



## DATA PROCESSING ADDENDUM

*(Revision September 2024)*

This Data Processing Addendum, including its Schedules, (“DPA”) forms part of the Master Services Agreement between Heystack and Customer for the purchase of Professional Services from Heystack (the “Agreement”) to reflect the Parties’ agreement with regard to the Processing of Personal Data or other agreement which references this DPA.

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

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

### 1. DEFINITIONS

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

“**Approved Sub-processors**” means (a) Heystack’s Affiliates; and (b) third-party Processors engaged by Heystack and Heystack’s Affiliates that may process Personal Data as part of providing Professional Services, as agreed to by Customer in writing, including in the applicable SOW(s).

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

“**Customer**” means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed an SOW. For the purposes of this DPA only, and except where indicated otherwise, the term “Customer” shall include Customer and its Authorized Affiliates.

“**Data Protection Laws and Regulations**” means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including those of the United Kingdom, the European Union and their member states.

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

“**Non-Heystack Processors**” means third-party software programs and subcontractors that are not provided or engaged by Heystack as Approved Sub-processors, and that Heystack uses at Customer’s instruction or with Customer’s consent.

“**Personal Data**” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as Personal Data or personally identifiable information under applicable Data Protection Laws and Regulations), and where for each of (i) or (ii), such data is provided by or for Customer to Heystack as a Processor in order to perform the Professional Services pursuant to an Agreement. Personal Data excludes information processed by Non-Heystack Processors.

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

“**Processor**” means the entity which Processes Personal Data on behalf of the Controller.

“**Professional Services**” means the support, implementation, training, and consultancy services Heystack provides to Customer under the Agreement, as identified in the SOW.

“**Professional Services Data**” means electronic data constituting Confidential Information, including Personal Data, provided by or for Customer to Heystack as part of Professional Services.

“**Security and Privacy Documentation**” means the Security and Privacy Documentation applicable to the specific

Professional Services purchased by Customer, as updated from time to time, and accessible via Heystack's Legal webpage at <https://www.heystack.cx/legal> or as otherwise made reasonably available by Heystack.

**"Sensitive Personal Data"** means any Personal Data that is deemed sensitive or special under applicable Data Protection Laws and Regulations, including but not limited to, personal information related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, genetic data, biometric data, and financial data (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers).

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

## 2. PROCESSING OF PERSONAL DATA

- 2.1. **Customer's Processing of Personal Data.** Customer as a Controller or Processor shall Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations (including where the Customer is a Processor, by ensuring that the ultimate Controller does so), including (a) meeting any applicable requirement(s) to provide notice to Data Subjects of Customer's use of Heystack as Processor; (b) complying with applicable data subject rights; and (c) ensuring Customer's use of the Professional Services complies with any obligations of Customer related to the Processing of Sensitive Personal Data. Customer's instructions to SFDC for Processing Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data, including the means by which it was collected and shared with SFDC. Customer specifically acknowledges and agrees that its use of the Professional Services will not violate the rights of any Data Subject, including those that have opted-out from sales or other disclosures of Personal Data, to the extent applicable under Data Protection Laws and Regulations.
- 2.2. **Heystack's Processing of Personal Data.** Heystack shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable SOW(s) and (ii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.
- 2.3. **Details of the Processing.** The subject-matter of Processing of Personal Data by Heystack is the performance of the Professional Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 - Details of the Processing to this DPA.
- 2.4. **Customer Instructions.** Heystack shall inform Customer immediately (i) if, in its opinion, an instruction from Customer constitutes a breach of the UK GDPR and/or (ii) if Heystack is unable to follow Customer's instructions for the Processing of Personal Data.
- 2.5. **UK GDPR.** Heystack will Process Personal Data in accordance with the UK GDPR requirements directly applicable to Heystack's provision of its Professional Services.

## 3. RIGHTS OF DATA SUBJECTS

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

## 4. HEYSTACK PERSONNEL

- 4.1. **Confidentiality.** Heystack shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and have executed written confidentiality agreements. Heystack shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

- 4.2. **Reliability.** Heystack shall take commercially reasonable steps to ensure the reliability of any Heystack personnel engaged in the Processing of Personal Data.
- 4.3. **Limitation of Access.** Heystack shall ensure that Heystack’s access to Personal Data is limited to those personnel performing Professional Services in accordance with the Agreement.

## 5. SUB-PROCESSORS

- 5.1. **Use of Approved Sub-processors.** Customer acknowledges and agrees that Heystack may engage Approved Sub-processors to provide Professional Services as agreed to by Customer in writing. Heystack or an Heystack Affiliate has entered into a written agreement with each Approved Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Professional Services provided by such Approved Sub-processor.
- 5.2. **Liability.** Heystack shall be liable for the acts and omissions of its Approved Sub-processors to the same extent Heystack would be liable if performing the Professional Services of each Approved Sub-processor directly under the terms of this DPA, unless otherwise set forth in the Agreement.
- 5.3. **Non-Heystack Processors.** Heystack may use Non-Heystack Processors in connection with the provision of Professional Services as agreed to by Customer in writing (email acceptable).

## 6. SECURITY

- 6.1. **Controls for the Protection of Personal Data.** Heystack shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data as set forth in the Professional Services Security and Privacy Documentation. Heystack will not materially decrease the overall security provided during an SOW.
- 6.2. **Audit Program.** During the duration of an SOW, upon Customer’s reasonable written request, and subject to the confidentiality obligations set forth in the Agreement, Heystack shall make available to Customer information regarding Heystack’s compliance with the obligations set forth in this DPA, including those obligations required by applicable Data Protection Laws and Regulations.
- 6.3. **Data Protection Impact Assessment.** Upon Customer’s request, Heystack shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer’s obligation under Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer’s use of the Professional Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Heystack.

## 7. DATA INCIDENT NOTIFICATION

- 7.1. **Heystack responsibilities.** Heystack shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Professional Services Data, including Personal Data, transmitted, stored or otherwise Processed by Heystack or its Sub-processors of which Heystack becomes aware (a “Data Incident”). Heystack shall make reasonable efforts to identify the cause of such Data Incident and take such steps as Heystack deems necessary and reasonable to remediate the cause of such a Data Incident to the extent the remediation is within Heystack’s reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer’s Users.
- 7.2. **Customer responsibilities.** If required under Data Protection Laws and Regulations, Customer shall notify Data Incident to the relevant authorities or Data Subjects in accordance with the Data Protection Laws and Regulations.

## 8. RETURN AND DELETION OF PERSONAL DATA

Excluding any Personal Data that may have, at Customer’s instruction, been submitted to the online services, upon request by Customer after the effective date of termination or expiration of the relevant SOW (the “Expiration Date”), Heystack will make the Personal Data in its possession or control available to Customer, to the extent applicable, for return, export or download for a period of 10 days after the Expiration Date. Heystack will otherwise have no obligation to maintain any Personal Data. Please note that Heystack may not always know whether Customer wishes to have its data deleted after termination or retained for use in a future Professional Services engagement. If Customer does not expect to ask Heystack to Process its Personal Data further, it should inform Heystack, and at the Customer’s instruction Heystack will delete Personal Data in its possession or control, unless legally prohibited. Until Personal Data is deleted or returned, Heystack shall continue to comply with this DPA and its Schedules.

## 9. DATA TRANSFERS

Heystack shall ensure that the transfer of Personal Data which are undergoing Processing or are intended for Processing after transfer to a third country shall take place only if such transfer meets the conditions outlined in the GDPR, specifically Chapter V.

## 10. AUTHORIZED AFFILIATES

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

**10.3.1** Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Heystack directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA, not separately for each Authorized Affiliate individually, but in a combined manner for itself and all of its Authorized Affiliates together (as set forth, for example, in section 10.3.2, below).

**10.3.2** The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an onsite audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Heystack and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

## 11. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Heystack, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, Heystack's and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

### List of Schedules

Schedule 1: Details of the Processing

## **SCHEDULE 1 - DETAILS OF THE PROCESSING**

### **Nature and Purpose of Processing**

Heystack will Process Personal Data as necessary to perform the Professional Services pursuant to the Agreement, as can be further specified in the Security and Privacy Documentation, and as further instructed by Customer in its use of the Professional Services.

### **Duration of Processing**

Subject to Section 8 of the DPA, Heystack will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

### **Categories of Data Subjects**

Customer may provide Personal Data to Heystack in order for Heystack to perform the Professional Services pursuant to an Agreement, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Users of online services authorized by Customer

### **Type of Personal Data**

Customer may provide Personal Data to Heystack in order for Heystack to perform the Professional Services pursuant to an Agreement, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

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