2026-02-24

Data Processing Agreement

1. Background and purpose

1.1 The Parties have entered into an agreement governing the provision of the Product(s), as applicable, to Customer and Customer's use thereof. The provision of the Product(s) entails processing of personal data by Supplier, the data processor, on behalf of Customer, the data controller, as further specified in Schedule A and/or Schedule B (as applicable) with data controller's instructions and details of processing, and the Parties have therefore entered into this DPA.

1.2 This DPA supplements the General Terms and sets out the rights and obligations of the data controller and the data processor when processing personal data on behalf of the data controller. The purpose of this DPA is to ensure the Parties' compliance with Article 28 (3) of 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 (the "**GDPR**"). This DPA shall not exempt the Customer from any of its obligations in its capacity as data controller pursuant to applicable legislation.

2. Definitions

In addition to the defined terms below and any terms defined in the Agreement, terms used in this DPA, *e.g.* 'data subject', 'personal data', 'processing', 'controller', 'processor', 'personal data breach' etc., shall be construed in accordance with the meaning given to them in the GDPR.

"**Data Protection Laws**" means the GDPR, supplementary national legislation and binding directions of the Swedish Authority for Privacy Protection or other competent body.

"**EU-U.S. DPF**" means the EU-US Data Privacy Framework self-certification program operated by the US Department of Commerce.

"**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.

"**Standard Contractual Clauses**" means 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.

3. The rights and obligations of the data controller

3.1 The data controller is responsible for ensuring that the processing of personal data by the data processor in accordance with Schedule A and/or Schedule B (as applicable) with data controller's instructions and details of processing complies with Data Protection Laws. The data controller's responsibilities include, but are not limited to, ensuring that the processing of personal

data under this DPA has a valid legal basis, informing data subjects of the processing carried out in accordance with this DPA, safeguarding the rights of the data subjects under the GDPR and, if required, obtaining the data subject's consent.

3.2 The data controller has the right and obligation to determine the purposes and means of the processing of personal data carried out for the provision of the Product(s) under the Agreement.

4. Processing of personal data

4.1 The data processor may process personal data for purposes necessary for the performance of its obligations under the Agreement, and undertakes to process personal data only in accordance with the Agreement, this DPA, and the data controller's documented instructions as specified in Schedule A and/or Schedule B (as applicable) with data controller's instructions and details of processing, unless otherwise provided by Data Protection Laws.

4.2 The data processor shall inform the data controller if instructions given by the data controller, in the opinion of the data processor, are insufficient or violate Data Protection Laws and await further instructions from the data controller.

4.3 If the processing is not based on the data controller's documented instructions, but instead on mandatory provisions pursuant to European Union or national law to which the data processor is subject, the data processor shall notify the data controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

5. Support for the data controller

5.1 The data processor shall upon request assist the data controller in ensuring compliance with its obligations pursuant to Articles 32–36 of the GDPR, considering the type of processing and the information available to the data processor.

5.2 The data processor shall, upon request, taking into account the nature of the processing, assist the data controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the data controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.

5.3 If a third party (*e.g.* a data subject, an authority or other party) contacts the data processor with a request pursuant to Chapter III of the GDPR or a request regarding the processing of personal data under this DPA in general, the data processor shall forward said request to the data controller without undue delay.

5.4 The data processor is not entitled to represent the data controller vis-à-vis a third party in matters involving the processing of personal data, unless the data controller has expressly consented to this. However, this shall not prevent the data processor from fulfilling its obligations in the form of cooperating with a supervisory authority pursuant to Article 31 of the GDPR. The data processor shall notify the data controller of such cooperation without delay, unless prohibited from doing so by applicable legislation.

6. Sub-processors

6.1 For the performance of the Agreement, the data processor engages sub-processors for certain tasks, such as IT operation, communications, data collection, etc. The data processor is

hereby given prior general authorization for the engagement of sub-processors through which personal data may be transferred in order for the data processor to be able to fulfil its obligations pursuant to the Agreement. The sub-processors engaged at each point in time are listed here (Voyado Engage) and/or here (Voyado Elevate).

6.2 The data processor shall notify the data controller of any plans to engage new sub-processors or to replace any sub-processor, thereby giving the data controller the opportunity to object to such changes.

6.3 The data processor is responsible for ensuring that the sub-processor, through a written agreement or other legal act pursuant to Data Protection Laws, is bound to data protection obligations equivalent to those laid down in this DPA, and for ensuring that the sub-processor provides sufficient guarantees that it will implement appropriate technical and organizational measures in such a manner that the data processing will meet the requirements of Data Protection Laws. Where a sub-processor fails to fulfil its data protection obligations, the data processor shall remain fully liable to the data controller for the performance of the sub-processor's obligations.

7. Transfer of personal data to third countries

7.1 Data processor shall not transfer personal data to third parties located in a country outside of the EU/EEA except for as necessary to perform the undertakings in the Agreement. The data processor may only transfer personal data to a recipient in a country outside the EU/EEA if such country is approved by the European Commission as providing an adequate level of protection for personal data (including the US, provided that the recipient is participating in the EU-U.S Data Privacy Framework), or otherwise if the transfer is made in conformity with the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to the GDPR in combination with necessary technical and organizational security measures, or any other of the allowed transfer mechanisms under Chapter V of the GDPR.

7.2 In the event data processor receives an order from any third party for compelled disclosure of any personal data that has been transferred under this section, the data processor will, where possible and not prohibited, inform the data controller of that legal requirement prior to the processing and redirect the third party to request data directly from the data controller. The data 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 European Union law or applicable member state law.

8. Confidentiality

8.1 The data processor undertakes to limit access to personal data to those individuals who require such access to perform the services.

8.2 The data processor shall ensure that any persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and will process the personal data solely in accordance with the data controller's instructions, unless otherwise provided by applicable law pursuant to Section 4.3.

9. Security

The data processor undertakes to adopt all measures which are required pursuant to Article 32 of the GDPR, stipulating that the data processor shall implement appropriate technical and

organizational measures to ensure a level of security appropriate to the risk, taking into account in particular the risks that are presented by the processing, the sensitivity of the personal data concerned, available technical options, and the costs of implementing the measures. The technical and organizational measures which shall be undertaken by the data processor are detailed in Schedule A and/or Schedule B (as applicable) with data controller's instructions and details of processing.

10. Notification of personal data breaches

The data processor shall, without undue delay, notify the data controller after becoming aware of a personal data breach involving personal data processed by the data processor pursuant to the Agreement. The data processor shall assist the data controller by providing the information necessary for the fulfilment of its obligation to notify the personal data breach to the competent supervisory authority and, when applicable, its obligation to communicate the personal data breach to the affected data subjects, taking into account the nature of processing and information available to the data processor.

11. Audit and inspection

11.1 The data controller or an independent third party appointed by the data controller (however not a competitor to data processor) is, subject to reasonable prior notice and compliance with data processor's technical and organizational security measures, entitled to perform an audit for the sole purpose of ensuring compliance with this DPA. Such audit is restricted to information necessary for demonstrating compliance with the obligations under this DPA and the auditor is required to enter into a non-disclosure agreement directly with the data processor prior to disclosure of such information. Audits shall be conducted during the data processor's ordinary business hours and shall not cause any unreasonable disruption to the data processor's business activities. The data processor shall provide the data controller with reasonable assistance and documentation as required to perform such an audit. Audits shall be carried out at the data controller's cost and expense.

11.2 Upon Customer's request and subject to applicable confidentiality obligations, Supplier shall provide copies of any certifications, audit report summaries and/or other relevant documentation it holds, to the extent such documentation is generally made available to its Customers. If the requested audit scope is addressed in an ISO 27001 certification or similar third-party audit report performed within the twelve (12) months preceding Customer's audit request, and Supplier confirms there are no known material changes in the audited controls, Customer agrees to accept such certification or audit report in lieu of conducting its own audit of the controls covered thereby.

11.3 The data processor shall be required to provide supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities subject to presentation of appropriate identification.

12. Liability

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 Agreement. Such limitations shall however not apply if the damage has been caused by the incorrect implementation of the Product(s) by the data controller or by an instruction given by the data controller, in such an event, the data controller will be fully liable for such damage.

13. Term and termination of DPA

13.1 This DPA shall enter into effect upon the date of signing of the Agreement by both Parties. The DPA terminates when the Agreement is terminated or when the data processor otherwise no longer processes personal data on behalf of the data controller.

13.2 Upon termination of the DPA, the data processor shall permanently delete or return all personal data to the data controller, depending on what the data controller chooses, unless the data processor is required to retain the personal data pursuant to applicable law. If the data controller has not informed the data processor of its choice within one (1) month from the termination of the DPA, the data processor shall permanently delete all personal data in accordance with its retention policy.

14. Miscellaneous

14.1 This DPA forms an integral part of the Agreement between Supplier and Customer. In case of conflicting provisions in the Agreement, the DPA shall prevail.

14.2 Should any provision of this DPA be or become invalid, or contain a gap, the remaining provisions shall remain unaffected. Supplier and Customer undertake to replace any invalid provision with legally valid provisions which come the closest to the intent of the invalid provision, and respectively, fill out the gap.

Schedule A – Data controller's instructions and details of processing for "Voyado Engage"

1. Nature and purpose of the processing

This Schedule applies to the provision of the Product "Voyado Engage". Customer's use of any Components and/or integrations to Third Party Services entails additional processing as further described in the Data processing specifications (see Section 7 below). The exact processing may also depend on the settings configured by Customer.

The purpose of the processing is to provide the Product under the Agreement and to continuously develop and improve the Product. The data processor may only process personal data for these purposes.

Personal data will mainly be imported to the Product by the data controller but may also, in certain cases, be imported from external sources, such as external service providers, where agreed in the Agreement, *e.g*. for the purpose of enriching and updating personal data. Personal data may also be imported directly from data subjects through their use of the Product.

The personal data in the Product will primarily be stored and used for segmentation and targeted campaign execution (mainly through e-mail and text message distribution). The campaign management system will generate personal data through its feedback loop on bounced e-mails, opened e-mails, click-throughs and similar monitoring activities.

Customer's use of any AI Functionality entails additional processing of personal data by Supplier in accordance with the applicable Data processing specifications in Help Center. If Customer elects to use such AI-powered functionalities, personal data may be used for, *e.g.*, AI assisted insights and strategy, AI assisted targeting and AI assisted content generation. The AI functionalities are designed to support the Authorised User's analysis, targeting, and content creation, and are not intended for automated decision-making within the meaning of Article 22 of the GDPR.

2. Relevant data subjects and personal data

Processing involves these categories of data subjects:

- Members, customers, prospective customers or other individuals registered in the data controller's applicable systems

The data processor shall process the following personal data:

- Name
- Address
- Date of birth
- Personal identification number
- Gender

- E-mail address
- Telephone number
- Applicable segmentation
- Information regarding previous purchases
- Activities by the data subjects, such as opening e-mails, clicks on links included in the e-mails, purchases, participation in challenges and similar, as well as data generated as a result of such activities or interactions (*e.g.* loyalty points, progress status, rewards etc.)
- Other personal information that is stored in the Product

Sensitive personal data under Article 9 of the GDPR and other personal data that may be regarded as sensitive from an integrity perspective may not be processed in the Product and the data controller shall not import or store such data unless these instructions are explicitly amended in writing and signed by both Parties.

3. The duration of the processing

Personal data will be processed for the term of the Agreement. The Customer shall, as the data controller, set the retention period for Contacts and associated personal data. More information on data retention is found in the Help Center article "Data Storage in Engage".

4. Technical and organizational security measures

Supplier has implemented the following technical and organizational measures (including an ISO 27001 certification) to ensure a level of security of personal data appropriate to the risk, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons:

4.1 General security measures

Measures which generally prevent unauthorized processing of personal data.

- Security standard – data processor shall maintain and operate an Information Security Management System (ISMS) certified under ISO/IEC 27001 (or equivalent), and shall apply technical and organizational security measures in accordance with this framework.
- Encryption of personal data – Data transfers to and from the data processor are protected using encryption following the current established practice. At rest, data is encrypted where technically feasible, at least using disk-level encryption.
- 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 and independent vulnerability- and penetration testing and regular security updates and patches.

4.2 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 deliver the Product to the customers on a need-to-know-basis.
- User authentication to protect access to data processing systems.
- Secure password policies. Employee workstations are encrypted using full-disk encryption and protected with strong passwords.

4.3 Organizational measures

Measures which ensure secure routines and practices within the organization.

- Risk management – data processor shall have documented processes and routines for handling risks within its operations. Data processor shall periodically assess the risk related to information systems and processing, storing and transmitting information.
- Change control – data processor maintains a structed change management process to ensure that changes are reviewed and tested before being deployed to production. Roll-back measures are in place in the event of any unintended behaviour.
- Secure testing – the data processor maintains separate production and testing environments.
- Data protection officer – the data 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 data processor and all employees are trained to identify security risks and take action to prevent any such.

4.4 Data breach management

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

- Data processor shall have established procedures for data breach management.
- Data 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.

4.5 Business continuity management

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

- Data processor shall identify business continuity risks and take necessary actions to control and mitigate such risks.
- Data 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 data processor's business continuity management and compliance with availability requirements shall be periodically evaluated.

4.6 Certifications

Supplier currently maintains the following certifications:

- ISO 27001

More information available at the Voyado Trust Center (http://trust.voyado.com/).

5. Data controller's obligations

Data controller shall store any user credentials in a safe manner and not provide access to any unauthorized individual. Data controller shall have routines and policies for use of the Product in a secure manner and shall educate its personnel on the acceptable use of the Product. The data controller must have policies for which personal data may be stored in the Product and for how long such data shall be retained.

The data controller is reminded of its obligations under the GDPR to only process personal data in accordance with Data Protection Laws and to maintain a high security for personal data by technical and organizational security measures. The data controller therefore acknowledges that it may for example not transfer any files containing personal data in unencrypted e-mails to the data processor and that the data controller may not submit any sensitive personal data (unless expressly agreed otherwise herein), or any other personal data not included in this instruction, such as bank account information, credit card information etc. to the data processor, for example when requesting support from the data processor nor in any other event. The data controller is further recommended to work actively with suitable data protection activities.

6. Sub-processors and third-country transfers

Data processor shall be authorized to transfer personal data to third countries for the limited purposes allowed under this DPA. Descriptions of the relevant data transfers to applicable sub-processors are described here. Data processor and data controller shall strive towards minimizing all third-country transfers in all situations.

7. Additional instructions for Components and integrations

Customer's use of any Components and/or integrations to Third Party Services entails additional processing of personal data by Supplier in accordance with the applicable Data processing specifications in Help Center.

Schedule B – Data controller's instructions and details of processing for "Voyado Elevate"

1. Nature and purpose of the processing

This schedule applies for the provision of the Product "Voyado Elevate". Please note that the exact processing will depend on the Component(s) and integrations utilized (see Section 7 below) and the settings made by Customer. The purpose of the processing is to deliver the Product under the Agreement and to continuously develop and enhance the functionality of the Product. The data processor may only process personal data for this purpose.

Through the collection, organization, structuring, storing, retrieval, erasure and analysis, the data processor will enhance the data controller's website(s) with more relevant showing of products based on the data subjects' activities on the website(s) in question.

2. Relevant data subjects and personal data

Processing involves these categories of data subjects:

- Visitors of data controller's website(s).

The data processor shall process the following personal data:

- Views on products, purchases of products, clicks on products, add-to-carts on products, search phrases, and session key, all stored on a pseudonymized customer key.
- IP-address and user agent.

3. The duration of the processing

The default duration of processing is set to twelve (12) months. More information on data retention is found in the "Data storage in Elevate" section here.

4. Technical and organizational security measures

Supplier has implemented the following technical and organizational measures (including an ISO 27001 certification) to ensure a level of security of personal data appropriate to the risk, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons:

4.1 General security measures

Measures which generally prevent unauthorized processing of personal data.

- Security standard – data processor shall maintain and operate an Information Security Management System (ISMS) certified under ISO/IEC 27001 (or equivalent), and shall apply technical and organizational security measures in accordance with this framework.
- 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.

- Data processor permits tenants to perform independent vulnerability assessments at request within the limitations of the processor's general testing guidelines.

4.2 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 deliver the Product 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.

- Data processor monitor and log privileged access (e.g., administrator level) to information security management systems.

4.3 Organizational measures

Measures which ensure secure routines and practices within the organization.

- Risk management – data processor shall have documented processes and routines for handling risks within its operations. Data processor shall periodically assess the risk related to information systems and processing, storing and transmitting information.

- Change control – data processor maintains a structured change management process to ensure that changes are reviewed and tested.

- Secure testing – data processor maintains separate production and testing environments.

- Data protection officer – data 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 data processor and all employees are trained to identify security risks and take action to prevent any such.

- Data processor has a documented security incident response plan, as well as well-established policies and procedures to adequately support services operations' roles.

4.4 Data breach management

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

- Data processor shall have established procedures for data breach management.
- Data 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.

4.5 Business continuity management

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

- Data processor shall identify business continuity risks and take necessary actions to control and mitigate such risks.
- Data 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 data processor business continuity management and compliance with availability requirements shall be periodically evaluated.

4.6 Certifications

Supplier currently maintains the following certifications:

- ISO 27001

More information available at the Voyado Trust Center (http://trust.voyado.com/).

5. Sub-processors and third-country transfers

Data processor shall be authorized to transfer personal data to third countries for the limited purposes allowed under this DPA. Descriptions of the relevant data transfers to applicable sub-processors are described here. Data processor and data controller shall strive towards minimizing all third-country transfers in all situations.

6. Additional instructions for Components and integrations

Customer's use of any Components and/or integrations to Third Party Services entails additional processing of personal data by Supplier in accordance with the applicable Data processing specifications in Help Center.

* * *