

**DATA PROCESSING**  
**ADDENDUM**  
***(Version April July***  
***2023)***

This Data Processing Addendum, including its Schedules, (“DPA”) forms part of the Flowfox Agreement or other written or electronic agreement between Flowfox and Client and / or Customer (“Client”) for the purchase or use of services from Flowfox (identified either as “Services” or otherwise in the applicable agreement, and hereinafter defined as “Services”) (the “Agreement”) to reflect the Parties’ agreement with regard to the Processing of Personal Data. This DPA, including its Schedules, is incorporated into the Agreement(s) under which Flowfox has agreed to provide Services to Client.

Client enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term “Client” shall include Client and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Client pursuant to the Agreement, Flowfox may Process Personal Data on behalf of Client and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

**Instructions for execution of this DPA:**

This DPA consists of two parts: the main body of the DPA, and Schedules 1 and 2.

Except as otherwise expressly provided in the Agreement, this DPA will become legally binding upon receipt by Flowfox of the validly executed Agreement.

For the avoidance of doubt, execution of an Agreement shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses, including Schedule 2.

**Application of this DPA:**

If the Client entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement.

If the Client entity signing this DPA has executed an Order Form with Flowfox or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Form(s), and the Flowfox entity that is party to such Order Form is party to this DPA.

If the Client entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Client entity who is a party to the Agreement executes this DPA.

**DATA PROCESSING TERMS**

**1. DEFINITIONS**

“**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “**Control**,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

**“Authorized Affiliate”** means any of Client’s Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between C as not signed its own Order Form with Flowfox and is not a “Customer” as defined under this DPA.

**“CCPA”** means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations.

**“Controller”** means the entity which determines the purposes and means of the Processing of Personal Data.

**“Client”** means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Order Forms.

**“Client Data”** means data and information submitted by or for Client to the Services,

**“Data Protection Laws and Regulations”** means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement as amended from time to time.

**“Data Subject”** means the identified or identifiable person to whom Personal Data relates.

**“Europe”** means the European Union, the European Economic Area, Switzerland and the United Kingdom.

**“GDPR”** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), including as implemented or adopted under the laws of the United Kingdom.

**“Personal Data”** means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as Personal Data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Client Data.

**“Processing”** or **“Process”** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**“Processor”** means the entity which Processes Personal Data on behalf of the Controller, including as applicable any “service provider” as that term is defined by the CCPA.

**“Public Authority”** means a government agency or law enforcement authority, including judicial authorities.

**“Security and Privacy and Documentation”** means the Security and Privacy Documentation applicable to the specific Services purchased by Client, as set forth hereto on Attachment I and as otherwise may be updated from time to time or made reasonably available to Client by Flowfox.

**“Flowfox”** means the Flowfox entity which is a party to this DPA, as specified in the section “Application of this DPA” above, Flowfox GmbH, Kleiner Kielort 6-8, 20144 Hamburg Germany.

**“Flowfox Group”** means Flowfox and its Affiliates engaged in the Processing of Personal Data.

**“Standard Contractual Clauses”** means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj).

**“Sub-processor”** means any Processor engaged by Flowfox or a member of the Flowfox Group.

## 2. PROCESSING OF PERSONAL DATA

- 2.1. Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Client is a Controller or a Processor, Flowfox is a Processor and that Flowfox will engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-processors” below.
- 2.2. Client’s Processing of Personal Data.** Client shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of Flowfox as Processor (including where the Client is a Processor, by ensuring that the ultimate Controller does so). For the avoidance of doubt, Client’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data. Client specifically acknowledges and agrees that its use of the Services will not violate the rights of any Data Subject, including those that have opted-out from sales or other disclosures of Personal Data, to the extent applicable under Data Protection Laws and Regulations.
- 2.3. Flowfox’s Processing of Personal Data.** Flowfox shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Client’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement.
- 2.4. Details of the Processing.** The subject-matter of Processing of Personal Data by Flowfox is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Description of Processing/Transfer) to this DPA.

## 3. RIGHTS OF DATA SUBJECTS

Flowfox shall, to the extent legally permitted, promptly notify Client of any complaint, dispute or request it has received from a Data Subject such as a Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request". Flowfox shall not respond to a Data Subject Request itself, except that Client authorizes Flowfox to redirect the Data Subject Request as necessary to allow Client to respond directly. Taking into account the nature of the Processing, Flowfox shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Client, in its use of the Services, does not have the ability to address a Data Subject Request, Flowfox shall upon Client's request provide commercially reasonable efforts to assist Client in responding to such Data Subject Request, to the extent Flowfox is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Client shall be responsible for any costs arising from Flowfox's provision of such assistance.

#### 4. FLOWFOX PERSONNEL

- 4.1. **Confidentiality.** Flowfox shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Flowfox shall ensure that such confidentiality obligations survive the termination of the personnel engagement.
- 4.2. **Reliability.** Flowfox shall take commercially reasonable steps to ensure the reliability of any Flowfox personnel engaged in the Processing of Personal Data.
- 4.3. **Limitation of Access.** Flowfox shall ensure that Flowfox's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.
- 4.4. **Data Protection Officer.** Flowfox has appointed a data protection officer. The appointed person may be reached at [privacy@flowfox.com](mailto:privacy@flowfox.com).

#### 5. SUB-PROCESSORS

- 5.1. **Appointment of Sub-processors.** Client acknowledges and agrees that (a) Flowfox's Affiliates may be retained as Sub-processors; and (b) Flowfox and Flowfox's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Flowfox or a Flowfox Affiliate has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Client Data to the extent applicable to the nature of the Services provided by such Sub-processor.
- 5.2. **List of Current Sub-processors and Notification of New Sub-processors.** The current list of Sub-processors engaged in Processing Personal Data for the performance of each applicable Service, including a description of their processing activities and countries of location, is listed under Sub-processor Attachment II attached hereto. Client hereby consents to these Sub-processors, their locations and processing activities as it pertains to their Personal Data. In the event such Sub-processor are modified Flowfox will provide notification to Client of same before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

- 5.3. **Objection Right for New Sub-processors.** Client may object to Flowfox's use of a new Sub-processor by notifying Flowfox promptly in writing within thirty (30) days of receipt of Flowfox's notice in accordance with the mechanism set out in section.
- 5.4. If Client objects to a new Sub-processor as permitted in the preceding sentence, Flowfox will use reasonable efforts to make available to Client a change in the Services or recommend a commercially reasonable change to Client's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Client. If Flowfox is unable to make available such change within a reasonable period of time, which shall not exceed ninety (90) days, Client may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Flowfox without the use of the objected-to new Sub-processor by providing written notice to Flowfox. Flowfox will refund Client any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Client.
- 5.5. **Liability.** Flowfox shall be liable for the acts and omissions of its Sub-processors to the same extent Flowfox would be liable if performing the services of each Sub-processor directly under the terms of this DPA, unless otherwise set forth in the Agreement.

## 6. SECURITY

- 6.1. **Controls for the Protection of Client Data.** Flowfox shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Client Data), confidentiality and integrity of Client Data, as set forth in the Security and Privacy Documentation. Flowfox regularly monitors compliance with these measures. Flowfox will not materially decrease the overall security of the Services during a subscription term.
- 6.1.1. **Audit.** Flowfox shall maintain an audit program to help ensure compliance with the obligations set out in this DPA and shall make available to Client information to demonstrate compliance with the obligations set out in this DPA as set forth in this Section 6.2.

**6.1.2. Third-Party Certifications and Audits.** To the extent that Flowfox has obtained third-party certifications and audits set forth in the Security and Privacy Documentation for each applicable Service, upon Client's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Flowfox shall make available to Client (or Client's Third-Party Auditor - as defined below in section 6.2.4) information regarding Flowfox's compliance with the obligations set forth in this DPA in the form of a copy of Flowfox's then most recent third-party audits or certifications set forth in the Security and Privacy Documentation. Such third-party audits or certifications may also be shared with Client's competent supervisory authority on its request. Where Flowfox has obtained ISO 27001 certifications and SSAE 18 Service Organization Control (SOC) 2 reports for a particular Service as described in the Documentation, Flowfox agrees to maintain these certifications or standards, or appropriate and comparable successors thereof, for the duration of the Agreement. Upon request, Flowfox shall also provide a requesting Client with a report and/or confirmation of Flowfox's audits of third party Sub-processors' compliance with the data protection controls set forth in this DPA and/or a report of third party auditors' audits of third party Sub-processors that have been provided by those third-party Sub-processors to Flowfox, to the extent such reports or evidence may be shared with Client ("Third-party Sub-processor Audit Reports"). Client acknowledges that (i) Third-party Sub-processor Audit Reports shall be considered Confidential Information as well as confidential information of the third-party Sub-processor and (ii) certain third-party Sub-processors to Flowfox may require Client to execute a non-disclosure agreement with them in order to view a Third-party Sub-processor Audit Report.

**6.1.3. On-Site Audit.** Client may contact Flowfox to request an on-site audit of Flowfox's Processing activities covered by this DPA ("On-Site Audit"). An On-Site Audit may be conducted by Client either itself or through a Third-Party Auditor (as defined below in section 6.2.4) selected by Client when:

- 6.1.3.1. the information available pursuant to section "Third-Party Certifications and Audits" is not sufficient to demonstrate compliance with the obligations set out in this DPA and its Schedules;
- 6.1.3.2. Client has received a notice from Flowfox of a Client Data Incident; or
- 6.1.3.3. such an audit is required by Data Protection Laws and Regulations or by Client's competent supervisory authority.

Any On-Site Audits will be limited to Client Data Processing and storage facilities operated by Flowfox or any of Flowfox's Affiliates. Client acknowledges that Flowfox operates a multi-tenant cloud environment. Accordingly, Flowfox shall have the right to reasonably adapt the scope of any On-Site Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of other Flowfox customers' information.

**6.1.4. Reasonable Exercise of Rights.** An On-Site Audit shall be conducted by Client or its Third-Party Auditor:

- 6.1.4.1. acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Services used by Client;
- 6.1.4.2. up to one time per year with at least four (4) weeks' advance written notice. If an emergency justifies a shorter notice period, Flowfox will use good faith efforts to accommodate the On-Site Audit request; and
- 6.1.4.3. during Flowfox's normal business hours, under reasonable duration and shall not unreasonably interfere with Flowfox's day-to-day operations.

Before any On-Site Audit commences, Client and Flowfox shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for which Client shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by or on behalf of Flowfox.

**6.1.5. Third-Party Auditor.** A Third-Party Auditor means a third-party independent contractor that is not a competitor of Flowfox. An On-Site Audit can be conducted through a Third Party Auditor if:

6.1.5.1. prior to the On-Site Audit, the Third Party Auditor enters into a non-disclosure agreement containing confidentiality provisions no less protective than those set forth in the Agreement to protect Flowfox's proprietary information; and

6.1.5.2. the costs of the Third Party Auditor are at Client's expense.

6.1.5.3. **Findings.** Client must promptly provide Flowfox with information regarding any non-compliance discovered during the course of an On-Site Audit.

**6.2. Data Protection Impact Assessment.** Upon Client's request, Flowfox shall provide Client with reasonable cooperation and assistance needed to fulfil Client's obligation under Data Protection Laws and Regulations to carry out a data protection impact assessment related to Client's use of the Services, to the extent Client does not otherwise have access to the relevant information, and to the extent such information is available to Flowfox. To the extent legally permitted, Client shall be responsible for any costs arising from Flowfox's provision of such cooperation.

## **7. CLIENT DATA INCIDENT MANAGEMENT AND NOTIFICATION**

7.1. Flowfox maintains security incident management policies and procedures specified in the Security and Privacy Documentation and shall notify Client without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Data, including Personal Data, transmitted, stored or otherwise Processed by Flowfox or its Sub-processors of which Flowfox becomes aware (a "Client Data Incident"). Flowfox shall make reasonable efforts to identify the cause of such Client Data Incident and take such steps as Flowfox deems necessary and reasonable to remediate the cause of such a Client Data Incident to the extent the remediation is within Flowfox's reasonable control. The obligations herein shall not apply to incidents that are caused by Client or Client's Users.

## **8. GOVERNMENT ACCESS REQUESTS**

- 8.1. **Flowfox requirements.** In its role as a Processor, Flowfox shall maintain appropriate measures to protect Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including by implementing appropriate technical and organizational safeguards to protect Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defense and public security. If Flowfox receives a legally binding request to access Personal Data from a Public Authority, Flowfox shall, unless otherwise legally prohibited, promptly notify Client including a summary of the nature of the request. To the extent Flowfox is prohibited by law from providing such notification, Flowfox shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable Flowfox to communicate as much information as possible, as soon as possible. Further, Flowfox shall challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. Flowfox shall pursue possibilities of appeal. When challenging a request, Flowfox shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. Flowfox agrees it will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. Flowfox shall promptly notify Client if Flowfox becomes aware of any direct access by a Public Authority to Personal Data and provide information available to Flowfox in this respect, to the extent permitted by law. For the avoidance of doubt, this DPA shall not require Flowfox to pursue action or inaction that could result in civil or criminal penalty for Flowfox such as contempt of court.
- 8.2. **Sub-processors requirements.** Flowfox shall ensure that Sub-processors involved in the Processing of Personal Data are subject to the relevant commitments regarding Government Access Requests in the Standard Contractual Clauses.

## 9. RETURN AND DELETION OF CLIENT DATA

Flowfox shall return Client Data to Client and, to the extent allowed by applicable law, delete Client Data in accordance with the procedures and timeframes specified in the Security and Privacy Documentation. Until Client Data is deleted or returned, Flowfox shall continue to comply with this DPA and its Schedules. To the extent legally permitted, Client shall be responsible for any costs arising from Flowfox's deletion or return of Client Data.

## 10. AUTHORIZED AFFILIATES

- 10.1. **Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, Client enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Flowfox and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 10 and Section 11. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is a party only to this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Client.
- 10.2. **Communication.** The Client that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Flowfox under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.
- 10.3. **Rights of Authorized Affiliates.** Where an Authorized Affiliate becomes a party to this DPA with Flowfox, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

- 10.3.1. Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Flowfox directly by itself, the parties agree that (i) solely the Client that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Client that is the contracting party to the Agreement shall exercise any such rights under this DPA, not separately for each Authorized Affiliate individually, but in a combined manner for itself and all of its Authorized Affiliates together (as set forth, for example, in section 10.3.2, below).
- 10.3.2. The parties agree that the Client that is the contracting party to the Agreement shall, when carrying out an On- Site Audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Flowfox and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

## 11. LIMITATION OF LIABILITY

- 11.1. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Flowfox, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.
- 11.2. For the avoidance of doubt, Flowfox's and its Affiliates' total liability for all claims from Client and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Client and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Client and/or to any Authorized Affiliate that is a contractual party to any such DPA.

## 12. EUROPE SPECIFIC PROVISIONS

- 12.1. **Definitions.** For the purposes of this section 12 and Schedule 1 these terms shall be defined as follows:  
"EU C-to-P Transfer Clauses" means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor).  
"EU P-to-P Transfer Clauses" means Standard Contractual Clauses sections I, II III and IV (as applicable) to the extent they reference Module Three (Processor-to-Processor).
- 12.2. **GDPR.** Flowfox will Process Personal Data in accordance with the GDPR requirements directly applicable to Flowfox's provision of its Services.
- 12.3. **Client Instructions.** Flowfox shall inform Client immediately (i) if, in its opinion, an instruction from Client constitutes a breach of the GDPR and/or (ii) if Flowfox is unable to follow Client's instructions for the Processing of Personal Data.
- 12.4. **Transfer mechanisms for data transfers.** If, in the performance of the Services, Personal Data that is subject to the GDPR or any other law relating to the protection or privacy of individuals that applies in Europe is transferred out of Europe to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws and Regulations of Europe, the transfer mechanisms listed below shall apply to such transfers and can be directly enforced by the Parties to the extent such transfers are subject to the Data Protection Laws and Regulations of Europe:
- 12.4.1. **The EU C-to-P Transfer Clauses.** Where Client and/or its Authorized Affiliate is a Controller and a data exporter of Personal Data and Flowfox is a Processor and data importer in respect of that Personal Data, then the Parties shall comply with the EU C-to-P Transfer Clauses, subject to the additional terms in Section 1 of Schedule 1; and/or

12.4.2. **The EU P-to-P Transfer Clauses.** Where Client and/or its Authorized Affiliate is a Processor acting on behalf of a Controller and a data exporter of Personal Data and Flowfox is a Processor and data importer in respect of that Personal Data, the Parties shall comply with the terms of the EU P-to-P Transfer Clauses, subject to the additional terms in Sections 1 and 2 of Schedule 1.

12.5. **Impact of local laws.** As of the Effective Date, Flowfox has no reason to believe that the laws and practices in any third country of destination applicable to its Processing of the Personal Data as set forth in the Infrastructure and Sub-processors Documentation, including any requirements to disclose Personal Data or measures authorising access by a Public Authority, prevent Flowfox from fulfilling its obligations under this DPA. If Flowfox reasonably believes that any existing or future enacted or enforceable laws and practices in the third country of destination applicable to its Processing of the Personal Data ("Local Laws") prevent it from fulfilling its obligations under this DPA, it shall promptly notify Client. In such a case, Flowfox shall use reasonable efforts to make available to the affected Client a change in the Services or recommend a commercially reasonable change to Client's configuration or use of the Services to facilitate compliance with the Local Laws without unreasonably burdening Client. If Flowfox is unable to make available such change promptly, Client may terminate the applicable Order Form(s) and suspend the transfer of Personal Data in respect only to those Services which cannot be provided by Flowfox in accordance with the Local Laws by providing written notice in accordance with the "Notices" section of the Agreement. Client shall receive a refund of any prepaid fees for the period following the effective date of termination for such terminated Services.

### 13. LEGAL EFFECT

This DPA is incorporated by reference into the Agreement(s) under which Flowfox has agreed to provide Services to Client and shall become legally binding between Client and Flowfox when the Agreement is executed by both Client and Flowfox.

#### List of Schedules

Schedule 1: Transfer Mechanisms for European Data Transfers  
Schedule 2: Description of Processing/Transfer

## SCHEDULE 1 - TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

### 1. STANDARD CONTRACTUAL CLAUSES OPERATIVE PROVISIONS AND ADDITIONAL TERMS

- 1.1. For the purposes of the EU C-to-P Transfer Clauses and the EU P-to-P Transfer Clauses, Client is the data exporter and Flowfox is the data importer and the Parties agree to the following. If and to the extent an Authorized Affiliate relies on the EU C-to-P Transfer Clauses or the EU P-to-P Transfer Clauses for the transfer of Personal Data, any references to 'Client' in this Schedule, include such Authorized Affiliate. Where this Section 2 does not explicitly mention EU C-to-P Transfer Clauses or EU P-to-P Transfer Clauses it applies to both of them.
- 1.2. **Reference to the Standard Contractual Clauses.** The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in Schedule 2.
- 1.3. **Docking clause.** The option under clause 7 shall not apply.
- 1.4. **Instructions.** This DPA and the Agreement are Client's complete and final documented instructions at the time of signature of the Agreement to Flowfox for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of Clause 8.1(a), the instructions by Client to Process Personal Data are set out in section 2.3 of this DPA and include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.
- 1.5. **Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Flowfox to Client only upon Client's written request.
- 1.6. **Security of Processing.** For the purposes of clause 8.6(a), Client is solely responsible for making an independent determination as to whether the technical and organisational measures set forth in the Security and Privacy Documentation meet Client's requirements and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by Flowfox provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of clause 8.6(c), personal data breaches will be handled in accordance with Section 7 (Client Data Incident Management and Notification) of this DPA.
- 1.7. **Audits of the SCCs.** The parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Section 6.2 of this DPA.
- 1.8. **General authorisation for use of Sub-processors.** Option 2 under clause 9 shall apply. For the purposes of clause 9(a), Flowfox has Client's general authorisation to engage Sub-processors in accordance with Section 5 of this DPA. Flowfox shall make available to Client the current list of Sub-processors in accordance with Section 5.2 of this DPA. Where Flowfox enters into the EU P-to-P Transfer Clauses with a Sub-processor in connection with the provision of the Services, Client hereby grants Flowfox and Flowfox's Affiliates authority to provide a general authorisation on Controller's behalf for the engagement of sub-processors by Sub-processors engaged in the provision of the Services, as well as decision making and approval authority for the addition or replacement of any such sub-processors.
- 1.9. **Notification of New Sub-processors and Objection Right for new Sub-processors.** Pursuant to clause 9(a), Client acknowledges and expressly agrees that Flowfox may engage new Sub-processors as described in Sections 5.2 and 5.3 of this DPA. Flowfox shall inform Client of any changes to Sub-processors following the procedure provided for in Section 5.2 of this DPA.
- 1.10. **Complaints - Redress.** For the purposes of clause 11, and subject to Section 3 of this DPA, Flowfox shall inform data subjects on its website of a contact point authorised to handle complaints. Flowfox shall

inform Client if it receives a complaint by, or a dispute from, a Data Subject with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Client. Flowfox shall not otherwise have any obligation to handle the request (unless otherwise agreed with Client). The option under clause 11 shall not apply.

- 1.11. Liability.** Flowfox 's liability under clause 12(b) shall be limited to any damage caused by its Processing where Flowfox has not complied with its obligations under the GDPR specifically directed to Processors, or where it has acted outside of or contrary to lawful instructions of Client, as specified in Article 82 GDPR.
- 1.12. Supervision.** Clause 13 shall apply as follows:
  - 1.12.1.** Where Client is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Client with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.
  - 1.12.2.** Where Client is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.
  - 1.12.3.** Where Client is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, The Hamburg Commissioner for Data Protection and Freedom of Information, Ludwig-Erhard-Str. 22, 20459 Hamburg shall act as the competent supervisory authority.
  - 1.12.4.** Where Client is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as competent supervisory authority.
  - 1.12.5.** Where Client is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.
- 1.13. Notification of Government Access Requests.** For the purposes of clause 15(1)(a), Flowfox shall notify Client (only) and not the Data Subject(s) in case of government access requests. Client shall be solely responsible for promptly notifying the Data Subject as necessary.
- 1.14. Governing Law.** The governing law for the purposes of clause 17 shall be the law that is designated in the Governing Law section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of Germany or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of the United Kingdom.
- 1.15. Choice of forum and jurisdiction.** The courts under clause 12.10 shall be those designated in the Venue section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree that the courts of either (i) Germany; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the United Kingdom, shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.
- 1.16. Appendix.** The Appendix shall be completed as follows:
  - 1.16.1.** The contents of Section 1 of Schedule 2 shall form Annex I.A to the Standard Contractual Clauses
  - 1.16.2.** The contents of Sections 2 to 9 of Schedule 2 shall form Annex I.B to the Standard Contractual Clauses

**1.16.3.** The contents of Section 10 of Schedule 2 shall form Annex I.C to the Standard Contractual Clauses

**1.16.4.** The contents of Section 11 of Schedule 2 to this Exhibit shall form Annex II to the Standard Contractual Clauses.

**1.17. Data Exports from the United Kingdom and Switzerland under the Standard Contractual Clauses.**

In case of any transfers of Personal Data from the United Kingdom and/or transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland (“Swiss Data Protection Laws”), (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Data Protection Laws and Regulations of the United Kingdom (“UK Data Protection Laws”) or Swiss Data Protection Laws, as applicable; and (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Data Protection Laws or Swiss Data Protection Laws, as applicable. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

**1.18. Conflict.** The Standard Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

## **2. ADDITIONAL TERMS FOR THE EU P-TO-P TRANSFER CLAUSES**

For the purposes of the EU P-to-P Transfer Clauses (only), the Parties agree the following.

- 2.1. Instructions and notifications.** For the purposes of clause 8.1(a), Client hereby informs Flowfox that it acts as Processor under the instructions of the relevant Controller in respect of Personal Data. Client warrants that its Processing instructions as set out in the Agreement and this DPA, including its authorizations to Flowfox for the appointment of Sub-processors in accordance with this DPA, have been authorized by the relevant Controller. Client shall be solely responsible for forwarding any notifications received from Flowfox to the relevant Controller where appropriate.
- 2.2. Security of Processing.** For the purposes of clause 8.6(c) and (d), Flowfox shall provide notification of a personal data breach concerning Personal Data Processed by Flowfox to Client.
- 2.3. Documentation and Compliance.** For the purposes of clause 8.9, all enquiries from the relevant Controller shall be provided to Flowfox by Client. If Flowfox receives an enquiry directly from a Controller, it shall forward the enquiry to Client and Client shall be solely responsible for responding to any such enquiry from the relevant Controller where appropriate.
- 2.4. Data Subject Rights.** For the purposes of clause 10 and subject to Section 3 of this DPA, Flowfox shall notify Client about any request it has received directly from a Data Subject without obligation to handle it (unless otherwise agreed), but shall not notify the relevant Controller. Client shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.



## **SCHEDULE 2 - DESCRIPTION OF PROCESSING/TRANSFER**

### **1. LIST OF PARTIES**

Data exporter(s): *Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union are as set forth in the Agreement*

Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Agreement and as further described in the Documentation.

Role: For the purposes of the EU C-to-P Transfer Clauses Client and/or its Authorized Affiliate is a Controller. For the purposes of the EU P-to-P Transfer Clauses Client and/or its Authorized Affiliate is a Processor.

Data importer(s): *Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*

Name: Flowfox GmbH

Address: Kleiner Kielort 6-8, 20144 Hamburg Germany

Contact person's name, position and contact details: Arne Platzbecker, DPO, [privacy@flowfox.com](mailto:privacy@flowfox.com), HABEWI GmbH & Co. KG ,Palmaille 96, 22767 Hamburg

Activities relevant to the data transferred under these clauses: Performance of the Services pursuant to the Agreement and as further described in the Documentation.

Role: Processor

### **2. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED**

Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- a. Prospects, customers, business partners and vendors of Client (who are natural persons)
- b. Employees or contact persons of Client's prospects, customers, business partners and vendors
- c. Employees, agents, advisors, freelancers of Client (who are natural persons)
- d. Client's Users authorized by Client to use the Services

### **3. CATEGORIES OF PERSONAL DATA TRANSFERRED**

Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data

- Professional life data
- Personal life data
- Localisation data

#### **4. SENSITIVE DATA TRANSFERRED (IF APPLICABLE)**

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:*

Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The applicable security measures are described under the Security and Privacy Documentation applicable to the specific Services purchased by Client, as updated from time to time, and accessible via Flowfox's webpage at [www.flowfox.com/privacy](http://www.flowfox.com/privacy) or as otherwise made reasonably available by Flowfox.

#### **5. FREQUENCY OF THE TRANSFER**

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):*  
Continuous basis depending on the use of the Services by Client.

#### **6. NATURE OF THE PROCESSING**

The nature of the Processing is the performance of the Services pursuant to the Agreement.

#### **7. PURPOSE OF PROCESSING, THE DATA TRANSFER AND FURTHER PROCESSING**

Flowfox will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Client in its use of the Services.

#### **8. DURATION OF PROCESSING**

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:*

Subject to Section 9 of the DPA, Flowfox will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

#### **9. SUB-PROCESSOR TRANSFERS**

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:*

As per 7 above, the Sub-processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement. Subject to section 9 of this DPA, the Sub-processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

Identities of the Sub-processors used for the provision of the Services and their country of location are listed under the Sub-processor Attachment II.

#### **10. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with clause 13:*

*Confidential*

- Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.
- Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as the competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The Hamburg Commissioner for Data Protection and Freedom of Information, Ludwig-Erhard-Str. 22, 20459 Hamburg shall act as the competent supervisory authority.

- Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as the competent supervisory authority.
- Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

#### 11. TECHNICAL AND ORGANISATIONAL MEASURES

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data provided pursuant to the Services, as described in the Documentation applicable to the specific Services purchased by data exporter, and accessible via Flowfox.com or otherwise made reasonable available to data importer.

Data Importer will not materially decrease the overall security of the Services during the Term of the Agreement. Data Subject Requests shall be handled in accordance with Section 3 of the DPA.

## Standard Contractual Clauses

Controller-to-Processor

**The Client entity identified in the Agreement** (hereinafter Data **Exporter**)

And

**The Flowfox entity identified in the Agreement** (hereinafter Data **Importer**)

### **SECTION I**

#### *Clause 1*

#### **Purpose and scope**

- a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)\_for the transfer of personal data to a third country.
- b. The Parties:
  - i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)
- c. have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- d. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- e. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

#### *Clause 2*

#### **Effect and invariability of the Clauses**

- a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

#### *Clause 3*

#### **Third-party beneficiaries**

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - ii. Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
  - iii. Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  - iv. Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
  - v. Clause 13;
  - vi. Clause 15.1(c), (d) and (e);
  - vii. Clause 16(e);
  - viii. Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18. b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

<sup>1</sup> Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].

#### *Clause 4* **Interpretation**

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

#### *Clause 5* **Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### *Clause 6* **Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

*Clause 7*  
**Docking clause**

- a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**SECTION II – OBLIGATIONS OF THE PARTIES**

*Clause 8*  
**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

- a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Transparency

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.4 Accuracy

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with

this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

#### 8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

#### 8.6 Security of processing

- a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent

supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

## 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

## 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.
- v. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

## 8.9 Documentation and compliance

- a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

<sup>2</sup>The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been

incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

#### *Clause 9*

##### **Sub-processors**

- a. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days advance, thereby giving the data exporter sufficient time to be able to object and terminate the agreement with the data processor prior to the engagement of the concerned sub-processor(s), provided that the controller has substantial and documented reasons for such objection. The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object. T
- b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

#### *Clause 10*

##### **Data subject rights**

- a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

#### *Clause 11*

## **Redress**

- a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - ii. refer the dispute to the competent courts within the meaning of Clause 18.
- d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

## *Clause 12* **Liability**

- a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

<sup>3</sup>This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

*Clause 13*  
**Supervision**

- a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
- Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
- b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

*Clause 14*  
**Local laws and practices affecting compliance with the Clauses**

- a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in

- light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
- iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
  - d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
  - e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
  - f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

#### *Clause 15*

### **Obligations of the data importer in case of access by public authorities**

#### **15.1 Notification**

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant

information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## **15.2 Review of legality and data minimisation**

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

<sup>4</sup>As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

## **SECTION IV – FINAL PROVISIONS**

### *Clause 16*

#### **Clauses and termination**

- a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

- b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - ii. the data importer is in substantial or persistent breach of these Clauses; or
  - iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.  
In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.
- d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17*  
**Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

*Clause 18*  
**Choice of forum and jurisdiction**

- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The Parties agree that those shall be the courts of Germany.
- c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- d. The Parties agree to submit themselves to the jurisdiction of such courts.

## **Attachment I**

### **Data Protection Concept of Flowfox GmbH**

#### **Technical and organisational measures within the meaning of Art. 32 (1) DSGVO**

##### **Table of Contents**

1. Introduction
2. Organisational Measures
3. Security measures
  - 3.1 Confidentiality
    - 3.1.1 Access control
    - 3.1.2 Access control
    - 3.1.3 Access control
    - 3.1.4 Separation requirement
  - 3.2 Integrity
    - 3.2.1 Transfer control
    - 3.2.2 Input control
  - 3.3 Availability, resilience and rapid recovery
  - 3.4 Procedures for regular review, assessment and evaluation
    - 3.4.1 Data protection management
    - 3.4.2 Incident-Response-Management
    - 3.4.3 Data protection-friendly default settings
    - 3.4.4 Job control

## 1. Introduction

The EU General Data Protection Regulation (GDPR) contains requirements on how personal data should be handled in technical and organisational terms. This serves the goal of data security. Data security thus represents a further and complementary aspect of data protection. Data security is regulated by law in Article 32 (1) of the GDPR. These regulations require that such technical and organisational measures be taken as are necessary to ensure the protection of personal data.

The GDPR contains various control areas, each of which contains various sub-items:

- Confidentiality
- Integrity
- Availability and resilience
- Procedures for periodic review, assessment and evaluation
- Pseudonymisation and encryption

The Contractor has implemented the following technical and organisational measures for its business. The contractual hosting in connection with the Service takes place on the systems of the "Amazon Cloud" of the carefully selected service provider Amazon Web Services, Inc. 410 Terry Avenue North, Seattle WA 98109, United States. The technical and organisational measures of this subcontractor can be found at [https://aws.amazon.com/de/security/?nc1=f\\_cc](https://aws.amazon.com/de/security/?nc1=f_cc).

## 2. Organisational matters

FlowFox GmbH guarantees the written documentation of the current level of data protection, as well as the written work instructions, guidelines and leaflets for employees. Employees involved in data processing are obliged to maintain data secrecy and confidentiality in accordance with Art. 28 Para. 3 S. 2 lit. B, 29, 32 Para. 4 DSGVO. Some of the security measures in the following checklist relating to this area are not shown separately, as they are not published in detail for reasons of maintaining security through confidentiality.

## 3. Security measures

The following points describe the technical and organisational measures operated by FlowFox GmbH.

### 3.1 Confidentiality

#### 3.1.1 Access control

Access control includes measures that are suitable for preventing unauthorised persons from gaining access to data processing systems with which personal data are processed or used.

- There is a documented and effective procedure for granting, changing and withdrawing access rights, including the return of access equipment.
- A responsible person is appointed for the administration of the means of access.

- Documentation of key allocation is maintained and updated on an ongoing basis.
- The office buildings are locked and can only be opened manually by staff.
- Visitors are only allowed in the building when accompanied by a staff member.

### **3.1.2 Access control**

Measures suitable for preventing data processing systems from being used by unauthorised persons.

- Reduce the number of persons authorised to access the system to a minimum.
- Binding procedure for the allocation of authorisations.
- Clear assignment of user accounts to users.
- Each authorised person has his or her own password, known only to him or her, which may not be passed on. If the password becomes known, it must be changed immediately.
- Each user ID is uniquely assigned to a natural person at all times.
- Secure passwords are used. They are created and handled in accordance with a documented password policy.
- Passwords may only be reset or changed by authorised persons in accordance with a defined process.
- Administrators use separate accesses for the management of systems and their privileged activities are logged.
- There is no delegation of rights - only original rights holders can exercise functions.
- All access to systems (applications, operating systems, BIOS, boot devices, etc.) is password protected or locked.
- External access (remote access) is secured via a firewall, using strong encryption and 2-factor authentication.
- Partial login with biometric data
- Automatic screen locks after max. 5 min (password protected).

### **3.1.3 Access Control**

Measures to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage.

Unauthorised reading, copying, modification or deletion of data media is prevented by:

- Ensuring that only those access rights are assigned that are necessary to fulfil the respective task.

- The allocation and release of access rights is documented in a comprehensible manner so that it can be determined who has access to the data.
- For all data, a responsible person is defined who decides who may have which access.
- In the applications, it is ensured that the assigned access rights are technically implemented.
- In all environments that contain production data (including development, test, etc.), unauthorised access is excluded.

The restriction of the access possibilities of the person authorised to use a DP system exclusively to the data subject to his access authorisation is ensured by:

- Minimum number of administrators
- Management of user rights by administrators

### **3.1.4. Separation requirement**

Measures to ensure that data collected for different purposes can be processed separately.

Personal data may only be used for the purpose for which it was originally collected. Different and separate processing is ensured by:

- Data collected for different purposes are separated (physically or logically) in such a way that they are processed, stored and deleted separately according to the purpose (roles and authorisation concept).
- Development, test and productive environments are separated.
- Multi-client capability of relevant applications
- Definition of database rights

## **3.2 Integrity**

### **3.2.1. Disclosure Control**

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorised persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

- Physical dispatch of data media is not envisaged.
- Private data carriers may not be used in the company
- Data carriers that are no longer needed are destroyed by multiple overwriting (Gutmann method).

Unauthorised reading, copying, modification or removal of data during transmission is prevented by:

- TLS or SSH encryption of the data transmission.

- All sensitive data intended for transport is encrypted.

The transfer of personal data takes place through the use of the following services:

- Other services and transport procedures that are equivalent or better to the desired purpose and the current state of security technology.

The following security measures exist:

- Programmes that prevent or detect the intrusion of viruses.
- USB drives are not mounted by default (exceptions possible after risk/benefit assessment).

### **3.2.2 Input Control**

Measures to ensure that it is possible to check and determine retrospectively whether and by whom personal data have been entered into, modified or removed from data processing systems.

Whether and by whom data have been entered, changed or removed can be checked and determined retrospectively by:

- Technical logging of the entry, modification and deletion of data.
- Assigning authorisations for entering, changing and deleting data on the basis of an authorisation concept.

FlowFox GmbH collects, changes or deletes personal data primarily within the framework of its own customer management systems (inventory and usage data).

### **3.3 Availability, resilience and rapid recovery**

Measures to ensure that personal data is protected against accidental destruction or loss and can be quickly restored in the event of a physical or technical incident.

That data is protected against accidental destruction or loss is ensured by:

- Multiple hourly incremental backups, daily full backups.
- Disaster recovery concept is established and maintained.
- Protective measures (UPS, backup power supply, fire extinguishers, fire detection, etc.) against elementary hazards - especially fire, water, failure of supply networks, denial of service - are in place.
- Equipment for supplying data processing systems is regularly maintained.
- The use of (system) resources is monitored and adjusted if necessary to ensure sufficient system capacity.
- Data is backed up in such a way that it can be restored within a defined time, separated according to purpose.
- When backing up data, the scope, frequency, type (full, differential, incremental), time frame, encryption and physically separate storage are taken into account and documented in a traceable manner.

- Whenever the backup procedure is changed, the recoverability of the data from the backup is verified.

### **3.4 Procedures for regular review, assessment and evaluation**

#### **3.4.1 Data protection management**

FlowFox GmbH is supervised by the external data protection officer, Arne Platzbecker. The legally compliant implementation of the EU General Data Protection Regulation (accountability according to Art. 5 para. 2 DSGVO) is monitored by the external data protection officer.

- Employees are regularly trained and committed to confidentiality/data secrecy and compliance with data protection regulations.

#### **3.4.2 Incident Response Management**

A proceduralised handling of security incidents is implemented. In the event of an incident, employees immediately inform IT or their supervisor, who in turn informs IT. This is followed by coordination with the data protection officer. The processing by the data protection officer is ensured by appropriate deputisation regulations.

- A process based on best practices (ITIL) is in place to ensure that security incidents are identified, assessed and dealt with appropriately.
- Escalation procedures and organisational interfaces are defined with all relevant parties and the Data Protection Officer is involved immediately.
- All information security incidents that go beyond a typical minor disruption in day-to-day business are reported immediately to designated parties without further review.
- Regular training and awareness-raising of staff.

#### **3.4.3 Data protection-friendly default settings**

As a matter of principle, only data that is appropriate and necessary for business purposes is collected and processed. Automated data collection and processing procedures are designed in such a way that only the necessary data can be collected. Customer data is kept fully encrypted.

- No more personal data is collected and processed than is necessary for the purpose in question.

#### **3.4.4 Order control**

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

Employees who have access to the systems as administrators have all been instructed with regard to data protection, are bound to data secrecy and have accepted corresponding confidentiality and non-disclosure agreements as part of their employment contract.

In the event of termination without notice, additional measures are taken to prevent the intentional misuse of infrastructure or data by the external service provider (e.g. by blocking access).

### **3.5 Pseudonymisation and encryption**

- Mail attachments containing personal data are sent in encrypted form.
- Data transfer from the website via SSL encryption.
- Access via user name and password.

## Attachment II

### Current Sub-processor

**Amazon Web Services EMEA Sarl.**

38 Avenue John F. Kennedy

L 1855

Luxemburg

Contact: [aws-EU-privacy@amazon.com](mailto:aws-EU-privacy@amazon.com)

**Functional Software, Inc. dba Sentry,**

45 Fremont Street,

8th Floor,

San Francisco,

CA 94105

USA

Contact: [compliance@sentry.io](mailto:compliance@sentry.io)

**Azure Form Recognizer, Microsoft Corporation**

One Microsoft Way

Redmond,

WA 98052-6399

USA

Contact: <https://www.microsoft.com/de-de/concern/privacy>

**Skaylink GmbH**

Zielstattstraße 42

81379 München

Germany

Contact: [info@skaylink.com](mailto:info@skaylink.com)