WEEVA

DATA PROCESSING ADDENDUM

Version 26 August 2022

1 INTRODUCTION

1.1 Weeva makes available a hosted, on-demand, web-based software-as-a-solution ("**Solution**") to Customer under the Software as a Services Agreement ("**SaaS Agreement**").

1.2 To the extent Weeva **may** be required to process personal data on behalf of Customer under the SaaS Agreement, Weeva will do so in accordance with the terms set out in this Data Processing Addendum ("**DPA**").

2 DEFINITIONS

The following capitalised terms shall have the following meanings whenever used in this Agreement.

2.1 "**Additional Safeguards**" means those terms set out in section 6 of **Attachment D**.

2.2 "**CCPA**" means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199).

2.3 "**Customer**" means the party who completes the Order and is invoiced by Weeva pursuant to the SaaS Agreement.

2.4 "**Data Exporter**" means a party that is transferring Personal Data directly or via onward transfer to a country that triggers additional requirements for the protection of Personal Data being transferred under applicable Data Protection Laws.

2.5 "**Data Importer**" means a party that receives Personal Data directly from a Data Exporter, or via onward transfer, and that is located in a country that triggers additional requirements for the protection of Personal Data being transferred under applicable Data Protection Laws.

2.6 "**Data Protection Laws**" means any law relating to data protection privacy, and security applicable to a party in connection with the processing of personal data under the SaaS Agreement including but not limited to (each as amended or replaced from time to time) (a) EU Data Protection Laws, (b) UK Data Protection Laws, (c) the CCPA, (d) the Swiss Federal Act of 19 June 1992 on Data Protection ("**FADP**"), and (e) any applicable laws worldwide relevant to Weeva or Customers (where applicable and as recipients of services provided by Weeva) relating to data protection.

2.7 "**EU**" means the European Union.

2.8 "**EU Data Protection Laws**" means the GDPR, any successor thereto, and any other law relating to the data protection or privacy of individuals that applies in the European Economic Area.

2.9 "**EU SCCs**" means Sections I, II, III and IV (as applicable) in so far as they relate to Module Two (Controller-to-Processor), Module Three (Processor-to-Processor) and Module Four (Processor-to-Controller), as applicable, within the Standard Contractual Clauses for the transfer of Personal Data to third countries under Regulation (EU) 2016/679 of the European Parliament and the Council approved by EC Commission Decision of 4 June 2021, as set out in **Attachment D**.

2.10 “**GDPR**” means the General Data Protection Regulation ((EU) 2016/679).

2.11 “**Personal Data**” means all personal data provided to Weeva by, or on behalf of, Customer through Weeva’s use of the Solution.

2.12 “**Privacy Notice**” means the then-current privacy notice describing Weeva’s treatment of Personal Data in its general business administration, management, and operations, which is made available at www.weeva.earth/policies (or successor site) and as may be updated by Weeva from time-to-time (effective upon publication).

2.13 “**Restricted Transfer”** means a transfer of Personal Data from a Data Exporter to a Data Importer.

2.14 “**Standard Contractual Clauses**” or “**SCCs**” means any pre-approved standard contractual clauses for the international transfer of personal data under applicable Data Protection Laws, including the EU SCCs, the Swiss Addendum and UK Addendum, as may be updated, supplemented, or replaced from time to time under applicable Data Protection Laws, as a recognized transfer or processing mechanism (as applicable)

2.15 “**Swiss Addendum**” means the EU SCCs as amended by **Attachment E**.

2.16 “**UK**” means the United Kingdom of Great Britain and Northern Ireland.

2.17 “**UK Addendum**” means the template Addendum B.1.0 issued by the Information Commissioner’s Office and laid before Parliament under s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the Mandatory Clauses of the Addendum. The UK Addendum is set out in **Attachment E**.

2.18 “**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.

2.19 “**UK GDPR**” means the GDPR as implemented in the UK.

2.20 “**Weeva**” means Weeva Limited (company no. 13811908), with its registered address at 1 Charter House Street, London, EC1N 6SA, England.

2.21 “**Weeva Group**” means Weeva and its current and future subsidiaries from time to time.

2.22 **Lower case terms**. The following lower-case terms used but not defined in this DPA, such as “**controller**”, “**data subject”**, “**personal data**”, “**personal data breach**” “**processor**” and “**processing**” will have the same meaning as set forth in Article 4 of the GDPR, or where not specifically defined under Data Protection Laws, the same meaning as analogous terms in those Data Protection Laws.

3 APPLICABLE LAW

3.1 Weeva may be required to process Personal Data on behalf of Customer under any applicable Data Protection Laws.

3.2 Unless expressly stated otherwise, in the event of any conflict between the main body of this DPA and Data Protection Laws, the applicable Data Protection Laws will prevail.

3.3 To the extent Weeva is a processor of Personal Data subject to the EU Data Protection Laws and/or UK Data Protection Laws, the mandatory sections required by Article 28(3) of the GDPR (or UK GDPR, as applicable) for contracts between controllers and processors that govern the processing of personal data are set out in clauses 5.1,5.2, 6.1,6.3, 6.4, 7, 8.1, 8.2, 9.1, 9.2, 10 to 13 (inclusive).

4 DURATION AND TERMINATION

4.1 This DPA will commence on the date it is signed by the party who signs it last and will remain in force so long as the SaaS Agreement remains in effect or Weeva retains any Personal Data related to the SaaS Agreement in its possession or control.

4.2 Weeva will process Personal Data until the date of expiration or termination of the SaaS Agreement, unless instructed otherwise by Customer in writing, or until such Personal Data is returned or destroyed on the written instructions of Customer or to the extent that Weeva is required to retain such Personal Data to comply with applicable laws.

5 PERSONAL DATA TYPES AND PROCESSING PURPOSES

5.1 The Customer and Weeva acknowledge that the Customer is the controller and Weeva is the processor or sub-processor of Personal Data.

5.2 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 concerning the Solution described in the SaaS Agreement ("**Business Purposes**"), are specified in **Attachment B**.

5.3 The Customer remains responsible for its compliance obligations under applicable Data Protection Laws, including providing any required notices, obtaining any required consents, and for the processing instructions it gives to Weeva.

6 WEEVA OBLIGATIONS

6.1 **Customer instructions**. When Weeva acts as the processor of Personal Data, it will only process the Personal Data on Customer's documented instructions from the categories of persons that the Customer authorizes to give Personal Data processing instructions to Weeva, as identified in **Attachment B** ("**Authorized Persons**") and to the extent that this is required to fulfil the Business Purposes. Weeva will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or applicable Data Protection Laws. Should Weeva reasonably believe that a specific processing activity beyond the scope of Customer's instructions is required to comply with a legal obligation to which Weeva is subject, Weeva must inform Customer of that legal obligation and seek explicit authorization from Customer before undertaking such processing. Weeva will not process the Personal Data in a manner inconsistent with Customer's documented instructions.

6.2 **Independent controller**. To the extent Weeva uses or otherwise processes Personal Data in connection with Weeva's legitimate business operations, Weeva will be an independent controller for such use, will process Personal Data in accordance with its Privacy Notice, and will be responsible for complying with all applicable laws and controller obligations.

6.3 **Compliance**. Weeva will reasonably assist Customers in complying with their obligations under applicable Data Protection Laws. In doing so it will take into account the nature of Weeva's processing and the information made available to Weeva, including in relation to data subject rights, data protection impact assessments and reporting to and consulting with data protection authorities under applicable Data Protection Laws. Weeva will notify Customer if, in its opinion, any instruction infringes applicable Data Protection Laws. This notification will neither constitute a general obligation on the part of Weeva to monitor or interpret the laws applicable to Customer, nor constitute legal advice to Customer.

6.4 **Disclosure**. Weeva will not disclose Personal Data except: (a) as Customer directs in writing, (b) as described in this DPA or (c) as required by law. Where Weeva is permitted by law to do so, upon receiving a request from a public authority, Weeva will use reasonable endeavors to notify the Customer and attempt to redirect the public authority to request the Personal Data directly from Customer.

7 CONTRACTING WITH SUB-PROCESSORS

7.1 **List of sub-processors**. A list of Weeva's sub-processors that Weeva directly engages for the specific Solution as a processor is available on request to the Weeva contact mentioned in **Attachment A** or as otherwise made available on an Weeva website.

7.2 **General authorization.** Customer provides its general authorization to Weeva's engagement with sub-processors, including current and future subsidiaries of the Weeva Group, to provide services in relation to the Solution and process Personal Data on its behalf. To the fullest extent permissible under applicable Data Protection Laws this DPA will constitute Customer's general written authorization to the subcontracting by Weeva of the processing of Personal Data to this agreed list of sub-processors.

7.3 **Changes.** Weeva will notify the Customer in writing of any intended changes to the agreed list of sub-processors at least 14 days in advance, thereby allowing the Customer to object to such changes. Such objection must be made in writing to the Weeva contact mentioned in **Attachment A** within 10 days of notification. Customer's failure to submit a written objection to the agreed list of sub-processors within 10 days of notification, will be deemed acceptance of the changes to the agreed list of sub-processors.

7.4 **Performance**. Weeva is responsible for its sub-processors compliance with Weeva's obligations in this DPA.

8 CUSTOMER OBLIGATIONS

8.1 **Data subject requests**. If Weeva receives a request from Customer's data subject to exercise one or more of its rights under applicable Data Protection Laws, in connection with the Solution for which Weeva is a processor or sub-processor, Weeva will redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request. Weeva will comply with reasonable requests by Customer to assist with Customer's response to such a data subject request. Customer will be responsible for reasonable costs Weeva incurs in providing this assistance.

8.2 **Customer requests**. Weeva must promptly comply with any Customer request or instruction from Authorized Persons (a) requiring Weeva to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorized processing, (b) relating to Customer's obligations regarding the security of processing and (c) requiring Customer's prior consultation obligations in terms of applicable Data Protection Laws, considering the nature of the processing and the information available to Weeva.

8.3 **Warranty**. Customer warrants that: (a) it has all necessary rights to provide the Personal Data to Weeva for the processing to be performed in relation to the provision of the Solution, and (b) Weeva's expected use of the Personal Data for the Business Purposes as specifically instructed by the Customer, will comply with all applicable Data Protection Laws.

8.4 **Privacy notices**. To the extent required by applicable Data Protection Laws, Customer is responsible for ensuring that all necessary privacy notices are provided to data subjects, and unless another legal basis set forth in applicable Data Protection Laws supports the lawfulness of the processing, any necessary data subject consents to the processing are obtained and a record of such consents is maintained. Should such consent be revoked by a data subject, Customer is responsible for communicating the fact of such revocation to Weeva, and Weeva remains responsible for implementing Customer's instruction with respect to the processing of that Personal Data.

9 SECURITY

9.1 **TOMs**. Weeva will implement appropriate Technical and Organizational Measures ("**TOMs**") to ensure the security of the Personal Data in terms of applicable Data Protection Laws, including the Data Security Addendum set out in Attachment C. This includes protecting the Personal Data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the Personal Data.

9.2 **Access to Personal Data.** Weeva will grant access to the Personal Data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring the SaaS Agreement. Weeva will ensure that persons authorized to process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

9.3 **Cost negotiations**. The parties will negotiate in good faith the cost, if any, to implement material changes other than those required by specific updated security requirements set forth in applicable Data Protection Laws or by data protection authorities of competent jurisdiction.

10 AUDITS

10.1 **Provision of evidence**. At Customer's written request, Weeva will provide Customer with evidence of any applicable certifications relating to the processing of Personal Data, including applicable certifications or audit reports of its computing environment and physical data centers that it uses in processing Personal Data to provide the Solution so that Customer can reasonably verify Weeva's compliance with its obligations under this DPA.

10.2 **Compliance with TOMS**. Weeva may also rely on those certifications to demonstrate compliance with the requirements set out in clause 9.1.

10.3 **Confidential information**. Any evidence provided by Weeva is confidential information and is subject to non-disclosure and distribution limitations of Weeva and/or any Weeva sub-processor.

10.4 **Customer Audits**. Customer may carry out audits of Weeva's premises and operations as these relate to the Personal Data of Customer if:

(a) Weeva has not provided sufficient evidence of the measures taken under clause 9; or

(b) an audit is formally required by a data protection authority of competent jurisdiction; or

(c) applicable Data Protection Laws provide Customer with a direct audit right (and as long as Customer only conducts an audit once in any twelve-month period, unless mandatory applicable Data Protection Laws require more frequent audits).

The Weeva Group are intended third-party beneficiaries of this section.

10.5 **Customer audit process**. The Customer audit may be carried out by a third party (but must not be a competitor of Weeva or not suitably qualified or independent) who must first enter into a confidentiality agreement with Weeva. Customer must provide at least 60 days advance notice of any audit unless mandatory applicable Data Protection Laws or a data protection authority of competent jurisdiction requires shorter notice. Weeva will cooperate with such audits carried out and will grant Customer´s auditors' reasonable access to any premises and devices involved with the processing of the Customer's

Personal Data. The Customer audits will be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. The Customer must bear the costs of any Customer audit unless the audit reveals a material breach by Weeva of this DPA in which case Weeva will bear the costs of the audit. If the audit determines that Weeva has breached its obligations under the DPA, Weeva will promptly remedy the breach at its own cost.

11 INCIDENT MANAGEMENT

11.1 **Security incidents**. If Weeva becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data while processed by Weeva (each a "**Security Incident**"), Weeva will promptly and without undue delay:

(a) notify Customer of the Security Incident;

(b) investigate the Security Incident and provide Customer with sufficient information about the Security Incident, including whether the Security Incident involves Personal Data of the Customer;

(c) take reasonable steps to mitigate the effects and minimize any damage resulting from the Security Incident.

11.2 **Security incident notification**. Notification(s) of Security Incidents will take place in accordance with clause 11.4. Where the Security Incident involves Personal Data of the Customer, Weeva will make reasonable efforts to enable Customer to perform a thorough investigation into the Security Incident, formulate a correct response, and take suitable further steps in respect of the Security Incident. Weeva will make reasonable efforts to assist Customer in fulfilling Customer's obligation under applicable Data Protection Laws to notify the relevant data protection authority and data subjects about such Security Incident. Weeva's notification of or response to a Security Incident under this clause is not an acknowledgement by Weeva of any fault or liability for the Security Incident.

11.3 **Other incidents**. Weeva will notify Customer promptly if Weeva becomes aware of:

(a) a complaint or a request concerning the exercise of a data subject's rights under any applicable Data Protection Laws about Personal Data Weeva processes on behalf of Customer and its data subjects; or

(b) an investigation into or seizure of the Personal Data of Customer by government officials, or a specific indication that such an investigation or seizure is imminent; or

(c) where, in the opinion of Weeva, implementing an instruction received from Customer about the processing of Personal Data would violate applicable laws to which Customer or Weeva are subject.

11.4 **Customer notifications.** Any notifications made to Customer under clause 11 will be addressed to the Customer contact mentioned in Attachment A using one of the contact methods set out in Attachment A.

12 CROSS BORDER TRANSFERS OF PERSONAL DATA

12.1 **General.** Except as described elsewhere in the DPA, Personal Data that Weeva processes on Customer's behalf may be transferred to and stored and processed in any country in which Weeva or its sub-processors may operate.

12.2 **Restricted Transfers**. Where there is a Restricted Transfer of Personal Data, the Data Exporter and the Data Importer must transfer and process the Personal Data in accordance with all applicable Data Protection Laws. In particular:

(a) **Attachment D** will apply where Personal Data that is subject to EU Data Protection Laws is transferred from a Data Exporter to a Data Importer acting as a Processor;

(b) **Attachment E** will apply where Personal Data that is subject to applicable Data Protection Laws in the specific jurisdiction provisions set forth in **Attachment E** is transferred outside the listed jurisdictions.

12.3 **Execution of SCCs**. If any cross-border transfer of Personal Data between Weeva and the Customer requires the execution of SCCs to comply with the applicable Data Protection Law, the parties' signature to this DPA or the SaaS Agreement will be considered as signature to the SCCs.

12.4 **Change of statutory transfer mechanism**. To the extent that Weeva is relying on the EU SCCs, UK Addendum or another specific statutory mechanism to normalize international data transfers and those mechanisms are subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, Customer and Weeva agree to cooperate in good faith to promptly suspend the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

13 RETURN OR DESTRUCTION OF PERSONAL DATA

13.1 **Customer deletion.** For certain Solution, Customer is responsible for installing, hosting, processing and using Personal Data. Here only Customer can access, extract and delete Personal Data stored in that Service. Where the particular Service does not support access, retention or extraction of software provided by Customer, Weeva has no liability for the deletion of Personal Data as described in this clause 13.1.

13.2 **Delete or return**. Where the SaaS Agreement requires Weeva to retain Personal Data, Weeva will delete that Personal Data within the period agreed to in the SaaS Agreement, unless Weeva is permitted or required by applicable law to retain such Personal Data. Where the retention of Personal Data has not been addressed in the SaaS Agreement, Weeva will either delete, destroy or return all Personal Data to Customer and destroy or return any existing copies when Weeva has finished providing Solution:

(a) related to the processing;

(b) when this DPA terminates;

(c) Customer requests Weeva to do so in writing; or

(d) Weeva has otherwise fulfilled all purposes agreed in the context of the Solution related to the processing activities where Customer does not require Weeva to do any further processing.

13.3 **Certificate of destruction**. Weeva will provide Customer with a destruction certificate at Customer's request. Where the deletion or return of the Personal Data is impossible for any reason, or where backups and/or archived copies have been made of the Personal Data, Weeva will retain such Personal Data in compliance with applicable Data Protection Laws.

13.4 **Third parties**. On termination of this DPA, Weeva will notify all sub-processors supporting its processing and make sure that they either destroy the Personal Data or return the Personal Data to Customer, at the discretion of Customer.

14 LIABILITY

14.1 Any limitation of liability in the SaaS Agreement **will apply** to this DPA.

14.2 Notwithstanding clause 14.1, in no event shall Weeva or Customer be liable to each other for any consequential, indirect, special, incidental, exemplary or punitive damages arising out of or related to this DPA nor for any loss of profit, loss of use, loss of revenue or loss of business, loss of goodwill, loss of reputation, loss of opportunity, loss of anticipated savings or loss of margin, or to any users of the Solution or to any third parties for the loss of data (including Personal Data), whether such claim arises contractually, through negligence/tort, as a result of a misrepresentation, restitution, under state or otherwise.

15 NOTICE

15.1 Any notice or other communication given to a party under or in connection with this DPA must be in writing and delivered to the other party by email.

15.2 Clause 15.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

15.3 Any notice or other communication will be deemed given when:

(a) delivered in person;

(b) received by mail (postage prepaid, registered or certified mail, return receipt requested); or

(c) received by an internationally recognized courier service (proof of delivery received by the noticing party) at the physical notice address (as identified above), with an electronic copy sent to the electronic notice address (as identified in the table above).

16 MISCELLANEOUS

16.1 **Conflict of terms**. The SaaS Agreement terms remain in full force and effect except as modified in this DPA. Insofar as Weeva will be processing Personal Data subject to applicable Data Protection Laws on behalf of the Customer in the course of the performance of the SaaS Agreement, the terms of this DPA will apply. If the terms of this DPA conflict with the terms of the SaaS Agreement, the terms of this DPA will take precedence over the terms of the SaaS Agreement.

16.2 **Governing law**. This DPA is governed by the laws of the country specified in the relevant provisions of the SaaS Agreement and the EU SCCs and UK Addendum are governed by the laws as provided for in the EU SCCs or UK Addendum.

16.3 **Dispute resolution**. Any disputes arising from or in connection with this DPA will be brought exclusively before the competent court of the jurisdiction specified in the relevant provisions of the SaaS Agreement.

16.4 **Counterparts**: This DPA may be executed in any number of counterparts, each of which will constitute an original, but which will together constitute one agreement. Where one or both of the parties chooses to execute this DPA by electronic signature, each electronic signature will have the same validity and legal effect as the use of a signature affixed by hand and is made to authenticate this DPA and evidence the intention of that party to be bound by this DPA.

16.5 **Amendments**. Weeva will publish any intended amendments to this DPA on an Weeva website or send written notification to the Customer at least 14 days in advance, allowing the Customer to object to such amendments. Such objection must be made in writing to the Weeva contact mentioned in **Attachment A** within ten days of notification. Customer’s failure to submit a written objection to the intended amendments within ten days of notification will be deemed acceptance of the amendments to this DPA.

Attachment A Contact points

Contact information of the Customer:

The Business Representative of the Customer registered with Weeva

If the Customer requires an alternative contact point for data protections matters, please contact the data protection officer of Weeva to update the Customer's contact details.

Contact information of the data protection officer of Weeva:

Contact Information:	Jill Pruett
Physical Address:	1 Charterhouse Street, London, EC1N 6SA
Email:	hello@weeva.earth

Attachment B Particulars of Processing

Categories of data subjects whose personal data is transferred

Weeva acknowledges that, depending on Customer’s use of the Solution, the data importer may process the personal data of any of the following types of data subjects:

- Employees, contractors, temporary workers, agents and representatives of data exporter;
- Users (e.g., Customers end users) and other data subjects that are users of the Solution;
- Juristic or legal persons (where applicable).

Categories of personal data transferred

Weeva acknowledges that, depending on Customer’s use of the Solution, the types of Personal Data processed by Weeva may include, but are not limited to the following:

- Basic personal data (for example first name, last name, email address and work address);
- Authentication data (for example username and password);
- Contact information (for example work email and phone number);
- Professional or employment-related information (for example, employer name and job title);
- Unique identification numbers and signatures (for example IP addresses);
- Location data (for example, geo-location network data);
- Device identification (for example IMEI-number and MAC address);

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.

- Biometric Information;
- Details of race or ethnicity

Please see **Attachment C** for applied restrictions.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Personal data may be transferred on a continuous basis in order to provide the Solution under the existing SaaS Agreement

Nature of the processing

The Personal Data transferred will be subject to the following basic processing activities: ,

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organisation and structuring
- Using data, including analysing, consultation, testing, automated decision making and profiling
- Updating data, including correcting, adaptation, alteration, alignment and combination
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion.

Purpose(s) of the data transfer and further processing

The purpose of processing personal data is for Weeva to provide the Solution under the existing SaaS Agreement.

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

See clause 13 of the DPA

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

In accordance with the DPA, Weeva may engage sub-processors to provide the Solution on Weeva's behalf or use any of current or future subsidiaries of the Weeva Group for the duration of the SaaS Agreement. Any such sub-processors will be permitted to obtain personal data only to provide the Solution Weeva has engaged them to provide, and they are prohibited from using personal data for any other purpose.

A list of Weeva's sub-processors that Weeva directly engages for the specific Solution as a processor is available on request to the Weeva contact mentioned in **Attachment A** or as otherwise made available on a Weeva website.

Authorized persons: Weeva will only process the personal data on Customer's documented instructions

Attachment C Technical and Organizational Measures

Weeva's Data Security Addendum is available at www.weeva.earth/policies

Attachment D EU Standard Contractual Clauses

1 Definitions

1.1 For the purposes of this **Attachment D**, the following definitions will apply:

(a) “**C-to-P Transfer Clauses**” means Sections I, II, III and IV (as applicable) in so far as they relate to Module Two (Controller-to-Processor) within the 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 EC Commission Decision of 4 June 2021.

(b) “**P-to-C Transfer Clauses**” means Sections I, II, III and IV (as applicable) in so far as they relate to Module Four (Processor-to-Controller) within the 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 EC Commission Decision of 4 June 2021.

(c) “**P-to-P Transfer Clauses**” means Sections I, II, III and IV as applicable) in so far as they relate to Module Three (Processor-to-Processor) within the 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 EC Commission Decision of 4 June 2021.

2 All modules

2.1 If, in the performance of the Solution, Personal Data that is subject to EU Data Protection Laws is transferred from a Data Exporter to a Data Importer, then the parties must comply with the terms of the EU SCCs (as further described in section 3 to 5 below) and the following provisions will apply:

(a) Clause 7 (docking clause) of the EU SCCs will not apply.

(b) The option under Clause 11 (redress) of the EU SCCs will not apply.

(c) Any dispute arising from the EU SCCs will be resolved by the courts of England and Wales.

(d) Annex I.A to the EU SCCs (List of the Parties): The activities relevant to the transfer of Personal Data under the EU SCCs relate to the Solution provided by Weeva to Customer (see details on front page) under the SaaS Agreement. **Attachment A** includes the contact person’s name, position and contact details. The parties agree that their signature to the SaaS Agreement, to this DPA or to any other binding document which otherwise incorporates the DPA will be considered as signature to the SCCs in accordance with the terms set out therein.

(e) The contents of **Attachment B** will form Annex I.B to the EU SCCs (Description of Transfer).

(f) Information Commissioner’s Office will act as the competent supervisory authority for the purposes of Annex I.C of the EU SCCs (Competent Supervisory Authority).

3 C-P Transfer Clauses

3.1 Where Customer is the controller and Data Exporter of Personal Data and Weeva is a processor and Data Importer in respect of that Personal Data, then the parties must comply with the terms of the C-to-P Transfer Clauses and the following provisions will also apply:

(a) Option 2 under Clause 9(a) (general written authorisation) will apply;

(b) For the purposes of Clause 13(a) (supervision), the relevant option set out in Clause 13(a) will apply depending on whether the Data Exporter is (i) established in an EU Member State, (ii) is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) of the

GDPR and has appointed a representative pursuant to Article 27(1) of the GDPR or (iii) is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR;

(c) Option 1 under Clause 17 (governing law) will apply and the governing law will be the law of England and Wales;

(d) The contents of **Attachment C** to this DPA (Technical and Organizational Measures) will form Annex II of the C-P Transfer Clauses (Technical and organisational measures including technical and organisational measures to ensure the security of the data); and

(e) The list of sub-processors referred to in **Attachment B** to this DPA will form Annex III of the C-P Transfer Clauses (List of Subprocessors).

4 **P-P Transfer Clauses**

4.1 Where Weeva is the processor and Data Exporter of the Personal Data and the sub-processer is the Data Importer of that Personal Data, then the parties will comply with the terms of the P-to-P Transfer Clauses and the following provisions will also apply.

(a) For the purposes of Clause 8.6(c) and (d) (security of processing), the sub-processor must provide notification of a personal data breach concerning Personal Data processed by the sub-processor to Weeva and not directly to the Customer. Where appropriate, Weeva will forward the notification to the Customer;

(b) For the purposes of Clause 8.9 (documentation and compliance), all enquiries from a Customer will be provided to the Customer by Weeva;

(c) Option 2 under Clause 9 (general written authorization) will apply. The parties also agree that the controller has delegated the decision making and approval authority for sub-processing to the Customer for the purposes of Clause 9 (use of sub-processors). Weeva has the Customer's general authorization (on behalf of the controller) for the engagement of the sub-processors referred to in Attachment B to this DPA. Weeva will follow the process set out in clause 7.2 of this DPA to inform Customer and not the controller of any intended changes to that list. Where appropriate, the Customer will inform the controller of any changes;

(d) For the purposes of Clause 10 (data subject rights), Weeva will notify Customer and not the controller about any request it has received directly from a data subject. Where appropriate, the Customer will forward the notification to the relevant controller. The authorization to respond to the request must be provided to Weeva by the Customer on behalf of the controller.

(e) For the purposes of Clause 13(a) (supervision), the relevant option set out in Clause 13(a) will apply depending on whether Data Exporter is (i) established in an EU Member State, (ii) is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) of the GDPR and has appointed a representative pursuant to Article 27(1) of the GDPR or (iii) is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR;

(f) For the purposes of Clause 15 (obligations of the data importer in case of access by public authorities), Weeva will notify Customer and not the data subject(s) in case of access by public authorities. Weeva agrees to provide information on request for access by public authorities to the Customer in accordance with section 6 of this Attachment D. In the event that Weeva receives a request from the competent data protection authorities for the information it preserves pursuant to Clauses 15.1 (a) to (c) or 15.2(b) under the P-P Transfer Clauses it will inform the Customer and involve the Customer in responding to the competent data protection authority;

(g) Option 1 under Clause 17 (governing law) will apply and the governing law will be the law of England and Wales; and

(h) The contents of Attachment C to this DPA (Technical and Organizational Measures) will form Annex II of the P-P Transfer Clauses (Technical and organisational measures including technical and organisational measures to ensure the security of the data).

5 P-C Transfer Clauses

5.1 Where Weeva is the processor and Data Exporter of Personal Data and Customer is a controller and Data Importer in respect of that Personal Data, then the parties will comply with the terms of the P-to-C Transfer Clauses and the governing law in Clause 17 (governing law) will be the law of England and Wales.

6 Additional Safeguards to the EU SCCs

6.1 To the extent that the EU SCCs apply, the following safeguards will apply to the EU SCCs set out in this section 6 of this **Attachment D**.

6.2 Where in the Customer's reasonable opinion transfer impact assessments, or risk assessments, are necessary, Weeva will upon request promptly provide reasonable assistance and cooperation to the Customer (at the Customer's own cost) about the carrying out of the transfer impact assessments, or risk assessments, to enable the Customer to normalize the international data transfers.

6.3 Each party warrants that it has no reason to believe that applicable laws to which it is subject, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent it from fulfilling its obligations under this DPA and Data Protection Laws. Each party declares that in providing this warranty, it has taken due account in particular of the following elements:

(a) the specific circumstances of the processing, including the scale and regularity of processing subject to such applicable laws; the transmission channels used; the nature of the relevant Personal Data; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by it for the type of Personal Data processed by it;

(b) the applicable laws to which it is/are subject, including those requiring to disclose data to public authorities or authorizing access by such authorities, as well as the applicable limitations and safeguards; and

(c) safeguards in addition to those under this DPA, including the technical and organisational measures applied to the processing of the Personal Data by Weeva and the relevant sub-processor.

6.4 Each party warrants that, in carrying out the assessment under section 6.3 above, it has made its best efforts to provide relevant information and agrees that it will continue to cooperate in ensuring compliance with this DPA. The parties agree to document this assessment and make it available on request and it agrees that such assessment may also be made available to a data protection authority.

6.5 Weeva agrees to promptly notify the Customer if, after having agreed to this DPA and for the duration of the term of this DPA, it has reason to believe that it is or has become subject to applicable laws not in line with the requirements under section 6.3, including following a change of applicable laws to which is it is subject or a measure (such as a disclosure request) indicating an application of such applicable laws in practice that is not in line with the requirements under section 6.3. Following such notification, or if Customer otherwise has reason to believe that Weeva can no longer fulfil its obligations under this DPA (including in relation to the relevant sub-processor), Customer will promptly identify supplementary measures (such as, for instance, technical or organisational measures to ensure security and confidentiality) to be adopted by itself or Weeva (and/or the relevant sub-processor), at Customer's cost, to protect the Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security, if appropriate in consultation with the competent data protection authority.

6.6 Unless prohibited by applicable law, Weeva agrees to promptly notify Customer if it (or the relevant sub-processor to whom a transfer is made):

(a) receives a legally binding request by a public authority under applicable laws to which it (or the relevant sub-processor) is subject for disclosure of Personal Data. Weeva agrees to review (and to procure that the relevant sub-processor to whom the transfer is made will review) the request, having regard to applicable laws to which it (and the relevant sub-processor) is subject, the legality of the request for disclosure, notably whether it remains within the powers granted to the requesting public authority. The notification to the Customer will include information about the Personal Data requested, the requesting authority and the legal basis for the request;

(b) becomes aware of any direct access by public authorities to Personal Data under applicable laws to which it (or the relevant sub-processor) is subject; such notification will include all information available to Weeva (and the relevant sub-processor).

6.7 If Weeva (or the relevant sub-processor to whom the transfer is made) is prohibited by applicable law from notifying the Customer as set out in section 6.6, Weeva will use commercially reasonable efforts to obtain a waiver of the prohibition, to communicate as much information as possible, as soon as possible to the Customer. If Weeva cannot obtain a waiver of the prohibition and is under a compelling legal obligation to disclose a legally binding request from a public authority, Weeva will provide the minimum information permitted by applicable law when responding to a request. Unless Weeva is legally prohibited from doing so (for example if there is a prohibition under criminal law to preserve the confidentiality of the investigation by the public authority), Weeva will provide the Customer with any responses provided to the public authority.

6.8 Weeva agrees to document its (and the relevant sub-processors) legal assessment as well as any challenge to the request for disclosure and, to the extent permissible under applicable laws to which it (or the relevant sub-processor) is subject, make it available to Customer. It will also make it available to the competent data protection authority upon request.

6.9 Weeva will use reasonable endeavours to provide (and to procure that the relevant sub-processor to whom the transfer is made will provide) the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

6.10 To the extent permissible under the applicable laws to which Weeva (and the relevant sub-processor) is subject, Weeva agrees to publish transparency reports or summaries regarding requests from public authorities to Weeva for access to data and the kind of reply provided, insofar publication is allowed by applicable law.

6.11 Weeva agrees to preserve the information under section 6.10 for the duration of the processing and make it available to the competent data protection authority upon request.

6.12 Weeva will comply with its Public Authority Data Request Policy governing the disclosure of Personal Data in response to requests from public authorities.

6.13 Weeva will inform (and will procure that the relevant sub-processor to whom the transfer is made will inform) data subjects in a transparent and easily accessible format, on its website, of a contact point authorised to handle complaints or requests and Weeva will (and will procure that the sub-processors will) promptly deal with any complaints about requests from public authorities.

Attachment E Cross-border specific jurisdiction provisions

1 General

1.1 In the interest of meeting their obligations under Data Protection Laws, the parties agree that this General section of Attachment E will apply where:

(a) Personal Data is transferred from a Data Exporter to a Data Importer; and

(b) the jurisdiction from which the Personal Data originates recognizes the EU SCCs as an adequacy mechanism, or such jurisdiction has not adopted another legally sufficient transfer mechanism under Data Protection Laws or such Restricted Transfer is not otherwise governed by country-specific laws, under this Attachment E.

1.2 For the purposes of this General section of Attachment E the EU SCCs will be amended as follows:

(a) the EU SCCs are deemed to be amended to the extent necessary so they operate:

(i) for transfers made by the Data Exporter to the Data Importer, to the extent that applicable Data Protection Laws apply to the Data Exporter"s processing when making that Restricted Transfer; and

(ii) to provide appropriate safeguards for the transfers in accordance with applicable Data Protection Laws.

(b) references to "Regulation (EU) 2016/679" or "that Regulation" in the EU SCCs must be understood as references to "applicable Data Protection Laws";

(c) references to specific articles of "Regulation (EU) 2016/679" in the EU SCCs are removed and replaced with the equivalent article or section of applicable Data Protection Laws, where appropriate;

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

(e) references to a "Member State" or "EU Member States" in the EU SCCs must be understood as references to "the country where the Data Exporter is established", except for Clause 11(c)(i), where applicable, where reference to "Member State" will be replaced with "country"; and

(f) the footnotes to the EU SCCs are removed.

1.3 For the avoidance of any doubt, the parties do not intend to grant third-party beneficiary rights to data subjects under the EU SCCs when those data subjects would not otherwise benefit from such rights under Data Protection Laws. The higher level of protection provided by the EU SCCs will only apply in jurisdictions outside Europe where such a higher level of protection is required for the protection of Personal Data being transferred under Data Protection Laws.

2 Switzerland

2.1 Where a Restricted Transfer of Personal Data from a Data Exporter to a Data Importer is subject to the GDPR and the FADP, the following additional provisions to the EU SCCs will apply for the EU SCCs to be suitable for ensuring an adequate level of protection for such transfer in accordance with Article 6 paragraph 2 letter (a) of FADP:

(a) "**FDPIC**" means the Swiss Federal Data Protection and Information Commissioner.

(b) "**Revised FADP**" means the revised version of the FADP of 25 September 2020, which is scheduled to come into force on 1 January 2023.

(c) The term "**EU Member State**" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility pursuing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).

(d) The EU SCCs also protect the data of legal entities until the entry into force of the Revised FADP.

(e) The FDPIC will act as the "competent supervisory authority" insofar as the relevant Restricted Transfer is governed by the FADP.

2.2 The parties will also comply with the with the additional safeguards to the EU SCCs as set out in section 6 of Attachment D.

3 UK

3.1 Where a Restricted Transfer of Personal Data from a Data Exporter to a Data Importer is subject to UK Data Protection Laws, this section 3 of Attachment E will apply. The parties also agree to comply with the additional safeguards to the EU SCCs as set out in **section 6 of Attachment D**

PART 1 – TABLES

Table 1: Parties and signatures

Start date	DPA effective date	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties" details	Weeva or Customer, as applicable. See Attachment B	Weeva or Customer, as applicable. See **Attachment B**.
Key Contact	Please see **Attachment A**	
Signatures (if required for the purposes of Section 2)	N/A	N/A

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed in Attachment E, including the Appendix Information.

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than **the parties), and which for this DPA is set out in:**

Annex 1A: List of Parties: The contents of Annex I.A of **Attachment D**
Annex 1B: Description of Transfer: See **Attachment B**
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See **Attachment C**
Annex III: List of Sub processors (Modules 2 and 3 only): See **Attachment B**

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party

PART 2 – MANDATORY CLAUSES

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.