Data Processing Addendum
Flower Labs GmbH

Table of Contents

Terms of Service Flower Labs ("ToS")
Data Processing Addendum ("DPA")

Section 1
PARTIES AND BACKGROUND

1.1 Customer has entered into the Agreement with Flower Labs GmbH ("**Flower Labs**") (each a "**Party**" and collectively the "**Parties**") under which Flower Labs has agreed to grant access to its Platform and to provide further services through the Platform as detailed in the Agreement between Flower Labs and the Customer (together the "**Services**") to the Customer (as amended from time to time) (the "**Agreement**").

1.2 In the course of providing the Services under the Agreement, Flower Labs will process Customer Personal Data. This Data Processing Addendum ("**DPA**") regulates the data protection obligations of the Parties when processing Customer Personal Data.

1.3 Whether or not one of the following Exhibits of this DPA apply depends on where the Customer and Customer Affiliates reside. This DPA covers the following situations:

a) Where the Customer and Customer Affiliate (as defined below) reside in the European Economic Area, including the European Union ("**EU**", together the "**EEA**") the Data Processor Clauses (as defined below) laid down in **Exhibit A** of this DPA are intended to govern the processing.

b) Where the Customer and/or Customer Affiliate (as defined below) reside in the UK (as defined below) the UK Addendum (as defined below) included in **Exhibit B** of this DPA is intended to govern the processing.

c) Where the Customer and/or Customer Affiliate (as defined below) reside in a Restricted Country (as defined below) the Standard Contractual Clauses (as defined below) are laid down in **Exhibit C** of this DPA and are intended to govern the processing.

1.4 The mandatory annexes of the Data Processor Clauses and the Standard Contractual Clauses are laid down in **Exhibit D**.

Section 2
DEFINITIONS

2.1 Capitalized terms used but not defined within this DPA shall have the meaning set forth in the Agreement. The following capitalized terms used in this DPA shall be defined as follows.

a) "**Customer Affiliate**" means an affiliate of the Customer who is a beneficiary to the Agreement.

b) "**Customer Personal Data**" means Personal Data processed by Flower Labs on behalf of Customer or Customer Affiliate in connection with the provision of the Services, which may also include Personal Data of Customer and Customer Affiliate's customers

and other third parties whose Personal Data is being processed by Customer or a Customer Affiliate.

c) "**Data Processor Clauses**" means standard contractual clauses set out in the annex of the Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council.

d) "**GDPR**" means Regulation (EU) 2016/679 (the "**EU GDPR**") or, where applicable, the "**UK GDPR**" as it forms part of the law for England and Wales, Scotland and Northern Ireland by virtue of section 3 of the UK European Union (Withdrawal) Act 2018.

e) "**Personal Data**" means any information relating to an identified or identifiable individual or device, or is otherwise "personal data," "personal information," "personally identifiable information" and similar terms, and such terms shall have the same meaning as defined by applicable data protection laws.

f) "**Restricted Country**" means a country, territory or a specified sector within a country, or an international organisation outside the EEA not deemed to ensure an adequate level of protection by the European Commission.

g) "**SCC**" means the Standard Contractual Clauses and the Data Processor Clauses.

h) "**Standard Contractual Clauses**" means module 4 of the standard contractual clauses set out in the annex of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

i) "**Sub-processor of Flower Labs**" means a processor appointed by Flower Labs to process Customer Personal Data; and

j) "**UK**" means the United Kingdom of Great Britain and Northern Ireland.

2.2 The terms "controller", "processor", "data subject", "process", "personal data breach" and "supervisory authority" shall have the same meaning as set out in the GDPR.

Section 3
INTERACTION WITH THE AGREEMENT

3.1 This DPA is incorporated into and forms an integral part of the Agreement and shall be effective and replace any previously applicable data processing and security terms as of the effective date of the Agreement ("**Effective Date**"). This DPA supplements and (in case of contradictions) supersedes the Agreement with respect to any processing of Customer Personal Data.

3.2 Any processing operation as described in Section 6 and Annex II of **Exhibit D** to this DPA shall be subject to this DPA.

3.3 Customer Affiliates shall be beneficiaries under this DPA and – through Customer (see Clauses 3.4 and 3.5) – be entitled to enforce all rights in relation to the Customer Personal Data provided by the respective Affiliate. Customer will ensure that all obligations under this DPA will be passed on to the respective Customer Affiliate.

3.4 Customer warrants that it is duly mandated by any Customer Affiliates on whose behalf Flower Labs processes Customer Personal Data in accordance with this DPA to (a) enforce the terms of this DPA on behalf of the Customer Affiliates, and to act on behalf of the Customer Affiliates in the administration and conduct of any claims arising in connection with this DPA; and (b) receive and respond to any notices or communications under this DPA on behalf of Customer Affiliates.

3.5 Customer shall be the only point of contact for all communication between the Customer Affiliates and Flower Labs.

Section 4
SCOPE OF PROCESSING CLAUSES

4.1 The Data Processor Clauses included in Section 1 of **Exhibit A** of this DPA shall by default apply where Customer Personal Data is provided by either Customer or a Customer Affiliate located in the EU and/or EEA, or to which the GDPR otherwise applies.

4.2 In addition to the Clauses applicable under Clause 4.1, the UK Addendum included in **Exhibit B** shall apply where Customer Personal Data is provided by a Customer or a Customer Affiliate is located in the UK.

4.3 The Standard Contractual Clauses included in Section 1 of **Exhibit C** of this DPA shall by default apply where Customer Personal Data is provided by a Customer or a Customer Affiliate located in a Restricted Country, or to which the GDPR otherwise does not apply.

Section 5
ROLES OF THE PARTIES

5.1 For the purposes of the GDPR, Flower Labs acts as "processor" or "sub-processor." Flower Labs' function as processor or sub-processor will be determined by the function of the Customer:

a) Where Customer acts as a controller, Flower Labs acts as a processor.

b) Where Customer acts as a processor on behalf of a controller, Flower Labs acts as a sub-processor.

5.2 Where Flower Labs acts as a sub-processor, the terms provided in the Data Processor Clauses or the Standard Contractual Clauses shall apply *mutatis mutandis*. The Customer must inform Flower Labs if it acts as a processor under the instructions of a controller. Flower Labs shall process the personal data only on documented instructions from the Customer's controller, as

communicated to Flower Labs by the Customer, and any additional documented instructions from the Customer. Such additional instructions shall not conflict with the instructions from the Customer's controller. The Customer's controller or the Customer may give further documented instructions regarding the data processing throughout the duration of the DPA.

Section 6
SUBJECT, DURATION, PURPOSE AND SPECIFICATION OF PROCESSING

6.1 The details of data processing (such as subject matter, nature and purpose of the processing, categories of personal data and data subjects) are described by the Parties in the Agreement and in **Exhibit D**.

6.2 The duration of the processing shall correspond to the duration of this DPA as set forth in Section 7.

Section 7
CONTRACT PERIOD

The duration of this DPA coincides with the duration of the Agreement. It commences and terminates with the provision of the Services under the Agreement, unless otherwise stipulated in the provisions of this DPA.

Section 8
MISCELLANEOUS

8.1 In the event of any conflict between the SCC, the DPA or the Agreement the order of prevalence between the terms included therein shall be as follows:

a) where applicable, SCC,

b) the terms in **Exhibit D** of the DPA which are meant to fill in the required information for the SCC (where applicable) and, in particular, its Appendix,

c) the remaining provisions of this DPA, and

d) the Agreement and other contractual documents.

8.2 In the event a clause under the Agreement has been found to violate the Applicable Laws, this shall not affect the validity of the remaining provisions, and the Parties will mutually agree on modifications to the Agreement to the extent necessary to ensure data privacy-law compliant processing.

8.3 The DPA shall be governed by the laws stipulated in the Agreement.

Exhibit A

Data Processor Clauses

1. The following outlines the Data Processor Clauses as implemented in the DPA, subject to the amendments in Section 2 of this **Exhibit A**:

Standard Contractual Clauses

based on Commission Implementing Decision (EU) 2021/915

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) 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, and repealing Directive 95/46/EC (General Data Protection Regulation)

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

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

Clause 5 - Optional

Docking clause

Clause 5 of the Data Processor Clauses (Docking Clause) does not apply;

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing 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 ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 2 weeks in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect

business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 10
Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter

complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

***** END Data Processor Clauses *****

2. For the purposes of the Data Processor Clauses:

2.1 For the purposes of Clause 7.7 of the Data Processor Clauses the agreed list of Sub-processors of Flower Labs for the purpose of Clause 7.7(a) of the Data Processor Clauses is set out in Annex IV of Exhibit D to this DPA (the "**Approved List**").

2.2 Clause 7.7 lit. e) of the Data Processor Clauses shall not apply.

2.3 If Customer objects to Flower Labs' use of a new Sub-processor of Flower Labs (including when exercising its right to object under Option 2 of Clause 7.7(a) of the Data Processor Clauses) on reasonable grounds, it shall provide Flower Labs with written notice of the objection within 2 weeks after Flower Labs has provided notice to the Customer described in Clause 7.7(a) of the Data Processor Clauses in Section 1 of this Exhibit A to the DPA of such proposed change ("**Objection**"). If Customer does not object to the engagement within the

objection period, consent regarding the engagement shall be assumed. In the event Customer objects to Flower Labs' use of a new Sub-processor of Flower Labs, Customer and Flower Labs will work together in good faith to find a mutually acceptable resolution to address such Objection. If the Parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, either Party may, as its sole and exclusive remedy, terminate the portion of the Agreement relating to the Services affected by such change by providing written notice to the other Party. During any such Objection period, Flower Labs may suspend the affected portion of the Services. Customer may only request a pro-rata refund if Customer can prove that the Objection is based on justified reasons of incompliance with Applicable Laws.

2.4 Annex I (List of Parties) of the Data Processor Clauses shall be deemed to incorporate the information in Annex I of **Exhibit D** to this DPA;

2.5 Annex II (Description of Transfer) of the Data Processor Clauses shall be deemed to incorporate the information in Annex II of **Exhibit D** to this DPA; and

2.6 Annex III (Technical and Organisational Measures) of the Data Processor Clauses shall be deemed to incorporate the information in Annex III of **Exhibit D** to this DPA.

2.7 Annex IV (Subprocesser) of the Data Processor Clauses shall be deemed to incorporate the information in Annex IV of **Exhibit D** to this DPA.

Exhibit B

UK Addendum

1. Definitions and Interpretation

1.1 Terms used in this UK Addendum but not defined in the DPA have the following meaning:

"**UK Data Protection Laws**" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

1.2 This UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation und the UK Data Protection Laws.

1.3 Where there is any inconsistency or conflict between the UK Addendum and Data Processor Clauses, the UK Addendum overrides the Data Processor Clauses, except where (and in so far as) the inconsistent or conflicting terms of the Data Processor Clauses provides greater protection for data subjects, in which case those terms will override the UK Addendum.

2. Incorporation of and changes to the Data Processor Clauses

2.1 This UK Addendum incorporates the Data Processor Clauses which are amended to the extent necessary so that they ensure compliance with the requirements under Art. 28 UK GDPR.

2.2 The Data Processor Clauses in Exhibit A including all amendments in Section 2 of Exhibit A shall be read and interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the parties' obligation to enter into an agreement that complies with Articles 28(3) and (4) of the UK GDPR.

2.3 The Data Processor Clauses are deemed amended to the extent necessary, so they operate:

2.3.1 for processing by Flower Labs on behalf of the Customer, to the extent that UK Data Protection Laws apply to such processing; and

2.3.2 to ensure compliance with Article 28(3) and (4) of the UK GDPR.

2.4 The amendments referred to in Section 2.2 include (without limitation) the following:

2.4.1 references to 'Regulation (EU) 2016/679', '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)' and 'that Regulation' are all replaced by 'UK GDPR';

2.4.2 references to specific Article(s) of 'Regulation (EU) 2016/679' are replaced with the equivalent Article or Section of UK GDPR;

2.4.3 references to Regulation (EU) 2018/1725 are removed;

2.4.4 references to the "Union", "EU" and "EU Member State" are all replaced with the "UK"; and

2.4.5 references to the "competent supervisory authority" shall be replaced with the Information Commissioner.

2.5 References to the 'Clauses' means this UK Addendum, incorporating the Data Processor Clauses.

Exhibit C

Standard Contractual Clauses

1. The following outlines the Standard Contractual Clauses as implemented in the DPA, subject to the amendments in Section 2 of this Exhibit C:

Standard Contractual Clauses

based on Commission Implementing Decision (EU) 2021/914

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')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) 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 8.1 (b) and Clause 8.3(b);

(iii) [Intentionally left blank]

(iv) [Intentionally left blank]

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

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 – Optional

Docking clause

[Intentionally left blank]

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 exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data , the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

[Intentionally left blank]

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

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.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

[Intentionally left blank]

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

Clause 14

Local laws and practices affecting compliance with the Clauses

The following applies where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU.

(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

The following applies where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

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.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the 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 [for Module Three: and the controller] 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 collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. 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 a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Berlin, Germany.

***** END Data Processor Clauses *****

2. For the purposes of the Standard Contractual Clauses:

2.1 Annex I.A (List of Parties) of the Standard Contractual Clauses shall be deemed to incorporate the information in Annex I of Exhibit D to this DPA; and

2.2 Annex I.B (Description of Transfer) of the Standard Contractual Clauses shall be deemed to incorporate the information in Annex II of Exhibit D to this DPA.

Exhibit D

Annex I of Exhibit D:

Customer referred to as the controller(s) in the Data Processing Clauses and data importer with respect to the Standard Contractual Clauses:

Name: The Customer is the party who has concluded the Agreement with Flower Labs

Address: is provided by the Customer in in the Agreement

Contact person's name, position, and contact details: are provided by the Customer in the Agreement

Contact details of the data processing officer: if applicable, are provided by the Customer in the Agreement

Activities relevant to the data transferred under the Standard Contractual Clauses: as described in the Agreement and any applicable Order.

Role under Applicable Law: controller or processor on behalf of a third party

Flower Labs referred to as the processor with respect to the Data Processing Clauses and data exporter with respect to the Standard Contractual Clauses:

Name: Flower Labs GmbH

Address: Winterhuder Weg 29, 7. Stock, 22085 Hamburg, Germany

Contact person: Taner Topal, email: taner@flower.ai

Contact details of the data processing officer: not yet appointed, as there is no legal requirement to do so. This will be checked on a regular basis in the future.

Activities relevant to the data transferred under the Standard Contractual Clauses: as described in the Agreement.

Role under Applicable Law: processor on behalf of Customer as a controller or sub-processor on behalf of Customer as a processor

[As an integral part of the Agreement, the DPA is effective without signature starting from the Effective Date of the Agreement]

Annex II of Exhibit D:

The following information is provided for all Services. Limitations to specific services are indicated where feasible.

Categories of data subjects whose personal data is processed:

- Employees of Customers, employees of Customers' customers and other third parties or partners, authorized Users of the Platform or any other Services (e.g., employees of the Customer/Customer Affiliates, administrators).

Categories of personal data transferred (for purposes of Standard Contractual Clauses) and personal data processed (for purposes of Data Processing Clauses)

- Identification and contact data (*e.g.*, name, business email, business phone);
- account/use data (*e.g.*, user ID, roles/permissions, log-in timestamps, platform log data); ticket/support-related metadata and communications as provided by the Customer;
- technical log and telemetry data necessary to provide the Services except for self-hosted services (*e.g.*, error messages, timestamps, request IDs).
- license validation data, certain support data and remote access logs for self-hosted services.
- No intentional processing of special categories; any such data is to be avoided by the Customer or pseudonymized/anonymized before disclosure; Customer Data processed through the Platform or any other Service, log-data.

For purposes of the Standard Contractual Clauses, the frequency of the transfer (*e.g.*, whether the data is transferred on a one-off or continuous basis).

- Transfers occur on a need-to-have and purpose-bound basis in the course of providing the Services; this may be event-driven (*e.g.*, a support case) or ongoing in a limited scope (*e.g.*, technical logs), in each case under the Customer's instructions.

Nature of the processing

- Flower Labs offers access to its Platform, certain Support Services for its Platform and Professional Services including consulting services and software development services with respect to its open-source software, or Flower Labs may also offer Software-as-a-Service offerings. In course of providing the Services, Customer may grant access to Flower Labs into their IT or share certain personal data. Flower Labs processes personal data in course of such Services. Generalized description of processing: collection, recording, organization, storage, adaptation/change, retrieval, consultation, use, disclosure by transmission (only to

sub-processors subject to instructions), alignment/combination, restriction, erasure/destruction, each solely to provide the Services.

Purpose(s) for which the personal data is processed, and for purposes of the Standard Contractual Clauses transferred, on behalf of the Customer

- The purposes are strictly limited to performance of the Agreement (operation of the platform, troubleshooting, support, quality assurance), implementation/consulting services on instruction, and ensuring the security, availability, and integrity of the Services. No processing for Flower Labs' own marketing purposes.

For Purposes of the Data Processing Clauses, the duration of the processing and for Purposes of the Standard Contractual Clauses, the period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- The personal data is processed for the duration of the contractual relationship. In the meantime, the personal data will be deleted upon request or if the purpose ceases to exist. After termination of the contractual relationship, the personal data is deleted in accordance with the internal deletion concept of Flower Labs.

For processing by (sub-) processors for purposes of the Data Processing Clauses, and for transfer to Sub-processors of Flower Labs, also specify subject matter, nature and duration of the processing

- Sub-processors of Flower Labs are used for the purpose of hosting and operation the software solutions provided by Flower Labs. Such transfer and/or processing serves the purpose of providing the Services and occurs for the duration of the contractual relationship. The nature of the processing includes activities such as storing, transmitting, deleting, structuring, organisation.

Annex III of Exhibit D:

1. Pseudonymisation and Encryption, Art. 32 para 1 point a GDPR

Pseudonymisation contains measures that enable one to process personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures. Encryption contains measures that enable one to convert clearly legible information into an illegible string by means of a cryptographic process.

- Stored data is encrypted where appropriate, including any backup copies of the data
- All SuperLink <> SuperNode communication encrypted via TLS 1.2+
- Data subjects are identified internally using unique, non-derivable account IDs

2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, Art. 32 para 1 point b GDPR

Confidentiality and integrity are ensured by the secure processing of personal data, including protection against unauthorized or unlawful processing and integrity and availability by measures to protect against accidental loss, destruction or damage.

2.1 Confidentiality

2.1.1. Physical access control

Measures that prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

- The Company does not operate publicly accessible offices or on-premise data centers
- Locked storage with restricted access for authorized personnel only
- Administrative access to systems is protected by hardware-based multi-factor authentication (e.g. security keys)
- Regulation of visitors and external staff
- Where the Customer deploys SuperGrid on self-hosted infrastructure, the Customer is solely responsible for implementing appropriate physical access control for their own infrastructure

2.1.2 System/Electronic access control

Measures that prevent data processing systems from being used without authorization.

- User authentication is implemented via a token-based centralized identity and access management system based on OpenID Connect
- Access and refresh token lifetimes follow reasonable default configurations
- Unique, non-shared credentials are assigned for each user
- Administrative access to systems is protected by multi-factor authentication (e.g. security keys)
- Secure transmission of credentials (using TLS)
- Guidelines exist for the secure handling of passwords and certificates
- Definition of authorized persons
- Access control to infrastructure that is hosted by cloud service provider
- In-time revocation of access for people who no longer need access / leave the company
- Automated alerting on illegal attempts of logging systems directly or indirectly connected to personal data
- Administrative access to production systems is restricted via VPN-based network segmentation where appropriate and centralized identity-based authorization; no direct public access is permitted
- Only explicitly authorized Flower Labs administrators belonging to designated identity groups may access production systems.
- Flower Labs provides secure license validation service (authentication, TLS) for self-hosted deployments

2.1.3 Internal Access Control

Measures that ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage.

- User sessions and administrative access are subject to automatic timeout mechanisms
- Access rights are granted individually, documented, and reviewed periodically
- Access right management including authorization concept, implementation of access restrictions, implementation of the "need-to-know" principle, managing of individual access rights.

2.1.4 Isolation/Separation Control

Measures to ensure that data collected for different purposes can be processed (storage, amendment, deletion, transmission) separately.

- Network separation
- Segregation of responsibilities and duties
- Document procedures and applications for the separation
- Federated architecture security: SuperLink runs in Flower Labs-controlled infrastructure with isolated tenants
- Network isolation via VPCs, security groups, and private subnets

2.1.5 Job Control

Measures that ensure that, in the case of commissioned processing of personal data, the data are processed strictly corresponding to the instructions of the principal.

- Training and confidentiality agreements for internal staff and external staff
- Information security assessment for vendors/partners

2.2. Integrity

2.2.1 Data transmission control

Measures ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.

- Secure transmission between client and server and to external systems by using industry-standard encryption
- Secure network interconnections ensured by Firewalls, anti-virus programs, routinely patching software etc.
- Logging of transmissions of data from IT system that stores or processes personal data
- All SuperLink <> SuperNode communication encrypted via TLS 1.2+
- Telemetry encryption in transit and at rest
- Regular security patching and vulnerability scanning

- Automated metering systems track capacity utilization per customer

2.2.2 Data input control

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

- Logging authentication and monitored logical system access
- Logging of data access including, but not limited to access, modification, entry and deletion of data
- Documentation of data entry rights and partially logging security related entries.
- Immutable audit logs for authentication, authorization, and federated run events

2.3 Availability and Resilience of Processing Systems and Services

Availability includes measures that ensure that personal data is protected from accidental destruction or loss due to internal or external influences. Resilience of processing systems and services includes measures that ensure the ability to withstand attacks or to quickly restore systems to working order after an attack.

- Backup Concept
- Protection of stored backup media
- Regular security patching and vulnerability scanning

3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, Art. 32 para 1 point c GDPR

Organisational measures that ensure the possibility to quickly restore the system or data in the event of a physical or technical incident.

- Formal measures to be completed shortly, such as Continuity planning and restoration capabilities.

4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, Art. 32 para 1 point d GDPR

Organisational measures that ensure the regular review and assessment of technical and organisational measures.

- Documentation of interfaces and personal data fields

- Regular internal assessments
- All support actions logged and provided to customer

Annex IV of Exhibit D:

The Customer has authorized the use of the following Sub-processor(s) of Flower Labs. Please note that sup-processors are listed Service-specific:

Sub-processor Name	Service Provided	Location	Purpose
Sup-processors Platform and SuperGrid			
Amazon Web Services (AWS) (Amazon Web Services EMEA SARL)	Cloud infrastructure hosting	Germany (eu-central-1), with potential expansion to other regions	Hosting SuperLink, data storage, network infrastructure
Google Cloud Platform	Cloud infrastructure hosting	Germany	Hosting SuperLink, data storage, network infrastructure
Microsoft Azure (Microsoft Corporation)	Cloud infrastructure hosting	Germany	Hosting SuperLink, data storage, network infrastructure
Hetzner Online GmbH	Cloud infrastructure hosting	Germany	Hosting SuperLink, data storage, network infrastructure
DataCamp Limited / CND	CDN infrastructure	Germany	CDN infrastructure
Datapacket	CDN infrastructure	Germany	CDN infrastructure
Google LLC (Google Analytics)	Analytics	United States	Website analytics, usage tracking (anonymized where possible)
Google LLC (Google Workspace)	Email Provider	United States	Email Provider, technical support
Plausible Insights OÜ / Plausible	Analytics	Germany	Website analytics, usage tracking (anonymized where possible)

Civilized Discourse Construction Kit, Inc. / Discourse	Discussion Board	United States and Germany	Discussion board for the community
Slack Technologies, LLC / Slack	Chat	United States	Community discussions
Docusign, Inc. / docusign	Contract Signing Service	United States and Germany	Signing contracts
Astrodon Inc. / loops.so	Transactional Email Provider	United States	Email sending
Sub-processor Selfhosted			
Civilized Discourse Construction Kit, Inc. / Discourse	Discussion Board	United States and Germany	Discussion board for the community
Slack Technologies, LLC / Slack	Chat	United States	Community discussions
Docusign, Inc. / docusign	Contract Signing Service	United States and Germany	Signing contracts
Astrodon Inc. / loops.so	Transactional Email Provider	United States	Email sending