Data Processing Addendum (“Addendum”)

Between:

- _____("Client“) and,

- Mainflow (meaning the legal entity with which Client has a contractual relationship according to the Terms of Service, “Mainflow” and the company behind Automait ApS, business registration number 41889969, registered in Denmark, Europe). Client and Mainflow are also referred to as a “Party” and collectively as the “Parties”.

1 Background

1.1 The Client has agreed to the Terms of Service, according to which Mainflow has agreed to provide certain services to Client (the “Services”).

1.2 When providing the Services, Mainflow may collect, process, and gain access to Personal Data of individuals on behalf of Client. From a data protection perspective, Client will be the Data Controller, and Mainflow will be the Data Processor.

1.3 This Addendum specifies the data protection obligations of the Parties under the Terms of Service. It applies to all activities performed by Mainflow in connection with the Terms of Service in which Mainflow, its staff, or a third party acting on behalf of Mainflow comes into contact with Personal Data of individuals as a Data Processor.

1.4 The Addendum is based on the provision of Article 28 of the GDPR and the definitions contained in the GDPR. Annex 1 to this Addendum specifies the jurisdiction-specific requirements for the United Kingdom. Annex 2 to this Addendum specifies the jurisdiction-specific requirements for Switzerland.

1.5 If there is a conflict between the terms of the Terms of Service and those of this Addendum, the provisions of this Addendum will prevail.

2 How to execute this Addendum

2.1 This Addendum has been pre-signed on behalf of the applicable Mainflow entity. To enter into this Addendum, Client must complete the signature block below by providing all relevant information and having this Addendum executed by an authorized representative of Client, and submit the completed and executed Addendum to info@mainflow.io.

2.2 When Mainflow receives the completed and signed Addendum as specified above, this Addendum will become a legally binding addendum to the Terms of Service.

3 Definitions

3.1 All capitalized terms used herein and not otherwise defined herein, shall have the meaning ascribed to such term in the Terms of Service.

3.2 Agreement means the Terms of Service, the Privacy Notice and this Addendum.

3.3 Client means a natural, legal person or entity who has accepted the Terms of Service with Mainflow. As set forth in the Terms of Service, Client has access to User Management at all times and can assign Authorisations to any User.

3.4 Client Data means files and any other digital data and information, which is subjected to the Services or otherwise inserted to the Mainflow system by the Client (including the specific users, products, persons, organizations, activities, pipelines, stages and deals associated with the Client).

3.5 Administrator means a User(s) of an Account which the Client has granted a special authorisation to manage the Client Account

3.6 Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

3.7 Data Processor means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

3.8 Data Protection Laws means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including but not limited to the European Union Regulation 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**"), the United Kingdom Data Protection Act of 2018 and the European Union Regulation 2016/679 as applicable by virtue of Section 3 of the European Union (withdrawal) Act of 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419) (the "**UK GDPR**"), the Swiss Federal Data Protection Act (the "**Swiss DPA**") as revised on 25 September 2020, as well as the California Consumer Privacy Act (the "**CCPA**"), in each case as amended, repealed, consolidated or replaced from time to time.

3.9 Data Subject means the individual to whom Personal Data relates.

3.10 Instructions means the written, documented instructions issued by Client to Mainflow, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deleting, making available).

3.11 Personal Data means any information relating to an identified or identifiable individual where such information is contained within Client Data and is recognised as personal data, personal information or personally identifiable information under applicable Data Protection Laws.

3.12 Personal Data Breach means 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 by Mainflow and/or its Sub-Processors in connection with the provision of the Services. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

3.13 Processing means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage,

adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms “Process”, “Processes” and “Processed” will be construed accordingly.

3.14 Sensitive Data means Personal Data that is protected under special legislation and requires unique treatment, such as “special categories of data”, “sensitive data” or other materially similar terms under applicable Data Protection Laws, which may include any of the following: (a) social security number, tax file number, passport number, driver’s license number, or similar identifier (or any portion thereof); (b) financial or credit information, including credit or debit card number; (c) genetic or health information; (d) information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biometric data for the purpose of uniquely identifying a natural person, data concerning a person’s sex life or sexual orientation, or data relating to criminal convictions and offenses; and/or (e) account passwords in unhashed form.

3.15 Sub-Processors means any Processor engaged by Mainflow to assist in fulfilling its obligations with respect to the provision of the Services under the Terms of Service.

3.16 Terms of Service means the terms available at mainflow.io.

4 Details of Processing

4.1 Purpose of Processing. Subject to Section 6.1 below, Mainflow will collect and Process Personal Data in connection with the Terms of Service only for the purpose of providing the Services. Mainflow will carry out the data Processing operations in accordance with the Terms of Service as well as any Instructions received from Client that do not conflict with the provisions of this Addendum or the Terms of Service. Copies or duplicates of any Personal Data made available hereunder may only be compiled with the approval of Client, as may be technically required for the provision of the Services, or required for lawful data retention.

4.2 Nature of Processing. Mainflow is a cloud-based, self-service, SaaS CRM (customer relationship management) platform.. Personal Data will be Processed in accordance with the Terms of Service, Privacy Notice and this Addendum, and may be subject to the following Processing activities:

- Storage and other Processing necessary to provide, maintain and improve the Services; and
- Disclosure in accordance with the Agreement (including this Addendum) and/or as compelled by applicable laws.

4.3 Controller Instructions. The Parties agree that the Terms of Service (including this Addendum), and the Privacy Notice, together with the Client’s use of the Services, constitute the Client’s complete and final Instructions to Mainflow in relation to the Processing of Personal Data, and any additional Instructions outside the scope of the Instructions shall require prior written agreement between the Parties.

4.4 Categories of Data Subjects. Mainflow will not have any knowledge or control over the categories of Data Subjects whose Personal Data the Client may elect to record or upload into the Service, except as provided in the Terms of Service. Personal Data to which Mainflow may receive access usually concerns, in particular, the following categories of Data Subjects:

- Client's directors, officers, employees, interns, trainees, agents, contractors, job applicants, customers, suppliers, subcontractors, business contacts;
- Any individuals working for third parties (e.g., Mainflow Marketplace Applications) with whom Mainflow interacts or is requested to interact in connection with the provision, operation, or maintenance of the Services on behalf of Client; and
- Any other individuals for which Client enters Personal Data or information into the Service.

4.5 Categories and Nature of Personal Data. Mainflow will not have any knowledge or control over the categories or nature of the Personal Data that Client may elect to record or upload into the Service, except as provided in the Terms of Service. The data Processing activities will generally include the following categories of Personal Data:

- Name, title, street address, email address, phone number, other contact information;
- Customer history;
- Contract billing and bank data;
- IP addresses;
- References, meeting notes; and
- Other data collected by Client and entered or uploaded into the Service by Client.

The Parties agree that the Services are not intended for the Processing of Sensitive Data, and, as such, the Parties do not anticipate the Processing of Sensitive Data.

4.6 Term. This Addendum will become effective when signed by the Parties ("Effective Date") and will run for the same term as the Terms of Service or as long as Mainflow Processes Personal Data in accordance with Section 6.11 below.

5 Client's Obligations

5.1 Compliance with Laws. Within the scope of the Agreement and in its use of the Services, Client will be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions it issues to Mainflow.

5.2 In particular, but without prejudice to the generality of the foregoing, Client acknowledges and agrees that it will be solely responsible for:

5.2.1 The accuracy, quality, and legality of Personal Data and the means by which it acquired Personal Data;

5.2.2 Complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including providing the necessary notifications and obtaining any necessary consents and authorizations (particularly for use by Client for marketing purposes);

5.2.3 Ensuring Client has the right to transfer, or provide access to, the Personal Data to Mainflow for Processing in accordance with the terms of the Agreement (including this Addendum);

5.2.4 Ensuring that Client's Instructions to Mainflow regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and

5.2.5 Complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed through the Services, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices.

5.3 Client will inform Mainflow without undue delay if Client is not able to comply with its responsibilities under this Section 5 or applicable Data Protection Laws.

6 Mainflow's Obligations

6.1 Scope of Processing. Mainflow commits to process Personal Data received within the scope of the Agreement only based on the documented Instructions from the Client. This does not apply to cases in which Mainflow is obliged to Process Personal Data under European Union or European Union Member State law to which Mainflow is subject. In such a case, Mainflow shall inform the Client of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

6.2 Confidentiality. Mainflow will ensure that persons authorized to Process Personal Data have committed themselves to confidentiality concerning Personal Data or are under an appropriate statutory obligation of confidentiality.

6.3 Qualified Personnel. Mainflow will use qualified personnel with data protection training to provide the Services.

6.4 Instructions to Personnel. Mainflow will oblige its personnel to Process Personal Data only in accordance with the Agreement, including its appendices, and any Instructions received from Client.

6.5 Notification of Violation. Mainflow will notify Client without undue delay if Mainflow is of the opinion that an Instruction received from Client is in violation of applicable Data Protection Laws and/or in violation of contractual duties under the Agreement.

6.6 Notification of Personal Data Breach. Mainflow will notify Client via email to the designated account Administrator(s) without undue delay after becoming aware of a Personal Data Breach involving Personal Data for which Client is Controller, and will assist Client in fulfilling its statutory obligations under applicable Data Protection Laws, including the GDPR, taking into account the nature of Processing and the information available to Mainflow.

6.7 Third Parties. Mainflow will keep confidential and will not make available any Personal Data received in connection with the Services to any third party except in accordance with the Terms of Service or this Addendum or as required by applicable law.

6.8 Data Subjects' Requests. Taking into account the nature of the Processing, Mainflow will support Client by implementing appropriate technical and organisational measures in fulfilling the rights of the Data Subject, as laid down in Chapter III of the GDPR, including but not limited to the correction, objection to the Processing of, deletion, and provision of Personal Data. If so instructed by Client, and if feasible, Mainflow will correct, block, delete and take other required actions with the Personal Data in accordance with Client's Instructions. If a Data Subject contacts Mainflow directly in order to have his or her data corrected, deleted, blocked or use any other rights under Chapter III of the GDPR, Mainflow will instruct the Data Subject to contact the Data Controller without undue delay after receipt of such request.

6.9 Security. Taking into account the nature of Processing and the information available to Mainflow, Mainflow will assist Client in ensuring compliance with its obligations under Article 32 of the GDPR regarding security of Processing.

6.10 Cooperation with Supervisory Authorities. Mainflow will use reasonable efforts to fully cooperate and to comply with any instructions, guidelines, and orders received from the relevant supervisory authority when such instructions, guidelines, or orders pertain to the Personal Data.

6.11 Deletion and Return of Personal Data. Upon termination of Services under the Terms of Service or, if applicable, an agreed exit phase, upon Instruction from Client, Mainflow will, in accordance with Client's Instructions either delete and/or return all Personal Data to Client unless Mainflow is under an legal obligation to retain the Personal Data. The return and/or destruction of the Personal Data transferred shall be deemed to have been achieved via Client initiating the export or deletion (as the case may be) of such Personal Data via the user interface or through Mainflow support in-app made available by Mainflow and noted as completed by Mainflow. If the Client terminates the Services but does not give any Instructions, the normal data retention period applies as described in Terms and Conditions.

6.12 Data Protection Impact Assessment and Prior Consultation. To the extent that the required information is reasonably available to Mainflow, and Client does not otherwise have access to the required information, Mainflow will provide reasonable assistance to Client with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by the GDPR or the UK GDPR (as applicable).

6.13 Records of Processing Activities. Mainflow shall keep a record of processing activities in accordance with Article 30(2) of the GDPR and make it available to the Client upon request.

7 Sub-Processors

7.1 Client grants Mainflow a general authorization in line with Article 28(2) of the GDPR to engage Sub-Processors for the purposes of providing the Services.

7.2 Client authorizes Mainflow's engagement of the Sub-Processors listed in Annex 4 to this Addendum at the time of the conclusion of this Addendum. Mainflow shall ensure that authorized Sub-Processors comply with the conditions provided for in Section 7.5 below at all times during provision of the Services.

7.3 Mainflow shall provide Client notification, prior to the appointment of any new Sub-Processor (irrespective of whether such new Sub-Processor is appointed for carrying out an existing Processing function or a new Processing function). The notification will be sent via email to the designated account Administrator(s). Upon notification regarding Mainflow's intention to engage a new Sub-Processor, Client may object to such engagement by notifying Mainflow promptly in writing via email at info@mainflow.io within ten (10) business days after receipt of Mainflow's notice.

7.4 In the event that Client objects to the use of any Sub-Processor, Mainflow will recommend to Client commercially reasonable changes in the configuration or use of the Services to avoid

Processing of Personal Data by the proposed Sub-Processor. If Mainflow is unable to assist Client with its objection regarding engagement of a Sub-Processor within a reasonable period of time which shall not exceed thirty (30) calendar days, Client may, upon written notice to Mainflow, terminate the Services. In the event of such termination, Mainflow will refund Company on a pro-rata basis any amounts paid by such Company for use of the Services.

7.5 Mainflow may only engage Sub-Processors for providing the Services under the Terms of Service, if Mainflow:

7.5.1 Communicates the name and the services to be provided by the Sub-Processor prior to engaging or replacing the Sub-Processor;

7.5.2 Has in place, or concludes prior to engaging the Sub-Processor, an agreement between Mainflow and the Sub-Processor that imposes similar, and in no way less protective, obligations than as set out in this Addendum;

7.5.3 Ensures that an adequate level of data protection for Sub-Processors that are located outside of the European Union / European Economic Area exists as per GDPR or is created (e.g., by concluding Processor-to-Processor EU Standard Contractual Clauses); and

7.5.4 Has sufficient rights against the Sub-Processor to enforce a claim, or request of the Client in the context of the Services provided by the Sub-Processor.

7.6 Mainflow shall be fully responsible for any data protection violations by the Sub-Processors in connection with the provision of Services, and shall remain fully liable to Client for any such violations in accordance with Section 11 of this Addendum.

8 Place of Data Processing and Data Transfers

8.1 Client acknowledges and agrees that Mainflow may access and Process Personal Data on a global basis as necessary to provide the Service in accordance with the Terms of Service and, in particular, that Personal Data may be transferred to and Processed by:

8.1.1 Mainflow affiliates in the United States and any other jurisdictions where Mainflow is registered. Client acknowledges that in connection with the performance of the Services, Mainflow, Inc. is a recipient of Client Data in the United States; and

8.1.2 Mainflow Sub-Processors in jurisdictions they have operations.

8.2 Wherever Personal Data is transferred outside its country of origin, each Party will ensure such transfers are made in compliance with the requirements of Data Protection Laws, especially the conditions pursuant to Chapter V of the GDPR.

8.3 Where Client is based in the European Economic Area (EEA), the Parties acknowledge that the transfer of Personal Data by Client to Mainflow will involve the transfer of data outside the EEA.

8.4 Mainflow and its entities have concluded an Intra Group Data Transfer Agreement (“IGDTA”) for any transfers of Personal Data between Mainflow entities. This way Mainflow ensures that adequate safeguards are in place for protecting Personal Data when transferred by data exporters to data importers. In particular, all Mainflow entities have entered into the EU

Standard Contractual Clauses for the transfer of Personal Data between Mainflow entities acting as data exporters and data importers, and Mainflow Inc. is a registered entity of the EU-US Data Privacy Framework.

9 Technical and Organizational Measures

Taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects, Mainflow will implement appropriate technical and organizational security measures to ensure a level of security appropriate to the risk (Article 32 of the GDPR) to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services. The technical and organizational measures implemented by Mainflow are set forth in Annex 3 to this Addendum.

10 Audits

Mainflow will grant to Client and its designees during the term of the Addendum all requested information and access rights strictly in accordance with Mainflow's security policy in order to verify Mainflow's compliance with the Terms of Service, this Addendum and with applicable Data Protection Laws upon written request by Client. Client may determine Mainflow's compliance with the agreed technical and organizational measures (see Annex 3 of this Addendum) at Mainflow's facilities upon a reasonable request in writing once a year, which is subject to confidentiality. If and to the extent Client engages third parties to conduct an audit, such third parties must be bound by confidentiality obligations similar to and no less protective than those agreed to under this Addendum. Client shall reimburse Mainflow for any time expended for any on-site audits at Mainflow's then-current professional services rates. Client shall promptly notify Mainflow and provide information about any actual or suspected non-compliance discovered during an audit.

11 Liability

For the purposes of this Addendum, the liability between "controller" and "processor" will be allocated pursuant to Article 82 of the GDPR.

12 Miscellaneous

12.1 The Addendum is governed by the law indicated as the governing law in the respective provisions of the Terms of Service.

12.2 This Addendum as well as changes and additions must be concluded by mutual agreement of the Parties recorded in signed writing.

Annex 1 – Jurisdiction Specific Requirements – United Kingdom

1. Applicability

Section 2 below applies to the extent that Mainflow's Processing of Personal Data under the Terms of Service is subject to the UK GDPR.

2. UK specific provisions

In the Addendum, reference to:

(a) "Union or Member State" in Section 6.1 shall be deemed to include the United Kingdom;
(b) "GDPR" in Sections 6.6, 6.9 and 7.1 shall be deemed to include the UK GDPR;
(c) "EU", "EEA" and "European Economic Area" in Sections 7.5.3 and 8.3 shall be deemed to include the United Kingdom;
(d) "EU Standard Contractual Clauses" shall be deemed to include the UK Addendum to the EU Commission Standard Contractual Clauses; and
(e) "GDPR" in Sections 1, 6.13, 8.2 and 9 shall be deemed to include the UK GDPR.

3. Conflict

In the event of a conflict or inconsistency between the Terms of Service (including the Addendum) and this Annex 1, the requirements of this Annex 1 shall take precedence to the extent of such conflict or inconsistency.

Annex 2 – Jurisdiction Specific Requirements – Switzerland

1. Applicability

This Annex 2 applies where Mainflow is established in Switzerland (or otherwise subject to the Swiss DPA) and processes Personal Data from the Client in Switzerland.

2. Definitions

Any references to the EU and EEA shall be read to include Switzerland. Moreover, any references to the GDPR shall be read as references to the equivalent provisions in the Swiss DPA.

3. Local Privacy Law Requirements

In addition to the provisions set out in the Addendum, the following applies for Switzerland:

- Section 6.6: Any notifications must occur as soon as possible;
- Section 8.3: The countries outside the EEA are: USA. In addition, Mainflow has concluded the EU Standard Contractual Clauses in order to ensure the transmission of the Personal Data to such third countries.
- Section 11.3: Since there is no equivalent of Article 82 GDPR under the Swiss DPA, the general provisions of the Swiss Code of Obligations on liability shall apply.

4. Conflict

In the event of a conflict or inconsistency between the requirements of the Agreement (including the Addendum) and any applicable requirements of this Annex 2, the requirements of this Annex 2 shall take precedence to the extent of the conflict or inconsistency.

Annex 3 – Technical and Organizational Measures

Description of the technical and organizational security measures implemented by Mainflow at the time of the conclusion of this Addendum according to Section 9 of the Addendum:

Mainflow is committed to protecting the Personal Data entrusted to it and has a broad corporate governance structure regarding information security in place. The program provides internal standards and best practices for personnel with access to Personal Data. The contents of the program reflect many of the security controls found within the International Organization for Standardization and the International Electrotechnical Commission's ISO/IEC 27001:2013 – Information security management systems – requirements but are also based on industry guidance and best practices.

Mainflow reserves the right to revise these Technical and Organizational Measures at any time, without notice, so long as any such revisions will not materially reduce or weaken the protection provided for Personal Data that Mainflow processes under the Agreement.

Technical and Organizational Security Measures	Evidence of Technical and Organizational Security Measures
Measures of pseudonymization and encryption of personal data	● Client Data at rest: is encrypted with 256-bit Advanced Encryption Standard (AES-256) ● Client Data in transit: Mainflow uses HTTP Strict Transport Security (HSTS) via Transport Layer Security (TLS) provided by HTTPS.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services and 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	● Incident Management ○ Mainflow operates a dedicated 24x7 on-call incident management function, ready to immediately respond to and mitigate any Client-impacting issues. ○ Mainflow has implemented a formal procedure for handling security events and incidents. When security incidents are detected, all relevant parties are notified and assembled to rapidly address the event. After resolving a security incident, a postmortem analysis is written and discussed with the relevant teams. This review also includes lessons learned from the incident and action items that will make detecting, preventing and reacting to similar events easier. ● Resilience: ○ Mainflow's business continuity plan provides guidance for successfully recovering people, business functions, and systems in the event of a business disruption (i.e., emergency or disaster).

	○ All Client Data is backed up for disaster recovery. ○ Backups are stored off-site and available for restoration in the event of data corruption or destruction. ○ Mainflow conducts periodic data recovery exercises to validate its ability to recover critical infrastructure and data to full operation in the data loss event. ● Infrastructure redundancy: ○ Mainflow utilizes reputable Infrastructure-As-A-Service providers and leverages their globally redundant services to ensure Services run reliably. ○ Mainflow benefits from dynamically scaling up or completely reprovisioning its infrastructure resources on an as-needed basis across multiple geographical areas, using the same vendor, tools, and APIs. This includes not just compute resources but storage and database resources, networking, security, and DNS. ○ Every component in Mainflow's infrastructure is designed and built for high availability. ○ Client Data will be stored on the clustered database servers.
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	● Mainflow conducts weekly scans of systems and analyzes the results for vulnerabilities, from which the IT department maintains accountability and response to minimize vulnerability risk. Critical zero-day vulnerabilities are expedited using Mainflow's incident response process. ● Penetration testing is conducted continuously by a bug bounty program and periodically by an industry-recognized offensive security company to identify external-facing vulnerabilities. ● The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance.
Measures for user identification and authorization	● Mainflow controls access to Client Data for permitted purposes and implements Identity Access Management capabilities such as Just-in-Time access and the least privilege principle. ● Strong password policy, device trust controls and multi-factor authentication where feasible. ● Identity Lifecycle Management processes in place. ● Entitlements Management to ensure an appropriate level of access. ● Automatic logoff of users that have not been used for a substantial period of time. ● Control of files, controlled and documented destruction of data.
Measures for the protection of data during transmission	● Encryption of data-in-transit and security perimeter controls (e.g., web application firewalls, cloud-native firewalls, IPS). ● Implement appropriate monitoring tools and procedures to detect and mitigate compromise attempts.

Measures for the protection of data during storage	• Network-based intrusion detection and prevention capabilities are deployed to endpoints.
	• Securing data processing equipment and personal computers;
	• Implementation of physical security controls for Mainflow premises;
	• Establishing access authorizations for employees and third parties, including the respective documentation.
	• Input Control
	  ○ Implemented protective measures for the data input into memory, as well as for the reading, alteration, and deletion of stored data
	  ○ Secrets management (e.g., passwords, encryption keys)
	• Information security awareness training occurs at employee onboarding and annually thereafter.
	• Mainflow updates its systems and software with upgrades, updates, bug fixes, new versions, and other modifications necessary to secure the Client Data.
	• Mainflow uses Endpoint Detection and Response software and keeps it up to date.
	• Client's instances are logically separated, and attempts to access data outside allowed domain boundaries are prevented and logged.

Measures for ensuring physical security of locations at which personal data are processed	• Physical Access Control. Mainflow's services and data are hosted in AWS' and Rackspace facilities and protected in accordance with their security protocols.
Measures for ensuring events logging	• See "Measures for the protection of data during storage" above.
Measures for ensuring system configuration, including default configuration	• Change and Configuration Management. Mainflow uses continuous automation for application and operating systems deployment for new releases. Integration and unit testing are done upon every build with safeguards for availability and reliability. Mainflow has a process for critical emergency fixes that can be deployed to Clients promptly. As such, Mainflow can roll out security updates as required based on criticality. • Access Control Policy and Procedures.
Measures for internal IT and IT security governance and management	• Mainflow maintains an information security risk management program to evaluate threats and vulnerabilities to ensure appropriate remediation plans are created. • Mainflow maintains a separate vendor risk management program to assess vendors' information security posture, including business continuity, security operations, data loss prevention, and third-party risk management.

	● Mainflow has implemented privacy and security-by-design mandatory reviews with the information security team into our software development lifecycle. ● All email communications on Mainflow-owned and managed devices are subject to inbound filters to identify and block or warn about known phishing and SPAM parameters. ● Phishing campaign exercises are coordinated and exercised on at least a semi-annual basis to help raise staff awareness regarding common phishing threat vectors. ● Employee policies and training in respect of each employee's access rights to Personal Data. ● Effective and measured disciplinary action against individuals who violate our Code of Conduct and other internal regulations.
Measures for ensuring data minimization	● Data collection is limited to the purposes of processing (or the data that the Client chooses to provide). ● Security measures are in place to provide only the minimum amount of access (least privilege) necessary to perform required functions. ● Upon termination of Services under the Terms of Service or, if applicable, an agreed exit phase, upon Instruction from Client, Mainflow will, in accordance with Client's Instructions, either delete and/or return all Personal Data to Client unless Mainflow is under a legal obligation to retain the Personal Data. The return and/or destruction of the Personal Data transferred shall be deemed to have been achieved via the Client initiating the export or deletion (as the case may be) of such Personal Data via the user interface or through Mainflow support in-app made available by Mainflow and noted as completed by Mainflow. If the Client terminates the Services but does not give any Instructions, the standard data retention period applies.

Measures for ensuring data quality	● Mainflow has a process that allows data subjects to exercise their privacy rights (including a right to amend and update their Personal Data), as described in Mainflow's Privacy Notice. ● See "Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services" above.
Measures for ensuring limited data retention	● See "Measures for ensuring data minimization" above.
Measures for ensuring accountability	● Mainflow has implemented data protection policies ● Mainflow follows a compliance-by-design approach ● Mainflow maintains records of processing activities ● Mainflow has appointed a data protection officer ● Mainflow adheres to relevant codes of conduct and signs up to certification schemes (see "Measures for certification/assurance of processes and products" above).
Measures for allowing data portability and ensuring erasure	● The client is able to export or delete Client Data using the self-service features of the Services as set forth in the applicable documentation for the Services.
Technical and organizational measures to be taken by the [sub]–processor to provide assistance to the controller and, for transfers from a processor to a [sub]–processor, to the Customer.	● When Mainflow engages a sub-processor under Section 7.1 (Authorization for Onward Sub-processing) of this Addendum, Mainflow and the sub-processor enter into an agreement with data protection obligations substantially similar to those contained in this Addendum. ● Each sub-processor agreement must ensure that Mainflow is able to meet its obligations to the Client. In addition to implementing technical and organizational measures to protect personal data, sub-processors must (a) notify Mainflow in the event of a Security Incident so Mainflow may notify Customer; (b) delete personal data when instructed by Mainflow in accordance with Client's instructions to Mainflow; (c) not engage additional sub-processors without Mainflow's authorization; d) not change the location where personal data is processed; or (e) process personal data in a manner which conflicts with Client's instructions to Mainflow.
Measures to ensure that data collected for different purposes can be processed separately.	● Access to data will be separated through application security for the appropriate users. ● Modules within the Mainflow App will separate which data is used for which purpose, i.e., by functionality and function. ● At the database level, data will be stored in different normalized tables, separated per module or function they support. ● Interfaces, batch processes, and reports will be designed for only specific purposes and functions, so data collected for specific purposes are processed separately.

Additional Organizational Requirements	● Mainflow maintains written processes and procedures that provide for review of and limit the scope of Personal Data disclosed by Mainflow in response to requests from public authorities. ● Mainflow maintains internal records of requests made by public authorities concerning Personal Data. ● Mainflow takes steps to limit the volume of disclosed data where possible.
Recourse mechanisms for EU individuals	● Mainflow, having its roots in Europe, has committed to dispute resolution at EU data protection authorities. We remain open to any Data Subject or Controller enforcing their rights under the EU GDPR locally in Europe based on the SCCs.

Annex 4 – List of Sub-Processors

The list of Sub-Processors used by Mainflow at the time of the conclusion of this Addendum is set out below. In case of changes to the list of Sub-Processors, the then-current list of Sub-Processors is available upon request via info@mainflow.io

Type	Processor	Entity country	Transfer mechanism	Applicable service	Type of personal data
Infrastructure	Incsub, LLC	USA	DPA + SCCs Module 3	Hosting and CDN services in Europe	All Client Data stored by Clients as defined in our Terms of Service
	Amazon SES, Inc	USA	DPA + SCCs Module 3	Transactional email services in Europe and globally, depending on Client location	All Client Data stored by Clients as defined in our Terms of Service