding the processing of the personal data, is set forth in Schedule 1.

2. DEFINITIONS

Terms used and defined in the GDPR shall have the same meaning in the DPA; whereof some have been noted below. In addition, the following terms in the DPA shall have the meaning set out below. In the event of a conflict between terms defined below and terms defined in the GDPR, the definitions in the GDPR shall take precedence.

processing	In accordance with article 4.2 in the GDPR, any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
DPA	As defined in section 1 above.
representative	A natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27 in the GDPR, represents the controller or processor with regard to their respective obligations under the GDPR.
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council.
Applicable law	is defined as the General Data Protection Regulation (EU) 2016/679, (GDPR) and in addition, applicable national legislation and the binding directions of the Swedish Authority for Privacy Protection, or other competent body.
Main Agreement	As defined in 1.1 above.
personal data	In accordance with article 4.1 in the GDPR, any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
personal data breach	In accordance with article 4.12 in the GDPR, a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Controller	The customer defined in the Main Agreement.
Processor	Voyado Lund AB, org. nr: 556588-5240
standard contractual clauses	The Commission Implementing Decision 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation 2016/679 of the European Parliament and of the Council or any replacing Commission Decision on standard contractual clauses.
third country	A country which is not a member of the EU or EEA.
sub-processor	A processor that has been engaged by the Processor and processes personal data on behalf of the Controller.

3. THE RESPONSIBILITIES OF THE CONTROLLER

3.1 The Controller shall ensure that there is a legal basis for the current processing of personal data in accordance with applicable law.

3.2 The Controller shall draw up and provide the Processor with written instructions to the extent this is necessary in order for the Processor and any sub-processor to perform its obligations under the DPA and under applicable law (Schedule 1).

3.3 The Controller may only provide the Processor with such personal data that are necessary for the specific purposes of the processing. The Controller shall ensure that all personal data provided by the Controller to the Processor is pseudonymized.

3.4 The Controller undertakes to inform the Processor without delay of changes in the processing that affect the obligations of the Processor pursuant to applicable law.

3.5 The Controller is responsible for advising registered persons of the processing carried out in accordance with the DPA and, if required, for obtaining the registered person's consent, and for safeguarding the right of registered persons to data transparency, deletion, etc.

4. PROCESSING OF PERSONAL DATA

4.1 The Processor may only process the Controller's personal data for the purpose stated in this DPA for fulfilling its duties towards the Controller and/or as specified in mandatory legislation.

4.2 The Processor undertakes to process the personal data only in accordance with this DPA and applicable law. Hence, the Processor may only process the personal data for the purposes instructed by the Controller.

4.3 The Processor may only process the personal data on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by mandatory legislation to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.4 If the Controller has given the Processor incomplete or faulty instructions, the Processor shall immediately notify the Controller of this. In the absence of instructions, which the Processor considers to be necessary for the performance of the assignment given to the Processor by the Controller, the Processor shall, without delay, inform the Controller and await any instructions that the Processor finds necessary.

4.5 The Processor shall, without unreasonable delay, inform the Controller when the Processor considers that a processing violates any applicable law and await further instructions from the Controller.

4.6 On request from the Controller, the Processor shall, without unreasonable delay:

(a) give the Controller access to a readable transcript of the personal data of a data subject that is processed by the Processor;

(b) give the Controller access to the personal data that the Processor has in its possession; and

(c) make a required rectification, erasure, restriction of processing or transfer of the personal data described in 6.6 (a) and (b) in accordance with applicable data protection regulations.

4.7 If the Controller has erased or instructed the Processor to erase personal data, the Processor shall take the necessary measures to make sure the erased personal data cannot be re-created.

4.8 The Processor, and where applicable, the Processor's representative, shall maintain a written (including in electronic form) record of all categories of processing activities carried out on behalf of the Controller, in accordance with article 30 of the GDPR. The record shall contain at least the following information:

(a) the name and contact details of the Processor or processors and of each controller on behalf of which the Processor is acting, and, where applicable, of the Controller's or the Processor's representative, and the data protection officer;

(b) where applicable, name and contact details of sub-processors and, if applicable, the representatives and data protection officers that has been appointed by the sub-processors;

(c) the categories of processing carried out on behalf of each controller;

(d) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, the documentation of suitable safeguards; and

(e) where possible, a general description of the technical and organisational security measures referred to in Article 32(1) of the GDPR.

4.9 The Processor and, where applicable, the Processor's representative, shall make the record available to the Controller and the supervisory authority on request.

5. CAPACITY AND ABILITY

5.1 Both Parties guarantee that it has the necessary technical and organisational capacity and ability, including technical solutions, competence, economic and personnel resources, routines, and methods to fulfil its obligations according to the DPA and applicable law.

5.2 The Processor shall, without unreasonable delay, give the Controller, or an independent third party appointed by the Controller, access to all information necessary to demonstrate that the Processor is in compliance with its obligations according to the DPA and applicable law, for example by providing relevant documentation, refer to relevant and approved code of conduct or certification as well as to enable and contribute to audits, including inspections, carried out by the Controller or by another auditor appointed by the Controller.

5.3 The Processor is only obliged to give the Controller, or an independent third party appointed by the Controller, access to facilities and equipment for the purpose of audits if such audits are necessary in order to perform a legal obligation.

6. SECURITY MEASURES

6.1 Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluation the effectiveness of technical and organisational measures for ensuring the security of the processing;

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

6.3 The Processor shall have an authorisation control system that impedes the unauthorised processing of personal data or unauthorised access to personal data. The Processor shall use a logging system that makes it possible for the processing of personal data to be traced and shall also ensure that the logs have adequate security protection.

6.4 If the Parties specifically agree that the Processor shall process personal data on behalf of the Controller, such processing shall be specified in Schedule 1. The Parties shall further agree on any necessary further security measures and the Controller shall be responsible for any additional costs for such.

6.5 The Processor shall take steps to ensure that any natural person acting under the authority of the Processor who has access to personal data does not process them except in accordance with this DPA and on instructions from the Controller unless he or she is required to do so by Union or Member State Law.

6.6 The Processor shall, through appropriate technical and organisational measures, limit the access of the personal data and only give authorization to the personnel that require access in order for the Processor to fulfil its obligations under the DPA. The Processor shall also make sure that the authorized personnel have the necessary education and that they have been instructed to handle the personal data in accordance with this DPA and in an appropriate and secure manner.

7. CONFIDENTIALITY

7.1 The Processor and the personnel working under this DPA shall respect their duty of confidentiality when processing personal data. The personal data, information, instructions, system solutions, descriptions, or other documents that the Processor receives through the exchange of information in accordance with this DPA or other agreement between the parties may not be used or disclosed for any other purpose than that stipulated in this DPA or other agreement between the Parties, whether directly or indirectly, if the Controller has not consented to this in writing.

7.2 The Processor undertakes to ensure that all employees, consultants, and other persons for whom the Processor is responsible and who process the personal data are bound by a confidentiality clause. (Confidentiality clauses are not required if the Processor and his personnel are bound by a duty of confidentiality sanctioned by penalties in accordance with the law.) The Processor also undertakes to ensure that there are appropriate confidentiality agreements in place with any sub-processor and a confidentiality clause governing the relationship between the sub-processor and his personnel.

7.3 A Party shall inform the other Party in writing without delay of any contacts with a supervisory authority that concern or may be of significance for the processing of the personal data. Neither Party has the right to represent the other Party or act on behalf of the other Party in dealings with supervisory authorities on matters that concern or may be of significance for the Processing of the personal data.

7.4 If Registered Persons, supervisory authorities and other third parties request information from the Processor concerning the Processing of personal data, the Processor shall refer these persons to the Controller. The Processor may not disclose personal data or other information on the Processing of personal data without the prior written permission of the Controller. The Processor undertakes, on receiving such permission, to assist in providing registered persons, supervisory authorities or other third parties with information on the processing of personal data.

8. PERSONAL DATA BREACH

8.1 The Processor shall provide and implement technical and practical solutions to investigate suspicions that an unauthorised person has processed or gained unauthorised access to the personal data.

8.2 The Processor shall notify the Controller without undue delay, not later than within 72 hours, after becoming aware of a personal data breach or the risk of a personal data breach. The notification shall contain all necessary and available information that the Controller will need in order to take appropriate preventive measures and remedial actions and to fulfil the Controller's obligations as regards notification of a personal data breach to the supervisory authority, document the personal data breach and inform the data subject of

the personal data breach in accordance with the applicable law. Furthermore, the Processor shall investigate the personal data breach and take appropriate measures to mitigate its possible adverse effects and prevent it from happening again.

8.3 The notification of a personal data breach shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and the approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach; and

(d) describe the measures taken by the Processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

9. COOPERATION

9.1 The Processor shall, taking into the account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to request for exercising the data subject's rights in accordance with applicable law.

9.2 The Processor shall, taking into account the nature of processing and the information available to the Processor, assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR or any applicable law amending these obligations, for example (i) security of processing, (ii) notification of a personal data breach to the supervisory authority, (iii) information to the data subject about a personal data breach, (iv) data protection impact assessment and (v) prior consultation. Unless the Parties agree otherwise, such assistance referred to in this section shall not entitle the Processor to any special compensation.

9.3 The Processor shall, without undue delay, notify the Controller if the Processor is contacted by a supervisory authority or any other third party for the purpose of accessing personal data that the Processor, or where applicable a sub-processor, has in its possession, unless prohibited to do so by applicable legislation.

10. ENGAGING SUB-PROCESSORS

10.1 The Processor is hereby given prior general authorization for the engagement of sub-processors through which personal data may be transferred in order for the Processor to be able to fulfil its obligations pursuant to the Main Agreement. The Processor shall notify the Controller of any plans to employ new sub-processors or to replace any sub-processor so that the Controller has the opportunity to object to such changes.

10.2 If the Controller has given the Processor a general written authorisation, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other processors, thereby giving the Controller the opportunity to object to such changes.

10.3 If the Processor engages a sub-processor for carrying out a specific processing activity on behalf of the Controller, the same data protection obligations as set out in the DPA shall be imposed on that sub-processor by way of a written DPA (including electronic), in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the applicable law.

10.4 On request, the Processor shall provide the Controller with a copy of parts of the Processor's contract with a sub-processor necessary to demonstrate that the Processor is in compliance with its obligations according to the DPA.

10.5 If the sub-processor fails to fulfil its obligations under applicable law or the DPA which should exist between the Processor and the sub-processor, the Processor shall remain fully liable to the Controller for the performance of the sub-processor's obligations.

10.6 The Processor shall at all times have a correct and updated record of sub-processors that have been engaged to process personal data. The record shall contain information on where (geographically) these sub-processors

are located. Furthermore, on request, the Processor shall provide the Controller with contact information of the sub-processors that process personal data. The Processor is currently engaging the sub-processors listed in Schedule 1.

11. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

11.1 The Processor shall not transfer personal data to third parties outside of the EU/EEA except for as necessary to perform the undertakings in the Main Agreement. The Processor shall only transfer personal data to countries approved by the European Commission as providing an adequate level of protection for personal data, or otherwise if the transfer is made in conformity with European Commission approved Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation 2016/679 of the European Parliament and of the Council in combination with necessary technical and organisational security measures or any other of the legal bases under Chapter V GDPR.

11.2 In the event Processor receives an order from any third party for compelled disclosure of any personal data that has been transferred under this section, the Processor will, where possible and not prohibited, inform the Controller of that legal requirement prior to the processing and redirect the third party to request data directly from the Controller. Processor shall further use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with the law of the European Union or applicable member state law.

12. LIABILITY FOR DAMAGE

12.1 Each party's liability, taken together in the aggregate arising out of or related to this DPA, shall be subject to the limitation of liability agreed between the Parties in the Main Agreement. Such limitations shall however not apply if the damage has been caused by the incorrect implementation of the Services by the Controller or by an instruction given by the Controller, in such an event, the Controller will be liable for such damage.

13. COMPENSATION

Compensation due under this DPA and any additional costs the Processor incurs in order to fulfil its obligations under this DPA are governed by the Main Agreement.

14. NOTICES

14.1 All messages, notices and alike under this DPA shall be in writing and sent to the other Party as set out in the Main Agreement.

15. TERM

15.1 This DPA enters into force when signed by both Parties and shall remain in force until the Processor has ended its processing of personal data on behalf of the Controller or this DPA has been superseded by another data processing agreement.

15.2 When the Processor has ended its provision of services relating to processing to the Controller, the Processor shall, at the choice of the Controller, delete or return in a standardized format all the personal data to the Controller and delete existing copies unless Union or Member state law requires storage of the personal data. The Processor shall ensure that any potential sub-processors do the same.

16. GOVERNING LAW AND DISPUTE RESOLUTION

16.1 This DPA shall be governed by Swedish Law, with the exemptions of the rules of conflict of laws.

16.2 Any dispute, controversy or claim arising out of or in connection with this DPA or the breach, termination or invalidity thereof, shall be finally settled in accordance with the regulations in the Main Agreement.

Schedule 1 - Instructions

These instructions from the Controller forms an integrated part of the DPA. The Processor shall at all times comply with these instructions when processing personal data, unless otherwise is explicitly stated in the DPA.

By signing the DPA, the Processor has confirmed the meaning of these instructions. No changes or amendments to these instructions shall be valid unless made in writing by the Controller.

Purposes of processing
The purpose of the processing is to provide the Controller's website data subjects with a relevant experience of the Controllers services and to provide agreed services.

Types of processing
Through the collection, organisation, structuring, storing, retrieval, erasure and analysis, the Processor will enhance the Controllers website(s) with more relevant showing of products based upon the data subjects, activities on the website in question.

Categories of data subjects
Visitors of Controller's website(s).

Categories of personal data
Views on products, purchases of products, clicks on products, add-to-carts on products, search phrases, all stored on a pseudonymized customer number.

Sub-processors and Location of processing operations

- Amazon Web Services EMEA SARL (AWS), 38 avenue John F. Kennedy, L-1855 Luxembourg. Cloud hosting provider (main processing location is Germany (Frankfurt), Sweden (Stockholm) or Ireland (Dublin).
- Iver Syd AB, Örja Skolväg 15, tel no.: +46 418 44 88 40. Used for hosting of dev/ops environment and will only be applicable as sub-processor if Controller chooses to process personal data in dev/ops environment.
- Salesforce SFDC Ireland Limited, Route de la Longeraie 9, Morges, 1110, Switzerland (used for customer support – meaning that personal data will only be processed by sub-processor if Controller enters personal data into a support ticket)

Duration of processing
The default duration of processing is set to twelve (12) months.

Technical and organizational security measures

General security measures
Measures which generally prevent unauthorized processing of personal data.

- Security standard – the Processor shall work with technical and organizational security according to the self-assessment model published by the **Cloud Security Alliance** or a replacing standard of similar quality.
- Encryption of traffic data – all external data transfers to and from the Processor are protected using encryption following the current established practice.

- Separation of data – customer data is separated by using logical separation or logical identifiers, tagging information to clearly identify ownership and ensuring that customer data can only be accessed by that customer.
- Regular security updates and patches for all systems.
- The Processor permit tenants to perform independent vulnerability assessments at request within the limitations of the Processor's general testing guidelines.

Physical Access control

Measures which prevent unauthorized persons from gaining access to data processing systems which process personal data.

- Access to systems and personal data is restricted only to those who need access to provide the Processor to the customers on a need-to-know-basis.
- User authentication to protect access to data processing systems.
- Secure password policies for all systems and workstations.
- The Processor monitor and log privileged access (e.g., administrator level) to information security management systems.

Organizational measures

Measures which ensure secure routines and practices within the organization.

- Risk management – the Processor shall have documented processes and routines for handling risks within its operations. The Processor shall periodically assess the risk related to information systems and processing, storing and transmitting information.
- Change control – the Processor maintains a structured change management process to ensure that changes are reviewed and tested.
- Secure testing – the Processor maintains separate production and testing environments.
- Data protection officer – the Processor maintains a data protection officer who has appropriate security competence and who has an overall responsibility for implementing the security measures and who will be the contact persons for customer's security staff.
- Security is the responsibility of everyone who works for the Processor and all employees are trained to identify security risks and take action to prevent any such.
- The Processor have a documented security incident response plan, as well as well-established policies and procedures to adequately support services operations' roles.

Data breach management

Measures which ensure secure and proper management in the event of any data breaches.

- The Processor shall have established procedures for data breach management.
- The Processor shall inform the applicable customer about any data breaches as soon as possible in accordance with the data processing agreement.
- All reporting of personal data breaches shall be treated as confidential information.
- Reporting shall include available information necessary to report to the supervising authority.

Business continuity management

Measures which ensure the on-going operation of the services.

- The Processor shall identify business continuity risks and take necessary actions to control and mitigate such risks.
- The Processor shall have documented processes and routines for handling business continuity.

- Information security shall be embedded into the business continuity plans.
- The efficiency of the Processor business continuity management and compliance with availability requirements shall be periodically evaluated.

Additional Instructions for Add-Ons and integration services

Please note that if you utilize Add-On Services and/or integrations to third party integrations additional processing will be performed. For Add-On Services such will either be described in your Add-On supplement or provided upon request by your customer contact. For integrations the applicable processing will be the processing you instruct us to perform. For the integration with Voyado Lund AB's affiliate Voyado AB and the service "Voyado Engage", the following processing is applicable:

- Cross platform identification and soft login. The purpose with the processing is to cross-identify a customer between Voyado AB and Voyado Lund AB. End-customer keys will be processed and stored by Voyado AB and Voyado Lund AB.
- Audience controlled promotions. The purpose with the processing is to enable a more personalized experience for the end-customer on the controller's web site by utilizing segments build in Voyado AB and used by Voyado Lund AB. End-customer keys will be requested, returned, and stored.
- Intent data in Voyado Engage. The purpose of the processing is to enable a more personalized experience for the end-customer by making use of intent data from Voyado Elevate in Voyado Engage. End-customer keys and intent data associated with end-customer keys, such as, occasions, product categories, favorite brand and frequency/activity will be processed by Voyado Engage.