Data Processing Agreement

Between

CLIENT_NAME

and

HeroBase A/S

(collectively the "Parties" and individually the "Party")

CLIENT_NAME
CLIENT_ADDRESS
CLIENT_ZIP AND CITY
CVR no.: xx xx xx xx
(the "Data Controller")

and

HeroBase A/S
Tobaksvejen 25, 2.
DK-2860 Søborg
CVR no.: 31073103
(the "Data Processor")

have concluded this Data Processing Agreement (the "Agreement") on the Data Processor's processing of personal data on behalf of the Data Controller.

1. The processed personal data

1.1 This Agreement has been entered into in connection with the Parties' execution of the "Contract regarding use of Hero Outbound and/or Hero Flows and/or Hero Payments" Agreement effective from SERVICE_START_DATE, including terms and conditions (appendix to the contract).

"Personal data" means personal data as defined in 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 as applicable as of 25 May 2018, as may be amended from time to time, in the following referred to as "the General Data Protection Regulation (GDPR)".

1.2 The Data Processor can process the following types of personal data on behalf of the Data Controller:

- Core data on individuals, in terms of name, address, telephone number(s), e-mail address(es) etc., typically classified as non-sensitive data, belonging to the Data Controller
- Additional data used for segmentation and targeting purposes, uploaded to the system "Hero Outbound" and/or the tool "Hero Flows" by the Data Controller, which could be classified as sensitive data, belonging to the Data Controller
- Additional data used for order handling and back-office processes within the Data Controller, collected from the individuals as part of the telemarketing and sales process, which could be classified as sensitive data, belonging to the Data Controller

For all data types mentioned above, applies that data has been uploaded to the tool "Hero Outbound" and/or the tool “Hero Flows” by the Data Controller, or collected from individuals and entered in the tool "Hero Outbound" and/or the tool “Hero Flows” by the Data Controller. The tool "Hero Outbound" and/or the tool “Hero Flows” allows users to upload, enter and edit all types of data to and within columns and fields defined by the users. Hence it is all up to the users of the tool "Hero Outbound" and/or the tool “Hero Flows”, in this case users from the Data Controller, to utilize this functionality and work with the data. The Data Processor protects and processes the data as stated in this agreement, but all decisions regarding which data has been uploaded, entered and edited are solely made by the Data Controller.

2. Data which is intended to upload to, and process/handle in, “Hero Outbound”, “Hero Flows” and/or “Hero Payments”

2.1 The Data Controller intends to upload, process and handle the following data types in “Hero Outbound” and/or “Hero Flows”. Note that there are two ways to provide this information, which is a formal part of this Data Processing Agreement. The information can either be stated by marking the (up to all) fields in section 2.2. Alternatively, the information (in similar format) can be written into the contract “Contract regarding use of Hero Outbound and/or Hero Flows and/or Hero Payments” Agreement effective from SERVICE_START_DATE. If the latter is chosen, it must be stated clearly in section 2.2.

2.2 Referring to above section 2.1, data types processed must be stated here (check the boxes).

☐ GDPR Article 6 data
(regular personal data, for example: name, address, phone number, economical data, social status etc.)

☐ GDPR Article 9 data
(sensitive personal data, for example: Union membership, ethnical origin, political standpoint, sexual orientation etc.)

If any GDPR Article 9 data: Please select which types below (one or more):

- ☐ GDPR Article 9 data, Union membership
- ☐ GDPR Article 9 data, Ethnical origin or Race
- ☐ GDPR Article 9 data, Political standpoint
- ☐ GDPR Article 9 data, Religious standpoint
- ☐ GDPR Article 9 data, Philosophical standpoint
- ☐ GDPR Article 9 data, Health data, Health information
- ☐ GDPR Article 9 data, Biometric data with purpose of identification
- ☐ GDPR Article 9 data, Sexual orientation
- ☐ GDPR Article 9 data, None of the above, but other sensitive data

☐ GDPR Article 10 data
(criminal convictions and offenses)

If any GDPR Article 10 data: Please select which types below (one or more):
- ☐ GDPR Article 10 data, Criminal offenses
- ☐ GDPR Article 10 data, Criminal convictions

☐ GDPR Article 87 data
(social security number)

2.3 The Data Controller will be using the following tools from the Data Processor. State which by marking the (up to all) fields in this section 2.3.

☐ Hero Outbound

☐ Hero Flows

☐ Hero Payments

3. Purpose

3.1 The Data Processor may only process personal data for purposes which are necessary in order to deliver the services in the "Contract regarding use of Hero Outbound and/or Hero Flows and/or Hero Payments" Agreement effective from SERVICE_START_DATE.

4. Obligations of the Data Processor

4.1 All processing by the Data Processor of the personal data provided by the Data Controller must be in accordance with instructions prepared by the Data Controller, and the Data Processor is, furthermore, obliged to comply with any and all data protection legislation in force from time to time. The Data Processor acts on instructions supplied by the Data Controller only. If no other instructions are explicitly supplied in writing, the default instructions are considered as section 3.1 in addition to the document "*Hero Outbound Platform Security & Data Privacy*" found on the webpage of the Data Processor. The direct link to the particular sub-page with the document is: https://herobase.com/legal-documents/.

4.2 The Data Processor must take all necessary technical and organisational security measures, including any additional measures, required to ensure that the personal data

specified in clause 1.2 and 2.2 is not accidentally or unlawfully destroyed, lost or impaired or brought to the knowledge of unauthorised third parties, abused or otherwise processed in a manner which is contrary to the Danish Act on the Processing of Personal Data (*lov om behandling af personoplysninger*), and the General Data Protection Regulation (GDPR). Thus, the Data Processor must, among other things,

- introduce login and password procedures and set up and maintain a firewall and antivirus software
- ensure that only employees with a work related purpose have access to the personal data
- store data storage media securely so that it is not accessible to third parties
- ensure that buildings and systems used for data processing are secure and that only high-quality hardware and software, which is regularly updated is used
- ensure that tests and waste material are destroyed in accordance with data protection requirements on the specific instruction of the Data Controller. In particular cases, to be determined by the Data Controller, such tests and waste material must be stored or returned
- ensure that employees receive proper training, adequate instructions and guidelines on the processing of the personal data. The Data Processor must ensure that the employees involved with the processing of the personal data are familiar with the security requirements.
- inform the Data Controller upon a breach or leak of the Data Controller's data, or suspicions hereof, via e-mail to the named contact person of the Data Controller stored in the Data Processor's CRM system. The notification must comply with the applicable legal requirements, but must at least contain: (a) description of the nature of the breach of personal data security, including the categories and number of data subjects involved, as well as the categories and number of registrations concerned; (b) contact information where further information can be obtained; (c) description of the likely consequences of the breach of personal data security; and (d) description of the measures proposed or implemented by the Data Processor in order to limit its possible harmful effects.
- ensure that employees act under professional secrecy regarding matters between the Data Processor and the Data Controller

4.3 If the Data Processor processes personal data in another EU/EEA member state other than Denmark, the Data Processor must comply with any and all legislation concerning security measures in that member state.

4.4 The Data Processor must notify the Data Controller where there is an interruption in operation, a suspicion that data protection rules have been breached or other irregularities in connection with the processing of the personal data occur.

4.5 Upon the request of the Data Controller, the Data Processor must provide the Data Controller with sufficient information for the latter to be able to ensure that the Data Processor has taken the necessary technical and organisational security measures. Further, the Data Controller is entitled, at its own expense, to have the Data Processor's processing of personal data inspected and audited annually by Data Controller and/or an independent third party.

4.6 If the Data Processor, receives a request for access to the registered personal data from a data subject or his agent, the Data Processor must immediately send such request to the Data Controller, for the Data Processor's further processing thereof, unless the Data Processor is entitled to handle such request itself.

5. Transfer of data to other data processors or third parties

5.1 The Data Processor is only entitled to transfer the personal data stipulated in clause 1.2 and 2.2 to other data processors or third parties in circumstances where it falls within the instructions stating how the Data Processor should process data on behalf of the Data Controller. The Data Processor is not entitled to disclose or hand over personal data to any other third parties or data processors without the prior written instruction of the Data Controller, unless such disclosure or handover is stipulated by law. The sub-data processors of the Data Processor, which are needed to provide the services to the Data Controller, and which are therefore approved by the Data Controller, can always be found on the webpage of the Data Processor. The direct link to the particular sub-page with list of sub-data processors is: https://herobase.com/sub-data-processors/.

5.2 Before transferring personal data to another data processor (sub-supplier), the Data Processor must ensure that such data processor has executed a data processing agreement in which the data processor undertakes vis-à-vis the Data Processor to be bound by back-to-back terms with respect to the security requirements under this Agreement.

5.3 If the data is transferred to foreign data processors, it must, in the said data processing agreement, be stated that the data protection legislation applicable in the Data Controller's country applies to foreign data processors. Furthermore, if the receiving data processor is established within the EU, it must be stated in the said data processing agreement that the receiving EU country's specific statutory requirements regarding data processors, e.g. concerning demands for notification to national authorities, must be complied with.

6. Amendments

6.1 In the event of amendments to the Danish data protection legislation, the Data Controller is entitled to amend the instructions set out in this Agreement on the giving of 2 (two) weeks' written notice when forwarding the new written instructions to the Data Processor. The Data Processor must however, at all times, comply with the applicable legislation on the protection of personal data.

7. Breach

7.1 Conditions related to the Data Processor's breach of this Agreement are defined in the "Contract regarding use of Hero Outbound and/or Hero Flows and/or Hero Payments" Agreement effective from SERVICE_START_DATE.

8. Effective date and termination

8.1 This Agreement becomes effective on the signature of the "Contract regarding use of Hero Outbound and/or Hero Flows and/or Hero Payments" Agreement effective from SERVICE_START_DATE.

8.2 Termination of the separately concluded "Contract regarding use of Hero Outbound and/or Hero Flows and/or Hero Payments" Agreement effective from SERVICE_START_DATE, between the Data Controller and the Data Processor will result in the termination of this Agreement. However, the Data Processor remains subject to the obligations stipulated in this Agreement, as long as the Data Processor processes personal data on behalf of the Data Controller.

8.3 In the event of the termination of the Agreement, the Data Controller is entitled to determine the media format to be used by the Data Processor when returning the personal data and to determine if personal data should instead be deleted.

9. Approval and Effectuation

9.1 This Agreement is concluded along with the "Contract regarding use of Hero Outbound and/or Hero Flows and/or Hero Payments" Agreement effective from SERVICE_START_DATE.