SUPERFLOW DATA PROCESSING ADDENDUM

Version 1.0, effektive 22.02. 2024

Superflow Software GmbH ("Superflow" or "**Processor**") and the party agreeing to these conditions ("Customer" or "**Controller**") have reached an agreement through our Terms of Service or another written or electronic document for the Services Superflow provides (the "**Main Agreement**"). This Data Processing Addendum, including its appendices (the "DPA"), is an integral part of the Main Agreement.

This DPA comes into effect and supersedes any previously applicable terms regarding its matter (including any data processing amendment, agreement, or addendum related to the Services) from the date on which the Customer signed or the parties otherwise agreed to the DPA ("**DPA Effective Date**").

If you are accepting the DPA on the Customer's behalf, you warrant that: (a) you have the full legal authority to commit the Customer to this DPA; (b) you have read and understood this DPA; and (c) you consent, on behalf of the Customer, to this DPA. If you do not possess the legal authority to commit the Customer, please refrain from accepting the DPA.

1 Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "**Agreement**" means this Data Processing Agreement and all Schedules;

1.1.2 "**Customer Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Customer pursuant to or in connection with the Main Agreement;

1.1.3 "**Contracted Processor**" means Superflow and any Subprocessor;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.8 "**Data Transfer**" means:

1.1.8.1 a transfer of Customer Personal Data from the Customer to a Contracted Processor; or

1.1.8.2 an onward transfer of Customer Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "**Services**" means the services the Customer is provided pursuant to the Main Agreement.

1.1.10 "**Subprocessor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Customer in connection with the Agreement.

1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2 Processing of Customer Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and

2.1.2 not Process Customer Personal Data other than on the relevant Customer's documented instructions, including the Main Agreement, unless Superflow has a reasonable basis to consider that the documented instructions provided are either unlawful or in violation of applicable Data Protection Laws. Should Superflow be of the opinion that the Customer's documented instructions may contravene relevant Data Protection Laws or be unlawful, Superflow will promptly notify the Customer of this concern.

2.2 The Customer instructs Processor to process Customer Personal Data.

3 Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Main Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4 Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. Superflows measures are descriped in ANNEX II.

5 Subprocessing

5.1 Superflow will only share Personal Data with sub-Processors for the explicit purpose of delivering the Services.

5.2 Superflow commits to only using sub-Processors that agree to written terms securing the protection of Personal Data, which are at least as stringent as those set out in this DPA. Superflow will be responsible for any sub-Processor's adherence to these terms and will hold them accountable for any violations.

5.3 By granting a general authorization in writing, the Customer allows Superflow to: (a) assign other members within Superflow as sub-Processors, and (b) permit Superflow to engage third-party data center operators, alongside providers of business, engineering, and customer support, as sub-Processors to facilitate the provision of the Services.

5.4 Superflow commits to keeping an updated list of sub-Processors on their website at https://www.superflow.app/sub-processors/, ensuring to include any new or changed sub-Processors at least 14 days before they process any Personal Data. Should the Customer have legitimate data protection concerns about any new or altered sub-Processor, they must voice these concerns in writing within seven (7) days after Superflow has updated the list. Both parties will attempt to resolve these concerns amicably. Should Superflow choose to proceed without the contested sub-Processor, this does not affect any rights under this section about the disputed usage of the sub-Processor. Conversely, if Superflow decides the sub-Processor is essential and cannot alleviate the Customer's concerns, the Customer may end the related Order Form before Superflow starts using this new or changed sub-Processor, specifically for the Services processing Personal Data. Failure of the Customer to object within the specified timeframe signifies consent to the use of the sub-Processor and waives any right to object.

6 Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer obligations, as reasonably understood by the Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which Superflow is subject, in which case Superflow shall to the extent permitted by Applicable Laws

inform Customer of that legal requirement before the Superflow responds to the request.

7 Personal Data Breach

7.1 Superflow shall notify Customer without undue delay upon Superflow becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Superflow shall co-operate with the Customer and take reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8 Data Protection Impact Assessment and Prior Consultation

Superflow shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Superflow of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9 Deletion or return of Customer Personal Data

9.1 Subject to this section 9 Superflow shall promptly and in any event within 31 business days of the date of cessation of any Services involving the Processing of Customer Personal Data (the “Cessation Date”), delete and procure the deletion of all copies of those Customer Personal Data.

10 Audit rights

10.1 Subject to this section 10, Superflow shall make available to the Customer on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Customer only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

10.3 The Customer is to inform Superflow with adequate prior notice if an audit or inspection as stipulated in Section 10.1 is to be carried out and must ensure (and

require its appointed auditors to ensure) that all efforts are made to prevent (or, if prevention is not possible, to minimize) any harm, injury, or disturbance to the premises, equipment, workforce, and operations of Superflow during the presence of its personnel on those premises for the purpose of such audit or inspection. Access to Superflow's premises for the purpose of conducting such audit or inspection will not be granted:

a) to any indivudual unless they can provide reasonable proof of identity and authorization;

b) outside of the regular working hours at those premises unless the audit or inspection requires immediate attention and the Customer conducting the audit has notified Superflow of this necessity before beginning attendance outside of regular hours;

c) for more than one audit or inspection regarding Superflow in a calendar year, except for additional audits or inspections which:

i) the Customer deems necessary due to actual concerns regarding Superflow's adherence to this DPA; or

ii) the Customer must perform pursuant to Data Protection Law, a Supervisory Authority, or any similar regulatory authority enforcing Data Protection Laws in any jurisdiction, provided the Customer has communicated its concerns or the specific requirement or demand in its notification to Superflow regarding the audit or inspection; or

d) to an external party conducting the audit on behalf of the Customer, unless this external auditor has signed a nondisclosure agreement approved by Superflow prior to the audit.

10.4 Should an on-site audit take place, the Customer will compensate Superflow for any time spent during such an audit, where applicable, at the professional service rates current at Superflow, to be disclosed to the Customer upon request. Prior to initiating any such on-site audit, Customer and Superflow will reach mutual agreement on the audit's scope, timing, and length, as well as the rate of reimbursement for which Customer will be accountable. All rates for reimbursement will be fair, reflecting the resources utilized by Superflow. The Customer is required to immediately notify Superflow about any discrepancies discovered during an audit.

10.5 The Customer is obligated to provide Superflow with any audit reports produced

in relation to any audit free of charge, unless forbidden by law. The Customer is permitted to use these audit reports solely for fulfilling its audit obligations under the Data Protection laws and/or verifying compliance with the provisions of this DPA. These audit reports are to be considered confidential.

10.6 Nothing within Section 10 will obligate Superflow to violate any confidentiality agreements with any of its clients, employees, or Subprocessors.

11 Data Transfer

11.1 Superflow may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Customer or by explicit settings made by the customer (or by adopting a default setting) within the service. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12 General Terms

12.1 Confidentiality

Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement (“Confidential Information”) confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

a) disclosure is required by law;

b) the relevant information is already in the public domain.

12.2 Liability and Indemnification

The liability of each party to this DPA, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, shall be subject to the limitations or exclusions of liability set out in Section 13 of the Main Agreement. Furthermore, the terms of indemnification by both Parties shall be governed by Section 13 of the Main Agreement as appropriate.

12.3 Notices

All notices and communications given under this DPA shall be made in accordance with Section 17 of the Main Agreement.

12.4 Amendment

This DPA is subject to the applicable terms for amendment set forth in the Principal Agreement.

13 Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of Austria.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Innsbruck, Austria.

ANNEX I

Data Processsing Description

This Section lays out specific details regarding the processing of Customer Personal Data as mandated by Article 28(3) of the GDPR. It further details the processing in connection with the transfer of Personal Data as detailed in Section 11 of the DPA and Schedule 4 to the DPA.

The subject matter and longevity of the processing of Customer Personal Data are delineated in the Main Agreement and this DPA.

The nature and objective of processing Customer Personal Data Superflow shall process Customer Personal Data as required to deliver the Services stipulated under the Principal Agreement, as detailed in any relevant Project Addendum or Statements of Work, and pursuant to any further directions provided by the Customer in utilizing the Services.

The types of Customer Personal Data to be processed The Customer may provide Superflow with Customer Personal Data for the delivery of Services, the scope of which is solely determined and controlled by the Customer, and may include, but is not limited to, the following categories of Personal Data:

- First and last name
- Title
- Birthday/age
- Customer ID
- Physical address(es)
- IP address(es)
- E-Mail address(es)
- Employer
- Position/Function
- Phone number
- Contact information (company name, email, phone, business address)

The categories of Data Subjects associated with the Customer Personal Data
The Customer may provide Superflow with Personal Data for the provision of Services, the scope of which is solely determined and controlled by the Customer, and may

include, but is not limited to, Personal Data pertaining to the following categories of data subjects:

- Customers, prospects, business partners and vendors of Customer (who are natural persons)
- Contact persons of Customer's prospects, customers, business partners and vendors
- Employees, advisors, agents, freelancers of Customer (who are natural persons)
- Customer's Users authorized by Customer to use the Services

List of Parties

Data exporter(s):

Customer according the Main Agreement
Role: Controller (or Processor on behalf of a third-party Controller).

Data importer(s):

Superflow Software GmbH
Eduard-Bodem-Gasse 2
6020 Innsbruck

Role: Processor (or sub-Processor)
Contact Person: Moritz Schöpfer, legal@superflow.app

ANNEX II

Technical and Organizational Security Measures

Superflow is committed to implementing and continually maintaining the security protocols outlined in this section. To ensure ongoing protection, Superflow reserves the right to update or modify these protocols, with the stipulation that any changes will not result in a material reduction of the Services' security standards.

The security measures established by Superflow encompass, but are not limited to, the following:

- A review process for all changes to production code before deployment, utilization of code analysis tools to uncover security flaws and vulnerabilities, and both automated and manual vulnerability assessments as part of the software development cycle.
- Utilization of our Subprocessors physical handling and management of servers, a setup that prohibits Superflow employees from having physical server access.
- The encryption of all data transmitted over public networks, except when otherwise requested by users, and the employment of SSH for data replication across public networks.
- Logical data segregation to ensure that customers access only their specific data, without general system access unless explicitly authorized to their data.
- Corporate policies regarding the handling of employee laptops, source code and remote access via VPN.
- Mandatory training programs for all Superflow staff, emphasizing the importance of data security responsibilities associated with their roles.
- Establishment of a security incident response strategy that outlines how customers will be informed in the event their data is compromised.
- Documented methods for authenticating customer access.
- Strict protocols regarding the use of production data, enforced by controls including auditing and technical safeguards; restriction of production data usage to essential diagnostic activities as per client requests; and clear policies dictating the permissible scenarios for such use.
- Measures to identify, assess, and counteract any reasonable foreseeable internal and external threats to the security, confidentiality, and integrity of systems or documents containing Personal Data, with ongoing evaluation and enhancement of protective measures as necessary.