Appendix C

Data Processing Agreement ("DPA")

1. Parties

Customer name as stated in the agreement.

hereinafter **"Customer"**

Mazepay A/S
Klostertorvet 6
DK-8000 Aarhus
Denmark

Company registration number: DK-39772388

hereinafter **"Mazepay"**

Customer and Mazepay together the "**Parties**" and individually a "**Party**".

2. Background & Purpose

2.1. This DPA to ensure that proper arrangements relating to personal data transferred from Customer to Mazepay under the Agreement between the Customer and Mazepay signed by Customer for the Mazepay Software-as-a-Service are in place.

2.2. Under the Agreement, Mazepay agrees to deliver the Services as listed in the Appendices to the Agreement and in accordance with any agreed Purchase Order(s) to be used by or delivered to Customer, any of its vessels owned or managed (under contract) by Customer.

2.3. Customer may order services and products for use by its Affiliates. If it does, the licenses granted to Customer under this Agreement will apply to such Affiliates. Customer will remain responsible for all obligations under this Agreement and for its Affiliates' compliance with this Agreement.

2.4. This Agreement is compliant with the requirements of Article 28 of the General Data Protection Regulation.

3. Definitions

"**Affiliate**" means a party which has any of the following: (i) direct or indirect ownership of fifty percent (50%) or more of the share capital or other ownership interest in any other entity; or (ii) the right to exercise fifty percent (50%) or more of the votes in any other entity; or (iii) the contractual right to designate more than half of the members of such entity's board of directors or similar executive body; or by virtue of any power conferred by the law, constitutional documents, agreements or arrangements regulating to such undertaking.

"**Applicable Law**" means all laws, orders, decrees, rules, regulations, directives, notices, or guidelines (including the requirements of any Regulatory Authority) having legal effect and as applicable to a Party in respect of its rights and/or obligations under this Agreement.

"**Data Controller**" has the meaning given to that term in Data Protection Law.

"**Data Processor**" has the meaning given to that term in Data Protection Law.

"**Data Protection Law**" means any Applicable Laws relating to data protection, the processing of personal data and privacy from time to time, including (with limitation):

- the European Union ("EU") General Data Protection Regulation 2016/679 ("GDPR")
- the Danish Data Protection Act of 2018
- the United Kingdom General Data Protection Regulation 2020 and United Kingdom Data Protection Act 2018, as amended and
- any other data privacy or data protection law or regulation that applies to the processing of Data under the Agreement

"**Data Recipient**" means the party to whom the Data is disclosed.

"**Data Subject Request**" means a written request of either party as Data Controller by or on behalf of a Data Subject to exercise any rights conferred by Data Protection Law in relation to the Data.

"**Data Subject**" means an individual natural person who is the subject of any of the Data.

"**Data**" means any data, information or record that directly or indirectly identifies a natural person or relates to an identifiable natural person, including name, address, telephone number, email address, payment card data, identification number such as social security or tax ID number, date of birth, driver's license number, medical and health-related information, and any other personally identifiable information that the Disclosing Party or any third party acting on the Data Controller's behalf processes in connection with the Purpose.

"**Disclosing Party**" means the party disclosing the Data (or on behalf of whom Data is disclosed to the Data Recipient).

"**Group**" means a Party and any affiliates of a Party.

"**Group Entity**" means Customer, or Mazepay or its respective Affiliates.

"**Legal Basis**" means in relation to either party, the legal basis for processing and/or disclosing the Data in accordance with the Data Protection Law.

"**Purpose**" means the processing of the Data to (a) an extent and in such a manner as is necessary for performance of the Agreement; (b) for the purpose of compliance with Applicable Laws; (c) for either Party's legitimate record-keeping purposes; and (d) for the purpose of enabling communications between each Party's representatives, in connection with this Agreement.

"**Security Incident**" means any breach or suspected breach of any of the Data Processor's obligations or any other unauthorised or unlawful processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or damage or access to the Data.

"**Security Risk**" means any risks or vulnerabilities that are likely to affect the integrity or effectiveness of the Security Measures referenced in Clause 5.4 (including vulnerabilities relating to any software or third-party system or network) that are known or ought reasonably to be known to the Data Processor.

"**Supervisory Authority**" means any relevant supervisory authority under Data Protection Law.

"**Third Country**" means, generally, a country or jurisdiction other than that in which the Data originated or where the disclosing Party is established.

4. Interpretation and Roles

4.1. In this Data Processing Agreement, unless the context otherwise requires, words and expressions defined in Data Protection Law shall have the same meanings in this Data Processing Agreement.

4.2. Where a "Clause" number is referenced in this Data Processing Agreement, same will be intended to refer to the corresponding clause in this Data Processing Agreement unless otherwise specifically stated to the contrary.

4.3. All capitalised terms used herein shall have the definitions given to them in this Data Processing Agreement and any other capitalised terms that are not defined in this Data Processing Agreement, will have the meanings ascribed to them in the Agreement.

5. Disclosure from Data Controller to Data Processor

5.1. Performance of the Agreement requires Customer to disclose Data to Mazepay under circumstances where Mazepay processes the disclosed Data on behalf of and at the instruction of Customer. In such cases, Mazepay is the Data Processor and Customer is the Data Controller. This Clause 5 establishes the obligations of the Parties in the context of such a Data Controller-Data Processor relationship.

5.2. Data Processor will process the Data only to the extent and in such a manner as is necessary for the **Purpose**, but subject to and in accordance with Data Controller's instructions from time to time. If Data Processor considers that any instruction from Data Controller contravenes Data Protection Law, it shall immediately notify Data Controller, giving reasonable details.

5.3. Data Processor will acquire no rights or interest in or to the Data.

5.4. In accordance with its obligations under Data Protection Law, Data Processor shall take appropriate technical and organisational security measures in processing the Data, and any additional data security measures agreed by the Parties and/or reasonably specified by Data Controller from time to time in writing and/or that are otherwise consistent with good industry practice (the "Security Measures") so as to ensure an appropriate level of security is adopted to mitigate the risks associated with the processing of such Data, including unauthorised or unlawful processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or damage or access to the Data. A description of the technical and organisational security measures implemented by Data Processor under this clause is provided in Annex II.

5.5. Data Processor will:

(a) comply with its obligations under Data Protection Law;

(b) keep such records and information in relation to the processing of the Data as are required under Data Protection Law and promptly provide all such records and information on request from Customer to demonstrate compliance with Data Protection Law in relation to the processing of the Data by the Data Processor under the Agreement (including evidence of the Security Measures);

(c) promptly make changes to those measures to ensure that those measures are sufficient to ensure Data Controller's compliance with Data Protection Law; and

(d) assist Data Controller to ensure compliance with Company's obligations under Data Protection Law in relation to the processing of the Data.

5.6. Data Processor will promptly comply with any request from Data Controller requiring Data Processor to update or otherwise amend, transfer, delete or destroy the Data.

5.7. On a general basis, if Data Processor receives any complaint, notice, data subject request, or communication which relates directly or indirectly to the processing of the Data or to either party's compliance with Data Protection Law, it will immediately notify Data Controller and will provide Data Controller with full co-operation and assistance in relation to any such complaint, notice, data subject request, or communication.

5.8. Data Processor agrees to assist Data Controller, within such timescale as may be reasonably required by Data Controller, in responding to any Data Subject Request which is received by Data Controller or the Data Processor. However, Data Processor will not acknowledge or otherwise respond to any such Data Subject Request, nor disclose any of the Data to any Data Subject or to any third party, other than upon and in accordance with Data Controller's instructions or as otherwise provided for in the Agreement.

5.9. Data Processor will ensure that access to the Data is limited to:

(a) those of its employees who need access to the Data to meet the Data Processor's obligations under the Agreement (the "**Relevant Employees**") and shall ensure that no other employees of Data Processor or third parties are given access to the Data; and

(b) such part or parts of the Data as is strictly necessary for performance of that Relevant Employee's duties.

5.10. Data Processor will ensure that Relevant Employees:

(a) only process Data to the extent permitted by Clause 5.2;

(b) are bound by appropriate obligations of confidentiality in respect of the Data and understand that the Data is confidential in nature; and

(c) receive the appropriate training in data protection procedures. Data Processor shall identify and keep records of training received by such staff and the contents of all courses.

5.11. Data Processor shall not sub-contract the performance of any of its processing obligations under the Agreement to any sub-processor (or otherwise authorise any third party to process the Data on its behalf) without the prior written consent of Data Controller (which Data Controller may give or withhold in its absolute discretion). As of the executed of the Agreement, Data Controller has authorised Data Processor's use of the sub-processors listed in Annex III. Data Processor must notify Data Controller in writing before adding or replacing a sub-processor. Such sub-processor(s) will be deemed accepted if Data Controller does not object to this sub-processor within 30 days after receiving such notice. Data Controller has the right to object to a sub-processor if there is a legitimate reason and if Data Processor is notified thereof in writing within 30 days after receiving Data Processor's notice. Data Processor has the right to cure such objection within 30 days after receiving notice. If Data Processor does not cure the objection within these 30 days, either Party may terminate the affected service with reasonable written notice.

5.12. Subject to Clause 5.11, where Data Processor engages another data processor by way of sub-contract to perform processing activities on behalf of Data Controller, Data Processor shall:

(a) be solely responsible for complying with Data Protection Law in terms of ongoing sub-contracting;

(b) ensure that the sub-contract incorporates:

(i) terms and conditions which are substantially the same or equivalent to the terms of this Data Processing Agreement; and

(ii) a right to terminate automatically on termination of the Agreement for any reason; and

(c) be liable to Company for any act or omission by such data processor which breaches the obligations of Data Processor under this Data Processing Agreement.

5.13. Data Processor shall not disclose any Data to a third party in any circumstances other than in accordance with Clause 5.12 or as expressly authorised in writing by Data Controller.

5.14. Data Processor will immediately upon becoming aware of a Security Incident take such steps as are necessary to mitigate the detrimental impact of the Security Incident.

5.15. Data Processor will promptly (and, in any event, no later than forty-eight (48) hours after becoming aware of the breach or suspected breach) inform Data Controller in writing of any Security Incident. Such notification shall contain (at a minimum):

(a) the nature of the Security Incident;

(b) the date and time of occurrence;

(c) the extent of the Data and Data Subjects affected or potentially affected;

(d) the likely consequences of any Security Incident for Data Subjects affected by it and any measures taken or proposed to be taken by the Data Processor to contain the Security Incident; and

(e) any other information that Data Controller shall require to discharge its responsibilities under Data Protection Law in relation to such Security Incident.

5.16. Data Processor will thereafter promptly:

(a) provide Data Controller with all such information as Data Controller requests in connection with a Security Incident;

(b) take such steps as Data Controller requires it to take to mitigate the detrimental effects of any such Security Incident on any of the Data Subjects and/or on Data Controller; and

(c) otherwise cooperate with Company in investigating and dealing with such Security Incident and its consequences.

5.17. Data Processor will not retain Data any longer than it is reasonably necessary, in accordance with Data Controller record retention policies, to accomplish the Purpose for which the Data was processed pursuant to the Agreement.

5.18. When the Data are no longer necessary for performance of the Agreement or promptly upon the expiration or termination of the Agreement, whichever is earlier, or at an earlier time as Data Controller requests in writing, Data Processor shall:

(a) provide to Data Controller, a copy of all or, if specified by Data Controller, any part of the Data; and

(b) destroy all, or if specified by Data Controller, any part of the Personal Data in Data Processor's possession. Data Processor shall provide a certification of destruction and a detailed report summarising the sanitised or destroyed items if requested.

5.19. In the event that any Applicable Laws do not permit Mazepay to comply with the delivery or destruction of the Data, Mazepay warrants that it will ensure the confidentiality of the Data and that it will not use or disclose any Data at or after the termination or expiration of the Agreement unless required to do so in accordance with Applicable Law or by order of Regulatory Authorities.

5.20. Data Processor will indemnify Data Controller against any losses, costs, damages, awards of compensation, any monetary penalty notices, or administrative fines for breach of Data Protection Law and/or expenses (including legal fees and expenses) suffered, incurred by Data Controller, or awarded, levied, or imposed against Data Controller, as a result of any breach by Data Process or its obligations under law or under this Data Processing Agreement.

5.21. Details of the processing activities are provided in Annex I.

6. Disclosure from Data Controller to Data Controller

6.1. Performance of the Agreement may also necessitate that the Parties disclose Data to each other under circumstances where the Data Recipient receives the disclosed Data to process according to its own purposes, including for example where necessary to facilitate communication with the other Party. In such cases, both the Data Recipient and the Disclosing Party are acting as independent Data Controllers and any sharing of the Data shall be on a Data Controller to Data Controller basis. This Clause 6 establishes the obligations of the Parties in the context of such a Data Controller-Data Controller relationship.

6.2. The Disclosing Party warrants to the other Party (the Data Recipient) that in relation to any Data disclosed, such disclosure is justified by a Legal Basis in accordance with the Data Protection Law.

6.3. The Data Recipient agrees that:

(a) it is a separate and independent Data Controller in respect of the disclosed Data that it processes under the Agreement and that the Parties are not joint Data Controllers or Data Controllers in common;

(b) it is responsible for complying with the obligations incumbent on it as a Data Controller under Data Protection Law (including responding to any Data Subject Request);

(c) unless provided for in the Agreement, it shall not use any disclosed Data in a way that is incompatible with the Data Purpose;

(d) it shall implement appropriate Security Measures, so as to ensure an appropriate level of security is adopted to mitigate the risks associated with its processing of the disclosed Data, including against unauthorised or unlawful processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or damage or access to such Data; and

(e) it shall only transfer the Data to a Third Country in accordance with the requirements of the applicable Data Protection Law.

7. Responsibilities

7.1. Nothing in this Data Processing Agreement or the Agreement relieves either Party of its own direct responsibilities and liabilities under Data Protection Law.

8. Conflict

8.1. Notwithstanding any other clause of the Agreement to the contrary, in the event of any conflict between Data Protection Law, the terms of this Data Processing Agreement, and those of the body of the Agreement (or any other Appendix thereto), the order of priority between them shall be the order as they are placed below:

(i) Data Protection Law

(ii) this Data Processing Agreement

(iii) the Agreement.

ANNEX I

Details of processing activities

Categories of Data Subjects whose personal data is transferred	☒ Current Customer Group Entity employees, officers, directors, and contract workers ☐ Former Customer Group Entity employees, officers, directors, and contract workers ☐ Family members of Customer Group Entity employees, officers, directors, and contract workers ☐ Customer Group Entity customer and third-party representatives ☒ Other: Former Customer Group Entity employees, officers, directors, and contract workers who have used Mazepay Services
Categories of personal data transferred	☒ Contact Information ☒ Identification information ☐ Employment information ☐ Financial information ☐ Background information ☒ Geolocation data ☒ Digital footprints (e.g., cookies, IP address, device identifiers, URLs, online activities, user IDs) ☐ Other:
Sensitive data transferred (if applicable)	☒ None ☐ Race and ethnic origin ☐ Religious or philosophical beliefs ☐ Political opinions ☐ Trade union memberships ☐ Biometric data used to identify an individual ☐ Genetic data ☐ Health data ☐ Data related to sexual preferences, sex life, and/ or sexual orientation
Nature of the processing	The personal data is processed in order for Mazepay to deliver the process services for spend control automisation and activities related to the long tail spend of Customer.

Purpose(s) of the data transfer and further processing	☒ To fulfil the parties 'obligations under the agreement between the Data Exporter and Data Importer and/or their related bodies corporate or affiliates entities ☒ To comply with Applicable Law ☒ For either party's legitimate record-keeping purposes ☐ To enable communications between each party's representatives in connection with the Agreements ☐ Other: **Additional relevant details or explanation**: The purpose of the data transfer ensures that Mazepay can deliver its services to the data controller including to ensure that employees of Customer can be identified and that their identifies can be verified in order to comply with Payment Service Directive 2 and the associated Regulatory Technical Standard which outlines the requirements for strong customer authentication. Further the purpose of data transfer is to manage and monitor that employees of Customer are mandated to initiate the requests flows as set out in the data processors platform by Customer. Mazepay also uses data provided by the data controller in order to support supplier onboarding processes which leads to the establishment of separate data processing agreement between the data processor and the supplier.
Period for which personal data will be retained or, if that is not possible, the criteria used to determine that period	The personal data is processed in order for Mazepay to deliver the process services for spend control automisation and activities related to the long tail spend of the data controller. The personal data is retained as long as employees are employed by Customer and subsequently up to seven years or in accordance with applicable legislation. The retention period must always comply with applicable legislation regarding payments and bookkeeping procedures.
For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing	Transfer to Mazepay takes place in order to communicate with Customer's employees, validate their identities and ensure ongoing knowledge of their use of Mazepay's platform in accordance with regulatory requirements. The duration of the processing occurs for the duration of the contractual relationship and data is retained for up to five years after termination or in accordance applicable legislation for documentation purposes. Transfers to sub-processors take place in order to support Mazepay to fulfil the process outlined. The sub-processors are required – except where Mazepay stores the data – to refrain from maintaining data as data-at-rest.

ANNEX II

Details of technical and organisational security measures implemented by Mazepay

Description of the technical and organisational measures implemented by Mazepay and subsequently the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, considering the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons. The outlined measures are implemented in accordance with applicable policies and instructions. The policies and instructions are based on industry best practice (e.g., PCI DSS, NIST, etc.)	• Measures of encryption of personal data. • Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services. • Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. • Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing. • Measures for user identification and authorisation • Measures for the protection of data during transmission (encryption of data-in-transit). • Measures for the protection of data during storage (encryption of data-at-rest). • Measures for ensuring physical security of locations at which personal data are processed. • Measures for ensuring events logging. • Measures for ensuring system configuration, including default configuration. • Measures for internal IT and IT security governance and management. • Measures for certification/assurance of processes and products. • Measures for ensuring data minimisation. • Measures for ensuring data quality. • Measures for ensuring limited data retention. • Measures for ensuring accountability. • Measures for allowing data portability and ensuring erasure.
For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to aid the controller and, for transfers from a processor to a sub-processor, to the data exporter	All transfers to communication-related sub-processors of the data relies on the data being managed as 'data-in-transit' for the specific purpose of communicating to the employees of the data controller (e.g., validation of mail address, phone number, 2-factor authentication). There is as such no planned data retention as 'data-at-rest' to avoid undue exposure due to prolonged storage.

ANNEX III

List of sub-processors

Customer has authorised the use by Mazepay of the sub-processors as set out in Appendix D of the Agreement.