## DATA PROCESSING AGREEMENT

This Data Processing Agreement (the “DPA”) describes specific terms in respect of the processing of Personal Data by Ambassify to the Customer in connection with the provision of Services under the Agreement, the terms of which are incorporated herein by reference. $sourcefile$

### DEFINITIONS

For the purpose of this DPA, the following terms will have the following meaning. In case of any doubt or differences with the terms defined in the Data Protection Legislation, the definitions stipulated in the relevant Data Protection Legislation will prevail.

|  |  |
| --- | --- |
| **“Contact Person”** | means the individual(s) assigned by a Party and communicated to the other Party as point of contact and representing the Party for (a part of) the Services; |
| **“Data Controller”** | means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data; |
| **“Data Processor”** | means a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the Data Controller; |
| **“Data Protection Legislation”** | means the EU Regulation 2016/679 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), together with the codes of practice, codes of conduct, regulatory guidance and standard clauses and other related legislation resulting from such Directive or Regulation, as updated from time to time; |
| **“Data Subject”** | means an identified or identifiable natural person to whom the Personal Data relates. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. The relevant categories of Data Subjects are identified in Schedule 1; |
| **“Personal Data”** | means any information relating to a Data Subject. The relevant categories of Personal Data that are provided to Ambassify by, or on behalf of the Customer are identified in Schedule 1; |
| **“Personal Data Breach”** | means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed in connection with the provisioning of the Services; |
| **“Processing”, “Process(es)” or “Processed”** | means any operation or set of operations which is performed upon Personal Data or on sets of 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; |
| **“Services”** | means all services, functions, responsibilities and outputs of Ambassify as described in the Agreement; |
| **“Standard Contractual Clauses”** | means the standard contractual clauses of which the European Commission on the basis of Article 26 (4) of Directive 95/46/EC decided that these offer sufficient safeguards for the transfers of personal data to a third country, or the data protection clauses adopted by the European Commission or by a supervisory authority and approved by the European Commission in accordance with the examination procedure referred to in Article 93(2) of EU Regulation 2016/679. In the event of any such data protection clauses adopted in accordance with EU Regulation 2016/679, such clauses will prevail over any standard contractual clauses adopted on the basis of Directive 95/46/EC to the extent that they intend to cover the same kind of data transfer relationship; and |
| **“Sub-processor”** | means any subcontractor engaged by Ambassify to perform a part of the Services and who agrees to receive Personal Data intended for Processing on behalf of the Customer in accordance with the Customer’s instructions and the provisions of the Agreement. |

### INTERPRETATION

* 1. This DPA forms an integral part of the Agreement. The provisions of the Agreement therefore apply to this DPA. All capitalized terms not defined in this DPA will have the meaning set forth in the Agreement.
  2. In case of conflict between any provision in this DPA and any provision of another part of the Agreement, this DPA will prevail.

### SCOPE AND PURPOSE

* 1. In connection with and for the purpose of the performance of the Services under the Agreement, the Customer commissions Ambassify to process Personal Data in accordance with the provisions of this DPA.

### SPECIFICATION OF THE DATA PROCESSING AGREEMENT

* 1. Any Processing of Personal Data under the Agreement will be performed in accordance with the applicable Data Protection Legislation.
  2. For the performance of the Services, Ambassify is a Data Processor acting on behalf of the Customer. As a Data Processor, Ambassify will only act upon the Customer’s instructions. The Agreement, including this DPA, is the Customer’s complete instruction to Ambassify with regard to the Processing of Personal Data. Any additional or alternate instructions must be jointly agreed by the Parties in writing. The following is deemed an instruction by Ambassify to Process Personal Data: (1) Processing in accordance with the Agreement and (2) Processing initiated by the Customer’s users in their use of the Services.
  3. A more detailed description of the subject matter of the Processing of Personal Data in terms of the concerned categories of Personal Data and of Data Subjects (envisaged Processing of Personal Data) is contained in Schedule 1 hereto.

### DATA SUBJECTS’ RIGHTS

* 1. With regard to the protection of Data Subjects’ rights pursuant to the applicable Data Protection Legislation, the Customer will facilitate the exercise of Data Subject rights and will ensure that adequate information is provided to Data Subjects about the Processing hereunder in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
  2. Should a Data Subject directly contact Ambassify wanting to exercise his individual rights such as requesting a copy, correction or deletion of his data or wanting to restrict or object to the Processing activities, Ambassify will inform the Customer of such request within five (5) business days and provide the Customer with full details thereof, together with a copy of the Personal Data held by it in relation to the Data Subject where relevant. Ambassify will promptly direct such Data Subject to the Customer. In support of the above, Ambassify may provide the Customer’s basic contact information to the requestor. The Customer agrees to answer to and comply with any such request of a Data Subject in line with the provisions of the applicable Data Protection Legislation.
  3. Insofar as this is possible, Ambassify will cooperate with and assist the Customer by appropriate technical and organizational measures for the fulfilment of the Customer’s obligation to respond to requests from Data Subjects exercising their rights.

### CONSULTATION AND CORRECTION OF PERSONAL DATA

* 1. Ambassify will provide the Customer, in its role of Data Controller with access to Personal Data Processed under the Agreement, in order to allow the Customer to consult and correct such Personal Data.

### DISCLOSURE

* 1. Ambassify will not disclose Personal Data to any third party, except (1) as the Customer directs, (2) as stipulated in the Agreement, (3) as required for Processing by approved Sub-processors in accordance with Article 10 of this DPA or (4) as required by law, in which case Ambassify will inform the Customer of that legal requirement before Processing that Personal Data, unless that law prohibits such information being provided on important grounds of public interest.
  2. Ambassify represents and warrants that persons acting on behalf of Ambassify and who are authorized to Process Personal Data or to support and manage the systems that Process Personal Data (i) have committed themselves to maintain the security and confidentiality of Personal Data in accordance with the provisions of this DPA, (ii) are subject to user authentication and log on processes when accessing the Personal Data and (iii) have undertaken appropriate training in relation to Data Protection Legislation. Ambassify will inform the persons acting on its behalf about the applicable requirements and ensure their compliance with such requirements through contractual or statutory confidentiality obligations.

### DELETION AND RETURN OF PERSONAL DATA

* 1. At the latest within thirty (30) calendar days upon termination of the Agreement, Ambassify will sanitize or destroy any Personal Data that it stores in a secure way that ensures that all Personal Data is deleted and unrecoverable. Data used to verify proper data processing in compliance with the assignment and data that needs to be kept to comply with relevant legal and regulatory retention requirements may be kept by Ambassify beyond termination or expiry of the Agreement only as long as required by such laws or regulations.
  2. Upon written request submitted by the Customer no later than five (5) calendar days prior to termination of the Agreement, Ambassify will provide the Customer with a readable and usable copy of the Personal Data and/or the systems containing Personal Data prior to sanitization or destruction.

### LOCATION OF PROCESSING

* 1. Ambassify will store Personal Data at rest within the territory of the European Union.
  2. Any Processing of Personal Data by Ambassify personnel or subcontractors not located within the European Union may be undertaken only following prior written approval of the Customer and the execution of one of the then legally recognized data transfer mechanisms, such as an additional DPA governed by the Standard Contractual Clauses.

### USE OF SUB-PROCESSORS

* 1. The Customer acknowledges and expressly agrees that Ambassify may use third party Sub-processors for the provision of the Services as described in the Agreement.
  2. Any such Sub-processors that provide services for Ambassify and thereto Process Personal Data will be permitted to Process Personal Data only to deliver the services Ambassify has entrusted them with and will be prohibited from Processing such Personal Data for any other purpose. Ambassify remains fully responsible for any such Sub-processor’s compliance with Ambassify’s obligations under the Agreement, including this DPA. Ambassify will, prior to the entrusting of services to such Sub-processor, carry out any relevant due diligence on such Sub-processor to assess whether it is capable of providing the level of protection for the Personal Data as is required by this DPA, and provide evidence of such due diligence to the Customer where requested by the Customer or a regulator.
  3. Ambassify will enter into written agreements with any such Sub-processor which contain obligations no less protective than those contained in this DPA, including the obligations imposed by the Standard Contractual Clauses, as applicable.
  4. Ambassify will make available to the Customer the current list of Sub-processors for the Services identified in Schedule 2 that to this DPA. Such Sub-processors list will include the identities of those Sub-processors and their country of location. Ambassify will provide the Customer with a notification of a new Sub-processor before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the Services under this DPA.
  5. If the Customer objects to the use of a new Sub-processor that will be processing the Customer’s Personal Data, then the Customer will notify Ambassify in writing within fourteen (14) calendar days after receipt of Ambassify’s written request to that effect. In such a case, the Ambassify will use reasonable efforts to change the affected Services or to recommend a commercially reasonable change to the Customer’s use of the affected Services to avoid the Processing of Personal Data by the Sub-processor concerned. If the Ambassify is unable to make available or propose such change within sixty (60) calendar days, the Customer may terminate the relevant part of the Agreement regarding those Services which cannot be provided by the Ambassify without the use of the Sub-processor concerned. To that end, the Customer will provide a general written notice of termination that includes the reasonable motivation for non-approval.

### TECHNICAL AND ORGANIZATIONAL MEASURES

* 1. Ambassify has implemented and will maintain appropriate technical and organizational measures intended to protect Personal Data or the systems that Process Personal Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss or destruction. These measures will take into account and be appropriate to the state of the art, nature, scope, context and purposes of Processing and risk of harm which might result from unauthorized or unlawful Processing or accidental loss, destruction or damage to Personal Data. These measures will be specified in Schedule 3.3.
  2. Ambassify will adapt these measures systematically to the development of regulations, technology and other aspects and supplemented with the applicable technical and organizational measures of Sub-processors, as the case may be. In any event, the implemented technical and organizational measures will ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected, taking also into account the state of technology and the cost of their implementation.
  3. Upon the Customer’s request, Ambassify must provide the Customer within fourteen (14) calendar days of receipt by Ambassify of the Customer's request with an updated description of the implemented technical and organizational protection measures.

### PERSONAL DATA BREACHES

* 1. In the event of a (likely or known) Personal Data Breach and irrespective of its cause, Ambassify will notify the Customer without undue delay and at the latest within forty-eight (48) hours after having become aware of (the likelihood or occurrence of) such Personal Data Breach, providing the Customer with sufficient information and in a timescale, which allows the Customer to meet any obligations to report a Personal Data Breach under the Data Protection Legislation. Such notification will as a minimum specify:
* the nature of the Personal Data Breach;
* the nature or type of Personal Data implicated in the Personal Data Breach, as well as the categories and numbers of Data Subjects concerned;
* the likely consequences of the Personal Data Breach;
* as the case may be, the remedial actions taken or proposed to be taken to mitigate the effects and minimize any damage resulting from the Personal Data Breach;
* the identity and contact details of the Data Protection Officer or another Contact Person from whom more information can be obtained.
  1. Ambassify will without undue delay further investigate the Personal Data Breach and will keep the Customer informed of the progress of the investigation and take reasonable steps to further minimize the impact. Both Parties agree to fully cooperate with such investigation and to assist each other in complying with any notification requirements and procedures.
  2. A Party’s obligation to report or respond to a Personal Data Breach is not and will not be construed as an acknowledgement by that Party of any fault or liability with respect to the Personal Data Breach.

### CUSTOMER RESPONSABILITIES

* 1. The Customer will comply with all applicable laws and regulations, including the Data Protection Legislation.
  2. The Customer remains responsible for the lawfulness of the Processing of Personal Data including, where required, obtaining the consent of Data Subjects to the Processing of his or her Personal Data.
  3. The Customer will take reasonable steps to keep Personal Data up to date to ensure the data are not inaccurate or incomplete with regard to the purposes for which they are collected.
  4. With regard to components that Customer provides or controls, including but not limited to workstations connecting to Services, data transfer mechanisms used, and credentials issued to the Customer’s personnel, the Customer will implement and maintain the required technical and organizational measures for protection of Personal Data.

### NOTIFICATIONS

* 1. Unless legally prohibited from doing so, Ambassify will notify the Customer as soon as reasonably possible, and at the latest within two (2) business days of becoming aware of the relevant circumstances, if it or any of its Sub-processors:
     1. receives an inquiry, a subpoena or a request for inspection or audit from a competent public authority relating to the Processing;
     2. intends to disclose Personal Data to any competent public authority outside the scope of the Services of the Agreement. At the request of the Customer, Ambassify will provide a copy of the documents delivered to the competent authority to the Customer;
     3. receives an instruction that infringes the Data Protection Legislation or the obligations of this DPA.
  2. In this respect, Ambassify will co-operate as requested by the Customer to enable the Customer to comply with any assessment, enquiry, notice or investigation under the Data Protection Legislation, which will include the provision of:
     1. all data requested by the Customer (which is not otherwise available to the Customer) within the reasonable timescale specified by the Customer in each case, including full details and copies of the complaint, communication or request and any Personal Data it holds in relation to the relevant Data Subject(s); and
     2. where applicable, providing such assistance as is reasonably requested by the Customer to enable the Customer to comply with the relevant request within the Data Protection Legislation statutory timescales.
  3. Any notification under this DPA, including a Personal Data Breach notification, will be delivered to one or more of the Customer’s Contact Persons via email possibly supplemented by any other means Ambassify selects. Upon request of the Customer, Ambassify will provide the Customer with an overview of the contact information of the registered Customer’s Contact Persons. It is Customer’s sole responsibility to timely report any changes in contact information and to ensure the Customer’s Contact Persons maintain accurate contact information.

### TERM AND TERMINATION

* 1. This DPA enters into force on the date of its signing by all Parties and remains in force until Processing of Personal Data by Ambassify is no longer required in the framework of or pursuant to the Agreement.

**IN WITNESS WHEREOF**, the Parties have executed this Agreement on [EffectiveDate], in two (2) originals, each Party acknowledging receipt of one original.

|  |  |
| --- | --- |
| **On behalf of Ambassify**  **Ambassify NV**  Name:  Capacity: | **On behalf of the Customer**  **[Customer.Company]**  Name:  Capacity: |

**Schedules:**

1. Details of the Personal Data Processing;
2. List of current Sub-processors;
3. Technical and organisational measures.

### Schedule 1 - Details of the Personal Data Processing

|  |  |
| --- | --- |
| **Contact details of responsible for data protection and security** | **Controller:**  [Customer.DPO.Name] – [Customer.DPO.Phone] - [Customer.DPO.Email] (DPO)  [Customer.CISO.Name] – [Customer.CISO.Phone] - [Customer.CISO.Email] (CISO)  **Processor:**  Jorgen Evens – +32 496 62 96 82 - dpo@ambassify.com (DPO)  Wim Mostmans - +32 472 50 50 82 - security@ambassify.com (CISO) |
| **Object of Processing** | SAAS-SERVICES |
| **Purpose and means of Processing** | Setting up and managing marketing and communication campaigns. |
| **Categories of Personal Data being processed** | Minimaly required data categories   * passwords * unique identifier * name (first name, last name) * platform activity * preferred language * email address * email (communication) * notification (communication) * IP address * browser * Opt-in (compliance)   Optional data categories   * interests * profile picture * birth date * gender * text messages (communication) * employer * job titles * social unique identifier * number of connections * social access tokens * telephone number * physical address * country |
| **Categories of Data Subjects** | * Prospects * Clients * Suppliers * Employees |
| **Categories of Recipients** | Subcontractors |
| **Storage location** | EEA/outside EEA |
| **Storage period** | For the duration of the Agreement |
| **Transfer of Personal Data (outside the EEA)** | YES |

### Schedule 2 – List of current Sub-processors

|  |  |  |
| --- | --- | --- |
| **Name subprocessor** | **Nature of the processing** | **Country of processing** |
| **Amazon.com, Inc.** | * Storage * Application Processing * Content Delivery * Communication Delivery | * Germany * Ireland * Europe |
| **Salesforce.com, Inc.** | * Application Processing | * Ireland |
| **CloudFlare, Inc.** | * Content Delivery | * Global |
| **Redis Labs, Inc.** | * Storage | * Ireland |
| **Intercom, Inc.** | * Customer Support | * Ireland |
| **Planhat** | * Customer Support | * Ireland |
| **Twilio Inc.**  **(Optional - remove if text message addon is not requested)** | * Communication Delivery | * Germany |

### Schedule 3 – Technical and organisational measures

An overview of the security measures to be taken by the Processor as a minimum.

Checklist of technical security measures:

* Up-to-date virus scan, firewalls and Intrusion Detection Systems
* Password manager and unique login code and password which is changed regularly, and MFA enabled where available
* Encrypted e-mail
* No unsecured hard disks
* No unsecured backups
* Encryption of Personal Data both in transit and in rest
* Physical access security to rooms where Personal Data is processed/stored
* Logging and monitoring of all systems
* Pseudonimization or anonymization of data where possible

Checklist of organisational measures:

* Information policy to staff regarding privacy
* Training & awareness to staff
* Clean desk policy
* Policy on the use of company resources (laptops, phones, etc.)
* Procedure in case of incidents (data leak, etc.)
* Destroy old documents carefully
* Confidentiality clauses with employees
* Change management process (QA checks that include automated and manual security checks)
* No customer production data is used in staging environment
* Well defined roles
* Yearly security audit by external cybersecurity company
* Due diligence checks on processors
* Off-boarding process