Data Processing Agreement 2021-09-14

1. Definitions

The definitions specified in the Regulation (EU) 2016/679 of the European Parliament and of the Council ("General Data Protection Regulation") shall apply to the application of this data processing agreement, the ("**DPA**") in addition to the defined terms below and any terms defined in the Service Agreement.

- The "Service Agreement" is defined as the License Agreement entered into between the Parties and to which this DPA forms an appendix.
- "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.

2. General

The Parties have entered into a Service Agreement whereby Supplier, the data processor undertakes to provide IT services on behalf of the Customer, the data controller. For the performance of the services pursuant to the Service Agreement, the data processor will process personal data as well as other information on behalf of the data controller, including information on the data controller's customers and/or contacts for the purposes of customer service, communication and marketing. Further details on applicable processing activities, the nature of the personal data, retention periods etc. are specified in Schedule A – Data Controller's instructions and details of processing.

This DPA set out the rights and obligations of the data controller and the data processor when processing personal data on behalf of the Customer and the DPA have been designed to ensure the parties' compliance with Article 28 (3) of the GDPR. This DPA shall not exempt the Customer from any obligations the data controller is subject to pursuant to the GDPR or other applicable legislation.

3. The rights and obligations of the data controller

The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR and Applicable law.

The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data within the framework of the Services in the Service Agreement.

4. The data processor acts according to instructions

The data processor undertakes only to process personal data pursuant to the Service Agreement, Applicable Law and directions and general advice from the Swedish Data Protection Authority, or as otherwise emanates from European law or national Swedish law, as

well as from the data controller's documented instructions as specified in Schedule A. The data processor shall inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or Applicable law and await the data controllers further instructions. If the processing is not based on the data controller's documented instructions, but instead on provisions pursuant to European or national Swedish law to which the data processor is subject, the data processor shall notify the data controller of this legal requirement before the data are processed, provided that such information is not forbidden, referring to a vital public interest pursuant to this law.

If the data processor assesses that any instructions are insufficient, the data processor shall obtain additional instructions from the data controller. At the request of the data controller, the data processor shall provide assistance in fulfilling the obligations deriving from the performance of so-called impact assessments concerning data protection and advance consultation.

The specifications of this DPA notwithstanding, the data processor is entitled to process personal data to fulfil its obligations pursuant to Applicable Law to which the data processor is subject. For such processing, the data processor shall notify the data controller of this legal requirement before the data are processed, provided that such information is not forbidden, referring to a vital public interest pursuant to this law.

5. Support for the data controller

The data processor shall assist the data controller in fulfilling its obligations pursuant to Articles 32–36 of the GDPR considering the type of processing and the information to which the data processor has access.

6. Sub-processors

For the performance of the Service Agreement, the data processor engages external data 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 Service Agreement. The applicable sub-processors at each point in time are listed here. The data processor shall notify the Data controller of any plans to employ new data processors or to replace any data processor so that the data controller has the opportunity to object to such changes.

The data processor is responsible for ensuring that the sub-processor, through a written agreement or other legal act pursuant to Applicable Law, is bound to the same level of obligations in data-protection matters as laid down in this DPA and for ensuring that the sub-processor provides sufficient guarantees that it will implement appropriate technical and organizational measures so that the data processing meets the requirements of the GDPR.

7. Transfer to third countries or international organisations

Data processor shall not transfer personal data to third parties outside of the EU/EEA except for as necessary to perform the undertakings in the Service Agreement. The data 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.

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. 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 law of the European Union or applicable member state law.

8. Security and confidentiality

The Data processor undertakes to limit access to personal data to those individuals who require such access to perform the Services. The Data processor shall ensure that any persons with access to personal data have accepted that they will observe professional secrecy and that they are informed of how to process the personal data.

The data processor undertakes to adopt all measures which are required pursuant to Article 32 of the GDPR, stipulating that the data processor shall adopt appropriate technical and organizational measures to guarantee a level of security that is appropriate and proportionate to the risk and, in addition, in relation to the sensitivity of the personal data concerned, the separate risks that exist, available technical options, and the costs of implementing the measures. The technical and organisational measures which shall be undertaken by the data processor are detailed in Schedule A – Data controllers instructions and details of processing.

9. Notification of personal data breaches

In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach. The data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor shall assist with the information listed below, as available, which, pursuant to article 33 (3) GDPR shall be stated in the data controller's notification to the competent supervisory authority.

- The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data recors concerned.
- The likely consequences of the personal data breach.
- The measures taken or proposed to be taken by the data controller to address the personal data, including, where appropriate, measures to mitigate its possible adverse effects.

10. Contact with data subjects

If a third party (e.g. a data subject, an authority or other party) contacts the Data processor with a request pursuant to Articles 15–22 of the GDPR or a request for the processing of personal data in general, the Data processor shall forward said request to the Data controller without delay.

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. If possible and allowed, the data processor shall notify the data controller of such cooperation without delay, unless prohibited to do so.

11. Erasure and return of data

On termination of the provision of personal data processing services, the data processor shall either, at the data controller's request, permanently delete all personal data or return all personal data to the data controller, unless the storage of personal data is required pursuant to Applicable law.

12. Audit and inspection

The data controller or an independent third party appointed by the data controller (however not a competitor to data processor) is, subject to reasonable notice and compliance with data processors technical and organisational security measures, entitled to perform an audit for the sole purpose of ascertain compliance of this DPA. The audit is restricted to data relevant for this DPA and the auditor is required to enter into a non-disclosure agreement directly with data processor. Audits shall be done during data processor's ordinary business hours and shall not cause any unreasonable disruption to the data processor's business activities. 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.

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.

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

14. Miscellaneous

Except as expressly provided for in this DPA, any amendments shall be in writing and signed by both parties.

This DPA forms an integral part of the Service Agreement between Supplier and Customer. In case of other conflicts between other documents, the DPA will prevail.

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 the invalid

provision with legally valid provisions which come the closest to the interest of the invalid provision, respectively, fills out the gap.

15. Term of DPA

This DPA shall enter into effect in connection with the signing of the Service Agreement by the parties. The DPA terminates when the Service Agreement is terminated or when the Data processor otherwise no longer process personal data on behalf of the Data controller.

Schedule A – Data Controller's instructions and details of processing

1. Nature and purpose of the processing

The purpose of the processing is to provide the services under the Service Agreement and the data processor may only process personal data for this purpose.

Personal data will mainly be imported to the Services by the data controller but can also, in some cases, be imported from external sources like external service providers if agreed in the Service Agreement, e.g., for the purpose of enriching and updating personal data and may also be imported directly from the data subjects by use of the Services.

The personal data in the Services will primarily be stored and used for segmentation and targeted campaign execution (mainly by 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 through and similar monitoring.

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
- Authorized users of the Service

The Data Processor shall process the following Personal Data:

- Name
- Address
- Date of birth
- Personal identification number
- Gender
- E-mail address
- Telephone number
- Information regarding previous purchases
- Activities by the data subjects, such as opening of e-mails, clicks on links included in the e-mails and similar.
- Other personal information that is stored in the Services

Sensitive personal data under article 9 GDPR and other personal information which may be regarded as sensitive from an integrity perspective may not be processed in the Services and data controller is not allowed to 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 Service Agreement. The data controller shall set specific retention periods for specific and different categories of personal data.

4. Technical and organisational security measures

4.1. General security measures

Measures which generally prevent unauthorized processing of personal data.

- Security standard - Voyado shall work with technical and organisational security according to the self-assessment model published by the Cloud Security Alliance or a replacing standard of similar quality.
- Encryption of personal data – Data transfers to and from Voyado 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 provide Voyado 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 organisation.

- Risk management – Voyado shall have documented processes and routines for handling risks within its operations. Voyado shall periodically assess the risk related to information systems and processing, storing and transmitting information.
- Change control - Voyado 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 - Voyado maintains separate production and testing environments.
- Data protection officer – Voyado 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 Voyado 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.

- Voyado shall have established procedures for data breach management.
- Voyado 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 services.

- Voyado shall identify business continuity risks and take necessary actions to control and mitigate such risks.
- Voyado shall have documented processes and routines for handling business continuity.
- Information security shall be embedded into the business continuity plans.
- The efficiency of Voyado's business continuity management and compliance with availability requirements shall be periodically evaluated.

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 Services in a secure manner and shall educate its personnel on the acceptable use of the Services. The Data Controller must have policies for which Personal Data may be stored in the Services 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 Applicable law and to maintain a high security for personal data by technical and organisational 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. Instructions regarding third-country transfer

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. Please note that the sub-processors detailed are only applicable for the standard services, in the event Customer utilizes Add-On Services, additional information on the applicable sub-processors for such will be provided to the Customer. Data processor and data controller shall strive towards minimising all third-country transfers in all situations.