

## **Data Processing Agreement (Buyers)**

### **Preamble**

This Data Processing Agreement ("**DPA**") specifies the data protection obligations and rights of the Parties in connection with the personal data processed by Choco as a processor on behalf of Buyer when providing the services ("**Services**") as per the agreement governing Buyer's use of the Choco App ("**Agreement**").

For the purposes of this DPA "**Data Protection Laws**" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of personal data, including: (i) EU Regulation 2016/679 ("**GDPR**"); (ii) GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) any laws or regulations ratifying, implementing, adopting, supplementing or replacing the GDPR; (iv) in the UK, the Data Protection Act 2018; (v) any laws and regulations implementing or made pursuant to EU Directive 2002/58/EC (as amended by 2009/136/EC); and (vi) in the UK, the Privacy and Electronic Communications (EC Directive) Regulations 2003; in each case, as updated, amended or replaced from time to time; and the terms "**data subject**", "**processing**", "**processor**" and "**controller**" shall have the meanings set out in the Data Protection Laws. "**Personal Data**" has the meaning set out in Data Protection Laws, but is limited to personal data processed by Choco acting as a processor on behalf of Buyer under this Agreement as further described in Annex 1.

### **1. Subject and Scope of the Assignment**

1.1 Choco shall process the Personal Data which Buyer has provided directly or indirectly for the provision of the Services exclusively on behalf of, and in accordance with, the instructions of Buyer, unless it is otherwise required by the applicable law. In such a case, Choco shall notify Buyer of such legal requirements prior to the processing, unless the relevant law prohibits such notification.

1.2 The processing of Personal Data by Choco on behalf of Buyer is specified in Annex 1 to this DPA. Buyer warrants and represents that it has obtained all necessary consents and complied with all obligations required by Data Protection Laws for transferring or otherwise making available any Personal Data to Choco under this Agreement.

1.3 Buyer may issue further instructions regarding the scope of processing of Personal Data. If Choco is of the opinion that a Buyer instruction violates this DPA or Data Protection Laws, then it shall without undue delay inform Buyer thereof in writing. Choco shall be entitled to suspend the execution of such instruction until Buyer confirms it in writing. If Buyer insists on the execution of an instruction despite the concerns raised by Choco, then Buyer shall indemnify Choco against all damages and costs that it incurred due to the execution of the Buyer's instruction. Choco shall inform Buyer of any damages asserted against it and any costs incurred by it and shall not acknowledge any claims of third parties without Buyer's consent and shall, at Choco's option, conduct the defense in consultation with Buyer or leave it to Buyer.

## **2. Requirements of Personnel**

Choco shall ensure that all persons who are authorized to have access to the Personal Data are under a contractual obligation to maintain confidentiality or are under an appropriate statutory obligation of confidentiality when processing the Personal Data.

## **3. Processing Security**

3.1 Choco shall implement and maintain throughout the term of the Agreement appropriate technical and organizational measures ("**TOM**") as specified in Annex 2 to ensure a level of protection of the Personal Data commensurate to the risk, taking into account the state of the art, the cost of implementation and, to the extent known to Choco, the nature, scope, circumstances and purposes of the processing of the Personal Data and the varying likelihood and severity of the risk to the rights and freedoms of the data subjects. Choco shall regularly assess the effectiveness of the TOM and implement alternative measures if necessary for ensuring appropriate level of security.

3.2 It shall be incumbent upon Buyer to review the TOM taken by Choco, particularly to review whether these measures are also sufficient with regard to circumstances of the data processing that are not known to Choco.

## **4. Use of Sub-Processors and Data Transfers**

4.1 Buyer generally authorizes Choco to make use of services of sub-processors when processing the Personal Data. The current sub-processors engaged by Choco are listed in Annex 3. Choco will impose on any sub-processor substantially similar data protection obligations which are no less protective than the ones set out under this DPA and will remain liable towards Buyer for its sub-processors' performance under this DPA to the extent Choco will be liable for its own performance.

4.2 Choco will update the list of sub-processors in Annex 3 at least 30 days before authorizing a new sub-processor to process Personal Data on behalf of Buyer and send a notice of that update. If Buyer wants to receive these updates, it shall sign up to the notification mechanism available in Annex 3. If Buyer does not object within 14 days following Choco's notification by sending an email to [legal@choco.com](mailto:legal@choco.com), then the engagement shall be deemed approved.

4.3 If Buyer objects, Choco shall be entitled, at its choice, to either provide its Services without using the rejected additional sub-processor or to terminate the Agreement.

4.4 Buyer authorizes Choco, its affiliates and its sub-processors to transfer, access or process the Personal Data outside the UK or the European Economic Area ("EEA"), provided that the requirements of transfer or engagement under Data Protection Laws are met.

## **5. Rights of the Data Subjects**

5.1 Taking into account the nature of the processing of the Personal Data, Choco shall assist Buyer with appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Buyer's obligation to respond to requests for exercising the data subject's rights laid down in the Data Protection Laws.

5.2 Choco shall in particular:

- a. inform Buyer without undue delay if a data subject contacts Choco directly with a request to exercise his/her rights;
- b. provide Buyer upon Buyer's request with all information available to Choco regarding the processing of the Personal Data that Buyer needs to respond to the request of a data subject and that Buyer does not have itself;
- c. correct, delete or restrict the processing of the Personal Data without undue delay upon the instruction of Buyer, unless Buyer is able to do so itself and it is technically possible for Choco to do so;
- d. support Buyer to the extent necessary to receive the Personal Data processed in Choco's sphere of responsibility - insofar as this is technically possible for Choco - in a structured, common and machine-readable format, insofar as a data subject asserts a right to data portability.

## **6. Support Obligations**

6.1 Choco shall notify Buyer without undue delay after becoming aware of a breach of Personal Data. The notification shall include a description, if possible, of the nature of the breach; the categories and approximate number of data subjects affected by the breach; the probable consequences of the breach; of the measures taken or proposed by Choco to remedy the breach of the protection of the Personal Data and, if applicable, measures to mitigate its possible adverse effects.

6.2 Choco shall investigate the cause of the breach and, where appropriate, take reasonable measures to mitigate its possible adverse effects.

6.3 If Buyer is obligated to inform the supervisory authorities and/or data subjects about the personal data breach, Choco shall assist the Buyer with complying with this obligation, taking into account the nature of processing and the information available to Choco. Any additional costs incurred by Choco in this context, which exceed statutory processor obligations under the applicable law, will be borne by Buyer.

6.4 Choco shall notify Buyer of any subpoena or other judicial or administrative order, process or proceeding seeking access to, or disclosure of, the Personal Data insofar as such notification is not prohibited by law. If Buyer is obliged to provide information to a supervisory authority regarding the processing of the Personal Data or to otherwise cooperate with such authorities, Choco shall support Buyer in providing such information insofar as Buyer does not have the information itself and reasonably cooperate with Buyer and with supervisory authorities, including granting the competent supervisory authority the necessary rights of access, information and inspection.

6.5 Choco shall provide reasonable assistance to Buyer regarding Buyer's compliance with its obligations related to security of processing, data protection impact assessments and prior consultations with the supervisory authorities in each case taking into account the nature of the processing and information available to Choco. Any additional costs incurred by Choco in this context, exceeding the foreseen statutory processor obligations under the applicable law, will be borne by Buyer.

## **7. Data Deletion and Return**

7.1 Upon termination of the Agreement and written request from Buyer, Choco will either delete or return Personal Data, unless Choco is obliged to continue storing the Personal Data under applicable law.

7.2 Some Personal Data may be archived in our back-up systems and such archived Personal Data will be deleted in accordance with Choco's retention policy. Any Personal Data archived in backups will be isolated and protected from any further processing. For the period that the data is stored after the termination of the Agreement, the rights and obligations of the Parties under this DPA shall continue to apply.

## **8. Verifications and Audits**

8.1 Choco shall keep records of its processing activities performed on behalf of Buyer and upon request, make available to Buyer these records or any other information necessary to demonstrate compliance with statutory processor obligations set out under the Data Protection Laws.

8.2 Choco shall allow for and contribute to audits, including on-site inspections, by Buyer or an auditor mandated by Buyer in relation to the processing of the Personal Data. The audits and on-site inspections should, as far as possible, not hinder Choco in its normal business operations and should not place an undue burden on Choco. In particular, on-site inspections at Choco for no specific reason should not take place more than once per calendar year and only during Choco's normal business hours. Buyer shall notify Choco of inspections in written or text form at least 30 (thirty) days in advance, providing Choco with information about the scope, duration, and inspection plan. Buyer and Choco shall cooperate in good faith and mutually agree on the scope, duration, and start date of the inspection. Any costs incurred by Choco for any on-site inspections which are not clearly disproportionate or excessive, will be borne by the Buyer. The auditor mandated by Buyer shall be an independent contractor which does not compete with Choco and such auditor shall enter into a non-disclosure agreement with Choco.

## **9. Miscellaneous**

9.1 Each Party's and their affiliates' liability taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability provisions of the Agreement.

9.2 This DPA, including its annexes, constitutes an integral part of the Agreement between Choco and Buyer. If there are any inconsistencies between this DPA and the provisions of the Agreement, the provisions of this DPA shall take precedence.

9.3 Amendments and side agreements to any parts of this DPA must be made in writing. This rule also applies to this written form requirement itself. The governing law and jurisdiction under the Agreement shall apply accordingly for any parts of this DPA.

## **Annex 1 - Description of Personal Data Processing**

<b>Purpose of data processing</b>	Provision of Choco App and associated services
<b>Nature and scope of data processing</b>	<p>Collection, processing, storage and transfer of Personal Data as necessary for:</p> <ul style="list-style-type: none"> <li>• Provision of Choco App, such as transmission of messages, orders and other communications between the Buyer and its Supplier via agreed methods</li> <li>• Provision of support services</li> <li>• Managing Buyer's enterprise account</li> <li>• Any other service agreed between the parties</li> </ul>
<b>Type of data</b>	<ul style="list-style-type: none"> <li>• Name</li> <li>• Email address</li> <li>• Phone number</li> <li>• Log-in data</li> <li>• Title and company name</li> <li>• Any other personal data that may be provided by Buyer or its users</li> </ul>
<b>Categories of data subjects</b>	<ul style="list-style-type: none"> <li>• Buyer's personnel</li> <li>• Personnel of Buyer's Suppliers</li> </ul>
<b>Duration of processing</b>	For the duration of the Agreement as further set out in Section 7 of DPA

## Annex 2 - Technical and Organizational Measures

Taking into account the state of the art, the costs of implementation and the nature, scope, circumstances and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons, Choco shall, in its capacity as data processor, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, but not limited to, the following:

## **1 Confidentiality**

### **1.1 Physical access control**

Choco shall take appropriate measures to reduce the risk of unauthorized persons gaining access to data processing systems with which Buyer's personal data are processed and used.

#### **Technical measures**

- Automatic access control systems, control of access by gatekeeper services and alarm systems
- Lockable server cabinets
- key regulation, service directives stipulating that service rooms are to be locked when employees are absent

### **1.2 System access control**

Choco shall take appropriate measures to prevent data processing systems (computers) from being used by unauthorized persons. For this purpose, Choco shall take the following precautions:

#### **Technical measures:**

- Login with username + password
- Smartphone encryption
- Encryption of company laptops
- Remote laptop management
- Deployment of anti-virus software for laptops and systems

#### **Organizational measures:**

- Manage user permissions
- Create user profiles
- Policies on use of Company Hardware
- General policy on data protection and / or security

### **1.3 Data access control**

Choco shall take appropriate measures to ensure that the persons authorized to use the data processing systems can only access the personal data subject to their access authorization and that the Personal Data of Buyer cannot be read, copied, modified or removed without authorization during processing, use and after storage. For this purpose, Choco shall take the following precautions:

#### **Technical measures:**

- Erasure of data carriers on laptops before reuse.
- Logging of access to important documents, especially when entering, changing and deleting data.
- File shredder (min. level 3, cross cut)

#### **Organizational measures:**

- Creating an authorization concept
- Management of rights by system administrator

- Reduction in the number of administrators
- Closed area for sensitive documents

#### **1.4 Separation control**

Choco shall take appropriate measures to ensure that the Personal Data of Buyer collected for different purposes can be processed separately. For this purpose, Choco shall take the following precautions:

##### **Technical measures:**

- Separate storage on different software
- Software-based customer separation

##### **Organizational measures:**

- Creation of an authorization concept
- Determination of database rights

### **2 Integrity**

#### **2.1 Transmission control**

Choco shall take reasonable measures to reduce the risk that the Personal Data of Buyer can be read, copied, modified or removed without authorization during electronic transmission or during their transport or storage on data carriers. To this end, Choco shall take the following precautions:

##### **Technical measures:**

- Email encryption
- Logging of accesses and retrievals of important documents and data
- Provision *via* encrypted connections such as sftp, https

#### **2.2 Data input control**

Choco shall take appropriate measures to ensure that it is possible to check and determine retrospectively whether and by whom personal data of the customer have been entered into data processing systems, changed or removed. For this purpose, Choco shall take the following precautions:

##### **Technical measures:**

- Possibility of technical logging of the entry, modification and deletion of personal data.

##### **Organizational measures:**

- Traceability of entry, modification, and deletion of personal data through individual user names.
- Retention of forms from which personal data have been transferred to automated processing operations.
- Assignment of rights to enter, change, and delete personal data on the basis of an authorization concept.

### **3 Availability and resilience**

#### **3.1 Availability control**

Choco shall take reasonable measures to ensure that the Personal Data of Buyer is protected against accidental destruction or loss. For this purpose, Choco shall take the following precautions:

##### **Technical measures:**

- Fire and smoke detection systems
- Careful selection of the hosting service provider

**Organizational measures:**

- Regular control of the hosting service provider

**4 Procedures for regular review, assessment and evaluation.**

Choco shall implement procedures for regular review, assessment and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing.

**4.1 Data protection management**

**Organizational measures:**

- Central documentation of all procedures, regulations and guidelines on data protection with access for employees as required / authorized
- A review of the effectiveness of the technical protective measures is carried out regularly
- Employees trained and committed to confidentiality
- Raising employee awareness through training

**4.2 Incident response management**

**Organizational measures:**

- Documentation of security incidents and data breaches
- Regulation of responsibilities for the follow-up of security incidents and data breaches
- Security breach response support.
- Formalized process for handling requests for information from data subjects is in place.

**Annex 3 - Subprocessor List**

Name	Entity Location	Purpose
Amazon Web Services, Inc.	USA Location of processing: EU West 1 (Ireland, EU)	Cloud Infrastructure and AI services
Google Cloud EMEA Limited	Ireland Location of processing: EU West 1 (Ireland, EU)	Cloud Storage and AI services
salesforce.com Germany GmbH	Germany Location of processing: EU43 (Frankfurt, Germany; Paris, France)	CRM
Invisible Technologies Inc	USA	Back-office services
Iterable, Inc	USA	CRM



Mindbridge Private Limited	Pakistan	Back-office services
The Mail Track Company, S.L.	Spain	Customer outreach tool
OpenAI, L.L.C.	USA	Generative AI services
Twilio Ireland Limited	Ireland	Communication tool
Intercom, Inc.	Ireland	Customer support and customer communication in the software
Choco Communications DACH GmbH	Germany	Intra-group services
Choco Communications Espagna SL	Spain	Intra-group services
Choco Communications SAS	France	Intra-group services
Atlantic Food Waste Partners LLC dba Choco	USA	Intra-group services

We may need to add new subprocessors to the list above. If you'd like to receive a notification of these new sub-processors, you can subscribe using your business email address on this link: <https://choco.com/uk/subprocessors>.