

# Joint Controllership Agreement

## Preamble

This Joint Controllership Agreement ("**JCA**") specifies the data protection obligations and rights of the Parties in connection with the processing of personal data processed by Choco (hereinafter "**Contractor**") and the Supplier (hereinafter "**Customer**"), as joint controllers within the meaning of Art. 26 GDPR (as defined below), under the Software-as-a-Service Agreement concluded between the Parties (hereinafter "**Main Agreement**"). In accordance with the Main Agreement, the Customer may request the Contractor to provide the integration services described in the Integration General Terms and Conditions (hereinafter "**Integration Services**"), therefore, with the creation of the technical infrastructure as a result of the performance of such Integration Services, the Customer will be able to receive and transmit information and data to the Contractor (hereinafter "**Integrated Services**").

For the purposes of this JCA, "**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**", "**personal data**", "**processing**", "**joint controller**" and "**controller**" shall have the meanings set out in the Data Protection Act 2018.

If there are any inconsistencies between this JCA and provisions under the other agreements, specifically under the Main Agreement, then the provisions of this JCA shall take precedence.

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

## 1. Scope of Application

Exclusively for the provision of the Integrated Services, Parties shall process personal data ("Joint Controlled Data") as joint controllers within the meaning of Art. 26 GDPR, determining together the purposes and means of personal data being processed.

## 2. Subject and Scope of the Joint Controllership

2.1 Parties shall process the Joint Controlled Data for the purpose specified in Annex 1 to this JCA. The processing of Joint Controlled Data shall relate solely to the types of personal data and categories of data subjects designated therein.

2.2 The duration of the processing of the Joint Controlled Data corresponds to the duration of the Main Agreement.

2.3 Parties shall process the Joint Controlled Data each complying with their respective obligations as Controllers under the Data Protection Laws. Each party shall perform its obligations arising from this JCA at its own cost.

## 3. Obligations

3.1 Each Party shall:

- a) ensure that it has all necessary notices and lawful bases in place for the processing of the Joint Controlled Data;
- b) provide all information set out in this JCA to any data subject whose personal data may be processed under this JCA in accordance with the Arts. 13, and 14 GDPR;
- c) comply with any requests from data subjects as per Arts. 15 to 22 GDPR;
- d) ensure that all persons who are authorized to have access to the Joint Controlled Data are committed to confidentiality, or are under an appropriate statutory obligation of confidentiality when processing the Joint Controlled Data;

d) implement appropriate technical and organizational measures required to ensure a level of protection of the Joint Controlled Data commensurate to the risk, taking into account the state of the art, the cost of implementation, and the nature, scope, circumstances and purposes of the processing of the Joint Controlled Data and the varying likelihood and severity of the risk to the rights and freedoms of the data subjects;

e) not transfer, access, or process any Joint Controlled Data outside the UK or EEA or engage any data processors, unless the transfer or engagement is permitted by the Data Protection Laws.

3.2 Contractor shall provide data subjects with general information on collection, processing and exchange of the Joint Controlled Data with Customer, including a meaningful excerpt of this JCA and including, if applicable, all recipients of personal data on Contractor's side;

3.3 Customer shall provide data subjects with all information on the collection, processing and exchange of the Joint Controlled Data with Contractor, including a meaningful excerpt of this JCA and including, if applicable, all recipients of personal data on Customer's side;

#### 4. Mutual assistance

Each party shall provide reasonable assistance to the other in complying with the applicable requirements of the Data Protection Laws. In particular, each Party shall:

a) promptly inform the other party about the receipt of any requests from data subjects and other individuals, including supervisory authorities, regulators, and courts, as well as any controls or inspections by such authorities in connection with the Joint Controlled Data;

b) not disclose, amend, delete any Joint Controlled Data without first informing the other party wherever possible;

c) provide the other party with appropriate assistance in complying with the data subject requests and obligations laid down in the Arts. 32 through 36 GDPR;

d) inform the other party without undue delay after having become aware of the breach of the Joint Controlled Data. The notification should at least include the information referred to in Art. 33 (3) GDPR as well as any information necessary for the communication of a personal data breach to the data subjects;

e) inform one another immediately of any circumstances that have or may put in jeopardy the lawful processing of the Joint Controlled Data or compliance with the Data Protection Laws.

f) provide the other party with contact details of at least one employee as point of contact and responsible manager for all queries arising from the data subjects or related to the JCA or the Data Protection Laws.

#### Annex 1 - Purpose, Nature and Scope of Data Processing, Type of Data and Group of Data Subjects

<b>Purpose of data processing</b>	Provision of the Integrated Services which include the transmission of (i) the orders from the Contractor in real time via one of the transmission technologies, or Customer's ERP providers agreed between the Parties, or on a (S)FTP server to the Customer; (ii) the order confirmations from the Customer to the Contractor via a selected and agreed transmission technology; and (iii) ancillary information related to the previous two points from one party to the other (e.g. delivery confirmation, or customers' queries).
<b>Nature and scope of data processing</b>	<ul style="list-style-type: none"><li>• Storage and transmission of names and address data of customers,</li><li>• Storage of customer numbers,</li><li>• Transmission of personal data required to process individual orders to Customer and/or an ERP provider of</li></ul>

	Customer agreed between the Parties.
<b>Type of data</b>	<ul style="list-style-type: none"><li>• Names</li><li>• Email addresses</li><li>• Addresses</li><li>• Phone numbers</li><li>• Order information (e.g., products, product IDs, quantity, prices)</li></ul>
<b>Group of data subjects</b>	<ul style="list-style-type: none"><li>• Customer employees.</li><li>• Commercial buyers, and their personnel, of the gastronomy and food sector.</li></ul>