



CHARGEBEE - AMENDMENT TO VENDOR DPA

This is an amendment (“**Amendment**”) to any data processing agreement executed by and between CHARGEBEE INC. (“**Chargebee**”) and vendor entity identified in the signature block below (“**Vendor**”) (each a “**Party**” and collectively “**Parties**”) (the “**DPA**”).

This Amendment revises the DPA and SCCs to account for: (i) the new standard contractual clauses approved by the European Commission (Implementing Decision (EU) 2021/914 of 04 June 2021); (ii) the new international data transfer addendum (“**IDTA**”) approved by the UK Parliament on March 21, 2022; and (iii) the California Privacy Rights Act amending the California Consumer Privacy Act (“**CPRA**”). Any terms not defined in this Amendment shall have the meaning set forth in the DPA. In the event of a conflict between the terms and conditions of this Amendment and the DPA, the terms and conditions of this Amendment shall supersede and control. This Amendment is effective on the date last signed by either of the Parties to this Amendment (“**Amendment Effective Date**”).

- with the Consumers except as permitted under the CPRA.
- d. Enter into a written agreement with its sub-processors containing provisions required by the CPRA.

1. DEFINITIONS

“**SCCs**” means the standard contractual clauses as approved by the European Commission (Implementing Decision (EU) 2021/914 of 04 June 2021) and set forth as Exhibit A to this Amendment.

“**UK GDPR**” means the aspect of the GDPR as saved into the United Kingdom by virtue of section 3 of the United Kingdom European Union (Withdrawal) Act 2018.

“**Applicable Data Protection Law**” means all applicable laws, regulations, binding rules, codes and directives, whether federal, state, or foreign laws, including without limitation, and California Consumer Privacy Act (“**CCPA**”), the California Privacy Rights Act (“**CPRA**”) amending the CCPA, the General Data Protection Regulation (“**GDPR**”) (Regulation (EU) 2016/679); and the Swiss Federal Act on Data Protection (as may be amended or superseded).

2. INTERNATIONAL DATA TRANSFER MECHANISM

- 2.1 Where the Vendor Processes Personal Data under this Addendum that originates from the EEA, United Kingdom and/or Switzerland, any such Processing shall be conditional on compliance with the SCCs. By execution of this Addendum, Vendor and Chargebee execute the SCCs. Vendor shall not transfer Personal Data (nor permit Personal Data to be transferred) outside of the European Economic Area ("EEA") unless (i) it has first obtained Chargebee's prior written consent; and (ii) it takes place in compliance with the SCCs.
- 2.2 The provisions in Exhibit B shall additionally apply to the extent mandated under the UK GDPR for transfers of Personal Data originating in the United Kingdom to any other country not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for Personal Data.

3. CCPA AND CPRA OBLIGATIONS

In this Section the following terms “Personal Information”, “Consumers”, “Sell” shall have the meaning given in the CPRA.

- 3.1 Vendor agrees that Vendor will
 - a. Not Sell any Personal Information.
 - b. Not retain, use, or disclose the Personal Information except for any provision of the Services and as part of the direct relationship between Chargebee and the Vendor.
 - c. Not combine the Personal Information that is received from or on Chargebee’s behalf with Personal Information that is received from or on behalf of any other person or persons or from Vendor’s direct interaction

- 3.2 Vendor acknowledges that Chargebee has the right upon notice to take reasonable and appropriate steps to stop and remediate the unauthorized use of the Personal Information.
- 3.3 Vendor acknowledges and agrees that Chargebee has the right to take reasonable and appropriate steps to ensure that Vendor uses the Personal Information that they received from Chargebee or on Chargebee’s behalf in a manner consistent with your obligations under CPRA. Reasonable and appropriate steps can include ongoing manual reviews, automated scans of service provider’s systems, and regular assessments and audits or other operational or technical testing at least once in every 12 months.
- 3.4 Vendor shall provide reasonable and timely cooperation, without undue delay, to assist Chargebee to respond to requests from Consumers, including request for deletion of Personal Information or applicable data protection authorities relating to the processing of Personal Information under the DPA when Chargebee is required to respond to such requests under CPRA. In the event that any such request is made directly to Vendor, the Vendor shall not respond to such communication directly without Chargebee’s prior authorization, unless legally compelled to do so.
- 3.5 Vendor shall also ensure that all of its sub-processors perform actions necessary pursuant to any requests of Consumers including request for deletion of Personal Information, that are intimated to them by Chargebee.
- 3.6 Vendor certifies Vendor understands the restrictions in this Section and will comply with such restrictions. Upon Chargebee’s request, the Vendor agrees to provide a written certification to this effect.
- 3.7 Vendor represents and warrants that it is not a Third Party as defined in the CPRA.
- 3.8 Vendor shall notify Chargebee immediately, if the Vendor determines that they can no longer comply with the obligations under CPRA.
- 3.9 Any right, obligation or provision in the Agreement, to the extent CPRA applies, shall be governed by the laws of the State of California.

4. TERM AND TERMINATION

This Amendment shall come into force on the Amendment Effective Date and shall continue to be in full force and effect for the duration of the DPA and shall cease automatically thereafter. Where amendments are required to ensure compliance of this Amendment with applicable data protection law, the Parties shall agree on such amendments upon request of the Vendor. Where the Parties are unable to agree upon such amendments, Vendor has the right but not an obligation to

terminate the main services agreement, the DPA and this Amendment with prior written notice to Chargebee.

5. MISCELLANEOUS

Except as amended by this Amendment, the DPA will remain in full force and effect. In case of any conflict, the provisions of

this Amendment shall take precedence over the provisions of any other agreement between Chargebee and Vendor. Any supplementary agreements or amendments to this Amendment must be made in writing and signed by both Parties. Should individual provisions of this Amendment become void, invalid or non-viable, this shall not affect the validity of the remaining conditions of this Amendment.


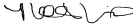
On behalf of CHARGEBEE INC.		On behalf of Spreadly, Inc.	
			
<small>Denis Curran (22nd December 2022, 9:25 GMT)</small>		<small>Nellie Vail (22nd December 2022, 9:48 GMT)</small>	
Name	Denis Curran	Name	Nellie Vail
Title	General Counsel	Title	CFO
Date Signed	Dec-22-2022	Date Signed	Dec-22-2022

Exhibit A – Standard Contractual Clauses

SECTION I

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.

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.

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), 8.9(a), (c), (d) and (e)
 - iii) Clause 9(a), (c), (d) and (e);
 - iv) Clause 12(a), (d) and (f);
 - v) Clause 13;
 - vi) Clause 15.1(c), (d) and (e);
 - vii) Clause 16(e);
 - viii) Clause 18(a) and (b)
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

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.

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.

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.

7. Docking clause

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

SECTION II – OBLIGATIONS OF THE PARTIES

8. Data protection safeguards

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

8.1. Instructions

- a. The data importer shall process the personal data only on documented instructions from the data exporter. Where the data exporter is a processor, the data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions throughout the duration of the contract.
- b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
- c. Where the data exporter is a processor, the data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2. Purpose limitation

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

8.3. Transparency

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

8.4. Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5. Duration of processing and erasure or return of data

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

8.6. Security of processing

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

8.7. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a

person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8. Onward transfers

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

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

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9. Documentation and compliance

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

9. Use of sub-processors

- a. **SPECIFIC PRIOR AUTHORISATION** The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least thirty (30) days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.
 - a. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
 - b. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
 - d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
 - e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

10. Data subject rights

- a. The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

- b. The data importer shall assist the data exporter, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter or, the controller, as communicated by the data exporter.

11. Redress

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

12. Liability

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

13. Supervision

- a. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
- b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

14. Local laws and practices affecting compliance with the Clauses

- a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
 - iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation and where the data exporter is a processor, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or where the data exporter is a processor, if instructed by the controller 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.

15. Obligations of the data importer in case of access by public authorities

15.1. Notification

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:
 - i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

Where the data exporter is a processor, the data exporter shall forward the notification to the controller.

- 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. Where the data exporter is a processor, the data exporter shall make the assessment available to the controller. 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

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 and, where the data exporter is a processor, the controller of such noncompliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- e. Either Party may revoke its agreement to be bound by these Clauses where
 - i. the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or
 - ii. Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

17. Governing Law

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

18. Choice of forum and jurisdiction

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

ANNEX I

Details specified in the DPA

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA
Details specified in the DPA

ANNEX III
LIST OF SUB-PROCESSORS
Details specified in of the DPA

Exhibit B

UK Addendum to SCCs

This Exhibit B shall stand included as an addendum to the SCCs set forth in Exhibit A. For the purposes of this Exhibit, “UK IDTA” shall refer to the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force from March 21, 2022.

The UK IDTA shall be deemed to be incorporated into this Exhibit and completed as follows:

Part 1: Tables

In Table 1 of the UK IDTA (*Parties*), the parties’ details and key contact information shall be as set forth in Annex I of Exhibit A.

In Table 2 of the UK IDTA (*Selected SCCs, Modules and Selected Clauses*), the version of the Approved EU SCCs which this UK IDTA is appended to, including the Appendix Information, shall be as set forth in Exhibit A.

In Table 3 (*Appendix Information*) of the UK IDTA:
Annex 1A: List of Parties: Shall be as set forth in Annex I of Exhibit A.
Annex 1B: Description of Transfer: Shall be as set forth in Annex I of Exhibit A.
Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: Shall be as set forth in Annex II of Exhibit A.
Annex III: List of Sub processors: Shall be as set forth in Annex III of Exhibit A.

In Table 4 (*Ending this Addendum when the Approved Addendum Changes*) of the UK IDTA, both the data importer and the data exporter may end the UK IDTA in accordance with the terms of the UK IDTA.

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 February 2, 2022, as it is revised under Section 18 of those Mandatory Clauses.

CONTRACT NAME	Vendor DPA Amendment CB INC
CONTRACT ID	59a7413b-3407-471b-b07a-844d3f94c0c1
STATUS	Executed

CONTRACT HISTORY



SIGNED

Signed by **Denis Curran** (denis.curran@chargebee.com).

22 December, 2022 17:25:42

UTC

IP: 0.0.0.0

Location unavailable



SENT

Sent for Signature to **Nellie Vail** (Nellie@spreadly.com) by **Luigi Ciniglio** (luigi@chargebee.com).

22 December, 2022 17:25:43

UTC



SIGNED

Signed by **Nellie Vail** (Nellie@spreadly.com).

22 December, 2022 18:49:27

UTC

IP: 136.56.111.2

Orange County, NC, USA



EXECUTED

This document has been signed and executed by all parties.