DATA PROCESSING ADDENDUM

Last updated on December 2022

This Data Processing Addendum, including all schedules attached hereto, (this "**DPA**") is incorporated into and forms part of the Heap Master Services Agreement (the "**MSA**") and Order Form(s) (together, the "**Agreement**") entered into by and between Customer and Heap Inc. ("**Heap**") (collectively, the "**Parties**"). This DPA shall apply to the extent that Heap processes Customer Personal Data on behalf of Customer or Customer Affiliates in connection with the provision of the Services. All capitalized terms not defined in this DPA shall have the meaning set forth in the Agreement.

By signing this DPA, the signing Customer entity enters into this DPA on behalf of itself and, to the extent required under applicable Data Privacy Laws, in the name and on behalf of its Affiliates, if and to the extent Heap processes Personal Data for which such Affiliates qualify as the entity that determines the purposes and means of the Processing (any such affiliate, an "**Customer Affiliate**"). For the purposes of this DPA only, the term "Customer" shall include Customer and Customer Affiliates.

HOW TO EXECUTE THIS DPA

This DPA has been pre-signed by Heap.

To complete this DPA, Customer must:

- complete the information in the signature block for Customer and execute this DPA on behalf of Customer; and
- send the executed DPA by email to legal@heap.io (indicating the name of the Customer entity signing this DPA and referencing the applicable Agreement or Order Form, and in the case of an Order Form, quote number).

Upon receipt by Heap of the validly complete DPA, this DPA will become legally binding.

INTERACTION WITH THE AGREEMENT

This DPA supplements the Agreement with respect to any processing of Customer Personal Data by Heap on behalf of Customer or a Customer Affiliate, as amended from time to time by written agreement between the Parties. In the event of any conflict between this DPA and the Agreement, the terms of this DPA shall prevail.

1. DEFINITIONS

"**Agreement**" has the meaning given to it above;

"**Customer Affiliate**" has the meaning given to it above;

"**Customer Personal Data**" means the personal data processed by Heap on behalf of the Customer in connection with the provision of the Services;

"**Data Protection Laws**" means the GDPR and all national, federal, state, provincial, or local privacy, cybersecurity, and data protection laws, together with any implementing or supplemental rules and regulations, applicable to the processing of Personal Data by Heap under this DPA, as amended or replaced from time to time;

"**DPA**" has the meaning given to it above;

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

"**Effective Date**" means the date of the Agreement.

"**GDPR**" means Regulation (EU) 2016/679 (the "**EU GDPR**") or, where applicable the "**UK GDPR**" as defined in the UK Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit) Regulations 2019;

"**Instruction**" means any documented instruction, submitted by Customer to Heap, directing Heap to perform a specific action with regard to personal data;

"**Member State**" means a member state of the EEA, being a member state of the European Union, Iceland, Norway, or Liechtenstein;\

"**Restricted Transfer**" means a transfer of Customer Personal Data in conditions such that, absent application of the provisions of clause 2 of this DPA, the transfer would be prohibited under Data Protection Laws;

"**Security Incident**" means any breach of security resulting in the unauthorized or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Customer Personal Data;

"**Services**" has the meaning given to it in the Agreement;

"**Standard Contractual Clauses**" means Module Two (*controller to processor*) and/or Module Three (*processor to processor*) annexed to Commission Implementing Decision (EU) 2021/914,

"**Sub-processor**" means a processor appointed by Heap to process Customer Personal Data.

The terms "**personal data**", "**controller**", "**processor**", "**data subject**", "**process**" and "**supervisory authority,**" and analogous terms shall have the same meaning as set out in applicable Data Protection Laws.

2. RESTRICTED TRANSFERS

2.1 The Parties agree that the terms of the Standard Contractual Clauses Module Two (Controller to Processor) or Module Three (Processor to Processor), as applicable depending on whether Customer is a controller or processor, apply to any Restricted Transfer from Customer (as data exporter) to Heap (as data importer) as specified below in 2.1(a):

(a) For Restricted Transfers subject to GDPR, Module Two shall apply in instances where Customer functions as a controller, whereas Heap functions as a processor. Module Three shall apply in the case where Customer functions as a processor on behalf of Customer's customers where

Heap

Customer and Customer's customer have concluded a data processing agreement in relation to the processing of personal data of Customer's customers.

(b) For Restricted Transfers subject to UK GDPR or Swiss data protection laws, the UK Addendum and/or Swiss Addendum (as applicable) set out in Schedule 3 shall apply.

2.2 The Parties agree that, for the purposes of the Standard Contractual Clauses:

(a) *Clause 7 - Docking clause* shall not apply*;*

(b) *In Clause 9 - Use of subprocessors*, Option 2 shall apply and the "time period" shall be thirty (30) days*;*

(c) *In Clause 11(a) - Redress,* the optional language shall not apply*;*

(d) *In Clause 13(a) - Supervision*, the following shall be inserted: the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex 1.C, shall act as competent supervisory authority.

(e) *In Clause 17 - Governing law,* Option 2 shall apply and the "Member State" shall be Ireland

(f) *In Clause 18 - Choice of forum and jurisdiction,* the Member State shall be Ireland*;*

(g) Annex I.A (*List of Parties*) shall be deemed to be Customer; Customer Affiliate; and Heap;

(h) Annex I.B (*Description of Transfer*) shall be deemed to incorporate the information in Schedule 1;

(i) Annex I.C (*Competent Supervisory Authority*) shall be deemed to refer to the supervisory authority of Ireland in the EEA ;

(j) Annex II (*Technical and Organisational Measures*) shall be deemed to incorporate the information in Schedule 2.

2.3 In the event of any conflict between the applicable Standard Contractual Clauses and this DPA, the applicable provisions of the Standard Contractual Clauses shall prevail.

3. INSTRUCTIONS FOR DATA PROCESSING

3.1 The Parties agree that the Agreement and this DPA shall constitute the Customer's instructions for the processing of Customer Personal Data.

3.2 To the extent that any of the Customer's instructions require processing of Customer Personal Data in a manner that falls outside the scope of the Services or this DPA, Heap may:

(a) make the performance of any such instructions subject to the payment by the Customer of any costs and expenses incurred by Heap or such additional charges as Heap may reasonably determine; or

(b) terminate the Agreement and the Services.

3.3 Notwithstanding the foregoing, Heap may process Customer Personal Data to the extent permitted or required by applicable Data Protection Laws, in which case Heap shall, to the extent permitted by such applicable law, inform the Customer of that legal requirement before processing that Customer Personal Data.

4. CUSTOMER WARRANTIES AND UNDERTAKINGS

4.1 The Customer represents and warrants that:

(a) it has provided all applicable notices to data subjects and, to the extent required, obtained consent from data subjects in each case as required for the lawful processing of Customer Personal Data in accordance with the Agreement and this DPA;

(b) it is duly authorised to enter into this DPA for and on behalf of any Customer Affiliates, and that, upon executing this DPA or a written amendment to the Customer Affiliates, each Customer Affiliate shall be bound by the terms of this DPA as if they were the Customer; and

(c) it is duly mandated to enforce the terms of this DPA on behalf of any Customer Affiliates, and to act on behalf of any Customer Affiliates in the administration and conduct of any claims arising in connection with this DPA.

5. SUB-PROCESSORS

5.1 The Parties agree that, as required by applicable Data Protection Laws:

(a) the Customer gives Heap general authorisation to engage sub-processors from an agreed list; and

(b) Heap shall maintain an up-to-date list of sub-processors at https://www.heap.io/sub-processors.

5.2 Heap will update the list of sub-processors, at least thirty (30) days prior to the date on which the sub-processor will commence processing Customer Personal Data. Customer may sign-up to receive email notification of changes to Heap's list of sub-processors at the aforementioned URL. If the Customer objects to Heap's use of a new sub-processor (such as when exercising its right to object under clause 9(a) of the Standard Contractual Clauses), Heap will use reasonable efforts to make available to the Customer a change in the Services, or will recommend a commercially reasonable change to the Services to prevent the applicable sub-processor from processing the Customer Personal Data.

5.3 If Heap is unable to make available such a change within a reasonable period of time, either Party may terminate that portion of the Agreement on which use of the new sub-processor would rely by providing not less than thirty (30) days' written notice to the other Party. During such notice period, Heap may suspend the affected portion of the Services.

5.4 For each new sub-processor engaged, Heap will (1) include terms in the agreement between Heap and the sub-processor that provide materially the same level of protection as this DPA, and (2), where required by applicable Data Protection Law, remain fully liable the acts or omission of its sub-processors.

6. SECURITY AND AUDIT

6.1 Heap may update the security measures set out in Schedule 2, including (where applicable) following any review by Heap of such measures, provided that such variation does not reduce the level of protection afforded to the Customer Personal Data by Heap under this DPA.

6.2 Heap shall treat the Customer Personal Data as the confidential information of the Customer, and shall ensure that (i) access to Customer Personal Data is limited to those employees or other personnel or agents who have a business need to have access to such Customer Personal Data; and (ii) any employees or other personnel have agreed in writing to protect the confidentiality and security of Customer Personal Data.

6.3 Upon Customer's written request, Heap shall provide Customer with a confidential summary report of audits or security assessments conducted by its external auditors to verify the adequacy of its security measures and other information necessary to demonstrate Processor's compliance with this Addendum. The report will constitute Heap's Confidential Information under the confidentiality provisions of the Agreement. The Parties may, if applicable Data Protection Law requires, agree to appoint a third-party auditor to verify the adequacy of Heap's security measures. The cost of any third-party audit will be borne by Customer, the third-party auditor shall not be any company that is a competitor to Heap, and audits shall be conducted in a manner so as to minimize the impact on Heap's business operations. Unless otherwise required by applicable Data Protection Law, Customer shall exercise this right only if and to the extent Heap's summary of its audits or security assessments are insufficient to allow Customer to demonstrate compliance with applicable Data Protection Laws.

6.4 With respect to any Customer Personal Data processed by Heap under applicable Data Protection Laws, if Heap or any sub-processor becomes aware of a Security Incident, Heap shall (i) notify the Customer of the Security Incident without undue delay; (ii) investigate the Security Incident and provide such reasonable assistance to the Customer (and any law enforcement or regulatory official) as required to investigate the Security Incident and (where required) notify data subjects and applicable supervisory authorities of the Security Incident, and (iii) take steps to remedy any non-compliance with this DPA.

7. ASSISTANCE AND INFORMATION

7.1 With respect to any Customer Personal Data processed by Heap under applicable Data Protection Laws, Heap shall, taking into account the nature of the processing and its role as a processor:

(a) provide reasonable assistance to Customer in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under the applicable Data Protection Laws;

(b) provide reasonable assistance to the Customer in responding to regulatory requests;

(c) implement (insofar as this is possible) appropriate technical and organisational measures for the fulfilment of the Customer's obligation to respond to requests for exercising data subject rights under applicable Data Protection Laws; and

(d) make available to the Customer on request information reasonably necessary to demonstrate compliance with this DPA and/or applicable Data Protection Laws.

7.2 Heap shall provide reasonable assistance to the Customer with any data protection impact assessments and with any prior consultations to any supervisory authority of the Customer, in each case solely in relation to processing of Customer Personal Data and taking into account the information available to Heap.

8. MODIFICATIONS

8.1 Heap may modify or supplement this DPA, with notice to Customer, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with applicable Data Protection Laws, (iii) to implement amended standard contractual clauses laid down by the European Commission or (iv) to adhere to a code of conduct or certification mechanism approved or certified pursuant to Art. 40, 42 and 43 of the GDPR. Customer shall notify Heap if it does not agree to a modification, in which case Heap may terminate this DPA and the MSA with two (2) weeks' prior written notice, whereby in the case of an objection not based on non-compliance of the modifications with applicable data protection law, Heap shall remain entitled to claim its agreed remuneration until the term end.

9. LAW AND JURISDICTION

9.1 Unless otherwise provided or required, this DPA shall be governed by, and construed in accordance with, the law of the jurisdiction as set forth in the Agreement. The Parties also agree to submit to the jurisdiction of the courts specified in the Agreement.

10. THIRD PARTY RIGHTS

10.1 Other than the right of data subjects or not-for-profit bodies, organisations or associations under the conditions set out in applicable Data Protection Laws, a person who is not a party to this DPA may not enforce any of its terms.

11. GENERAL

11.1 **Written Communications**. Applicable laws may require that some of the information or communications that the Parties send to each other should be in writing. The Parties agree, for the purposes of this DPA,

that communication between them will mainly be electronic and that the Parties will contact each other by e-mail. For contractual purposes, the Parties agree to this electronic means of communication and the Parties acknowledge that all contracts, notices, information and other communications provided by one Party to the other electronically comply with any legal requirement that such communications be in writing.

11.2 **Notices.** Any notices given by one Party to the other will be served if validly served in accordance with the Agreement and will be deemed received in accordance with the relevant provisions in the Agreement.

11.3 **Rights and remedies.** Except as expressly provided in the Agreement, the rights and remedies provided under the Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

11.4 **No partnership or agency.** Nothing in the DPA is intended to, or shall be deemed to, establish any partnership or joint venture between any of the Parties, constitute any Party the agent of another Party, or authorise any Party to make or enter into any commitments for or on behalf of any other Party. Each Party confirms it is acting on its own behalf and not for the benefit of any other person.

11.5 **Transfer of rights and obligations**. Neither Party shall transfer, assign or otherwise deal in the DPA, or any of its rights and obligations under this DPA, other than to an assignee of that Party's rights and obligations under the Agreement.

11.6 **Waiver**. No forbearance or delay by either Party in enforcing its rights shall prejudice or restrict the rights of that Party, and no waiver of any such rights or any breach of any contractual terms shall be deemed to be a waiver of any other right or of any later breach.

11.7 **Variation.** No variation of this DPA shall be effective unless it is in writing and signed by the Parties (or their authorised representatives).

11.8 **Severability**. If any provision of the DPA is judged to be illegal or unenforceable, the continuation in full force and effect of the remainder of the provisions of the DPA shall not be prejudiced.

12. CALIFORNIA CONSUMER PRIVACY ACT

12.1 This Section shall apply only insofar as Customer Personal Data contains personal information subject to the CCPA (as defined below) and shall apply in addition to, not in place of, any other requirements in this DPA.

12.2 In this Section, "**CCPA**" means the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act of 2020), codified at Cal. Civ. Code §§ 1798.100 – 1798.199.100, and the California Consumer Privacy Act Regulations issued thereto, Cal. Code Regs. tit. 11, div. 6, ch. 1, each as amended.

12.3 The Parties agree as follows:

(a) Each party shall comply with their respective applicable obligations under the CCPA and rules or regulations promulgated thereunder, and provide the same level of privacy protection as is required under the CCPA;

(b) Heap shall promptly notify the Customer if Heap determines that it can no longer meet its obligations under this Addendum or the CCPA. The Customer shall have the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information by Heap.

(c) Heap is processing Customer Personal Data subject to the CCPA for, or on behalf of, Customer, or Customer has made available Customer Personal Data to Heap, for the business or commercial purpose(s) identified in the Agreement.

(d) Heap shall not retain, use or disclose Customer Personal Data for any purpose outside the scope of the business relationship of the parties and other than for the specific purpose of performing services specified in the Agreement (including retaining, using or disclosing the Customer Personal Data for a commercial purpose other than providing the services specified in the Agreement) or as otherwise permitted by the CCPA as applicable to service providers;

(e) Heap shall not collect or use Customer Personal Data except to perform the services pursuant to the Agreement;

(f) Heap shall not Sell or Share (as defined in the CCPA), rent, release, disclose, disseminate, make available, transfer, or otherwise communicate Customer Personal Data that Heap receives from, or on behalf of, Customer to any third party for monetary or other valuable consideration.

(g) If Customer discloses deidentified Customer Personal Data to Heap, or Heap deidentifies Customer Personal Data previously disclosed by Customer, Heap shall take reasonable measures to ensure the deidentified Customer Personal Data cannot be associated with a consumer or household and shall not attempt to reidentify the deidentified personal information.

(h) Heap shall use reasonable efforts to assist Customer in Customer's fulfilment of its obligation to respond to California residents' requests to exercise rights with respect to their Customer Personal Data under the CCPA.

(i) Heap certifies it understands the obligations and restrictions contained above and will comply with them.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their respective duly authorized representative as of the Order Form Effective Date.

HEAP INC.	**CUSTOMER:**
Signature: Kate Helin	Signature:
Printed Name: Kate Helin	Printed Name:
Title: DPO	Title:
Date: 01 / 05 / 2023	Date:

SCHEDULE 1

DETAILS OF PROCESSING

1. **Categories of data subjects**

The categories of data subjects whose personal data are transferred:

Customer employees

Customer User data, if Customer configures the Services in such a way to capture this information

2. **Categories of personal data**

The transferred categories of personal data are:

Pageviews, user interactions, timing, IP addresses, browser details.

Additional identifying details might be present if the customer has coded explicit calls against the Heap API to associate such details with the incoming information stream, such as email addresses for logins, or other identifying information; these additional types of information are not intrinsic to the capture and require an explicit choice by the customer to code or enable.

3. **Special categories of personal data (if applicable)**

The transferred personal data includes the following special categories of data: N/A

The 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 are: N/A

4. **Frequency of the transfer**

The frequency of the transfer is: Continuous

5. Subject matter of the processing

The subject matter of the processing is: provide the Services to the Customer, including identifying behavioral patterns that are amenable to product improvements leading to better user experience or business-relevant outcomes.

6. Nature of the processing

The nature of the processing is: to provide the Services to the Customer, including collecting and analysing data to identify behavioural patterns.

7. Purpose(s) of the data transfer and further processing

The purpose/s of the data transfer and further processing is: to provide the Services to the Customer, including to produce aggregate behavioral reporting over the raw behavioral data set. More specifically, it involves the

reporting on specific customer-defined behavioral patterns of interest over the aggregate of the captured end-user behavioral data.

8.Sub-processor (if applicable)

For transfers to sub-processors, specify subject matter, nature and duration of the processing: *as set out at* https://www.heap.io/sub-processors.

SCHEDULE 2

TECHNICAL AND ORGANISATIONAL MEASURES

Description of the technical and organisational security measures implemented by the data importer / Heap (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons.

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

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

- The Heap system does not intrinsically capture directly identifying information; all data is highly pseudonymous behind opaque IDs. IP addresses are the most identifiable attributes, but they can be dropped through configuration. All actual direct identification is added to the system through customer opt-in enrichment mechanisms, like explicit API Identification calls, or optional third-party integrations.
- All data is end-to-end encrypted in-transit to Heap's internet-facing APIs and the web application using TLS 1.2 or higher. Data at rest is secured with SSE-S3 using AES-256.

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

Confidentiality and integrity are ensured by the secure processing of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Confidentiality and physical access control measures are designed to prevent unauthorised persons from gaining access to data processing systems with which personal data are processed or used.

Heap uses AWS to host its service and relies on AWS to maintain physical security of its data centers. Heap does not host any production infrastructure outside AWS, notably including Heap offices.

System/Electronic access control measures are designed to prevent data processing systems from being used without authorisation.

- We use an SSO provider to manage all access to any infrastructure, any systems, and any applications. All access to any databases, networks, or applications is restricted to only the employees that require access, and all access is protected by best-practice MFA.
- All employee access is logged and reviewed on a periodic basis.

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

- Heap applies the principle of least privilege, where employees are only provided with the level of access required for their role, upon manager approval.

Isolation/Separation Control measures to ensure that data collected for different purposes can be processed (storage, amendment, deletion, transmission) separately.

- All customer data is fully logically segregated by customer account. Data within a given account is only processed in accordance with the instructions from the relevant customer.

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

- All Heap employees are required to complete annual security & privacy and data-breach training. The staff that provide production system support completes annual incident-response drills to provide hands-on training experiences.
- All employees are also required to sign confidentiality agreements upon hire.
- The logical separation of data by customer account also supports that any support actions taken under instruction from the customer are isolated to the data belonging to that customer only.

Integrity

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

- Heap operates its production system so that operational access is only supported through a secured VPN and AWS Systems Manager. Only systems that need to serve customer or end-user traffic are configured to be exposed to the internet, and only allow access via HTTP(S) protocols.
- All data is end-to-end encrypted in-transit to Heap's internet-facing APIs and the web application using TLS 1.2 or higher. Data at rest is secured with SSE-S3 using AES-256.

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

- Data input into the Heap platform is generally auto-tracking data produced by visitors and users of the customer's platform. The intrinsic purpose of the platform is to analyze aggregate data, regardless of whether the captured data might include identifying details.
- All operational access to the production system is logged and tracked via AWS CloudTrail and secured in a secondary read-only audit account so it cannot be tampered with.

Availability and Resilience of Processing Systems and Services

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

- Heap is built on top of AWS; we have redundancy in critical systems and capacity for rapidly scaling user volume.
- The main data storage cluster operates in a sharded redundant RF=2 mode, meaning single-server outages do not lead to data unavailability.
- We also operate continuous backups--Database backups that cannot be deleted with any credentials that are stored in our codebase or on any Elastic Compute Cloud (EC2) instance. Data in backups is encrypted. Backups can only be manually interacted with by a small select group of engineers using a two-factor authenticated login to the Heap AWS account. Data is destroyed when no longer required or upon termination of account

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

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

- The data storage cluster uses a cell architecture that is resilient against single-node failures per cell through data replication. Failed nodes can be restored from continuous backups and brought back to full point-in-time recovery. Even if two nodes fail in a single cell, data will only temporarily be partially unavailable until both nodes can be restored from backup.

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

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

- Regarding data availability, redundant nodes in our data cluster fail in production on a regular basis, and data restoration is a routinely exercised and automated operation.

Additional technical and organisational measures

The following additional technical and organisational measures will be implemented:

- Heap does annual SOC2 Type II audits and undergoes HIPAA and GDPR evaluations on a periodic basis.
- Heap does not process any data exceeding the requirements of the customer (Controller).
- All data held for a customer is purged in accordance with our data retention policies and will, upon written request, be made available as a one-time export upon termination before deletion.

Description of the specific technical and organisational measures to be taken by the to assist with the fulfilment of data subject requests (Clause 10 (b) SCC)

In order to for the data importer / Heap to assist the data exporter / Customer with fulfilling its obligations to respond to data subjects' requests in accordance with Clause 10 (b) SCC, the Parties will set out the appropriate technical and organisational measures in the following, 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: The User Deletion API, which you can use to delete users and their personal data from your Heap account. We also offer an in-app user data deletion request tool, and you can delete user data via Postman.

Any data access or modification requests are directed to the Customer who is the controller of this data.

Technical and Organisational Security Measures in relation to special categories of data (where applicable) (Appendix, Annex I B. SCC; Schedule 3)

If special categories of personal are processed as outlined in the DPA, the 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 are: N/A

SCHEDULE 3

UK AND SWISS ADDENDUM

1. UK ADDENDUM

In respect of Restricted Transfers subject to the UK GDPR, the Parties agree that the Standard Contractual Clauses shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018, as amended or replaced from time to time ("UK IDTA"), and the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is as set forth below:

1.1 Table 1 – the Parties are Heap and Customer, with contact details as set forth in Schedule 1 to this DPA.
1.2 Table 2 – the Approved EU Standard Contractual Clauses with optional provisions as set forth in Section 2.2.
1.3 Table 3 – the Annexes are deemed completed with the relevant information contained in the Schedules to this DPA.
1.4 Table 4 – neither Party has the right of termination set forth in Section 19 of the UK IDTA.

2. SWISS ADDENDUM

As stipulated in clause 3.1(b) of the DPA, this Swiss Addendum shall apply to any processing of Customer Personal Data subject to Swiss data protection law or to both Swiss data protection law and the GDPR.

2.1 Interpretation of this Addendum

(a) Where this Addendum uses terms that are defined in the Standard Contractual Clauses Module 2 (Controller to Processor) and Module 3 (Processor to Processor), those terms shall have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses
Clauses	The Standard Contractual Clauses Module 2 (Controller to Processor) and Module 3 (Processor to Processor).
Swiss Data Protection Laws	The Swiss Federal Act on Data Protection of 19 June 1992 and the Swiss Ordinance to the Swiss Federal Act on Data Protection of 14 June 1993, and any new or revised version of these laws that may enter into force from time to time.

(b) This Addendum shall be read and interpreted in the light of the provisions of Swiss Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

(c) This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

(d) Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

2.2 Hierarchy

In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

2.3 Incorporation of the Clauses

(a) In relation to any processing of personal data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends the DPA to the extent necessary so they operate:

(i) for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws or Swiss Data Protection Laws and the GDPR apply to the data exporter's processing when making that transfer; and

(ii) to provide appropriate safeguards for the transfers in accordance with Article 46 of the GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

(b) To the extent that any processing of personal data is exclusively subject to Swiss Data Protection Laws, the amendments to the DPA including the SCCs, as required by clause 2.1 of this Swiss Addendum, include (without limitation):

(i) References to the "Clauses" or the "SCCs" means this Swiss Addendum as it amends the SCCs.

(ii) Clause 6 Description of the transfer(s) is replaced with:

"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 those specified in Schedule 1 of this DPA where Swiss Data Protection Laws apply to the data exporter's processing when making that transfer."

(iii) References to "Regulation (EU) 2016/679" or "that Regulation" or ""GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws extent applicable.

(iv) References to Regulation (EU) 2018/1725 are removed.

(v) References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".

(vi) Clause 13(a) and Part C of Annex I of the SCCs are not used; the "competent supervisory authority" is the Federal Data Protection and Information Commissioner (the "FDPIC") insofar as the transfers are governed by Swiss Data Protection Laws;

(vii) Clause 17 is replaced to state

"These Clauses are governed by the laws of Switzerland insofar as the transfers are governed by Swiss Data Protection Laws".

(viii) Clause 18 is replaced to state:

"Any dispute arising from these Clauses relating to Swiss Data Protection Laws shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts."

Until the entry into force of the revised Swiss Data Protection Laws, the Clauses shall also protect personal data of legal entities and legal entities shall receive the same protection under the Clauses as natural persons.

2.4 To the extent that any processing of personal data is subject to both Swiss Data Protection Laws and the GDPR, the DPA including the Clauses will apply (i) as is and (ii) additionally, to the extent that a transfer is subject to Swiss Data Protection Laws, as amended by clauses 2.1 and 2.3 of this Swiss Addendum, with the sole exception that Clause 17 of the SCCs shall not be replaced as stipulated under clause 2.3(b)(vii) of this Swiss Addendum.

2.5 Customer warrants that it and/or Customer Affiliates have made any notifications to the FDPIC which are required under Swiss Data Protection Laws.

Dropbox Sign

Audit trail

Title	Heap DPA
File name	Heap Revised DPA_ Dec. 2022.docx
Document ID	aaa3091aa1980e4693955939940156077 9cfc74c
Audit trail date format	MM / DD / YYYY
Status	● Signed

Document History

SENT	**01 / 05 / 2023** 09:59:35 UTC-8	Sent for signature to Kate Helin (kate.helin@heapanalytics.com) from kate.helin@heapanalytics.com IP: 136.56.44.77
VIEWED	**01 / 05 / 2023** 10:08:46 UTC-8	Viewed by Kate Helin (kate.helin@heapanalytics.com) IP: 136.56.44.77
SIGNED	**01 / 05 / 2023** 10:09:40 UTC-8	Signed by Kate Helin (kate.helin@heapanalytics.com) IP: 136.56.44.77
COMPLETED	**01 / 05 / 2023** 10:09:40 UTC-8	The document has been completed.