Version: **April 1st, 2023**

This Data Processing Addendum ("DPA") forms an integral part of the Agreement between Merchant and CMP covering Merchant's use of the CMP Services.

## 1. Definitions and interpretation

The terms contained in these Terms and Conditions initially capitalized are defined and have the meaning as set out in this Clause.

**Controller**: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

**Data Subject**: an identified or identifiable natural person relating to Personal Data.

**Technical and Organizational Measures**: measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access and against all other unlawful forms of Processing.

**Personal Data Breach**: a breach of security leading to the accident or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

**Processor**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

**Processing/to Process**: any operation or set of operations which is performed on 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.

**Sub-processor**: A party engaged by CMP for processing activities for which CMP is a Processor under this DPA, as listed on: www.cm.com/trust-center/privacy/. The expression 'Data Protection Impact Assessment,' shall have the meaning ascribed to them in the Applicable Data Protection Law.

1.2. References to the Applicable Data Protection Laws shall be replaced with or incorporate references to any laws replacing or amending those Applicable Data Protection Laws, and the equivalent terms defined in such laws, once in force and applicable.

1.3. This Data Processing Terms and Conditions shall exclusively apply to the processing of Personal Data by CMP as a Processor on behalf of Merchant. In case of any conflict, the provisions of this Data Processing Terms and Conditions concerning Processing of Personal Data shall take precedence over the provisions of the Terms and Conditions Agreement. Where individual provisions of this Data Processing Terms and Conditions are invalid or unenforceable, the validity and enforceability of the other provisions shall not be affected.

## 2. Scope and Applicability

2.1 This DPA shall apply to the Personal Data processing activities, for which CMP is a Processor subject to Applicable Data Protection Laws.

2.2 CMP is a Processor for the processing activities described in article 6 of these DPA.

## 3. Obligations of the Merchant

3.1 Merchant shall, in its use of the CMP Service, Process Personal Data in accordance with the requirements of Applicable Data Protection Laws. Merchant's instructions for the Processing of Personal Data shall comply with Applicable Data Protection Laws. Merchant is responsible for the accuracy, quality, and legality of Personal Data and the means by which Merchant acquired Personal Data. Merchant shall ensure that it meets all requirements for processing and transferring the Personal Data under Applicable Laws, including but not limited to, ensuring a lawful ground of processing and/or cross-border transfers. Merchant shall inform CMP without undue delay if it can no longer meet its obligations in relation to the processing of Personal Data under the Applicable Laws and/or the Agreement.

3.2 Without limiting the generality of any other provision of the Agreement, prior to using the CMP Service, Merchant shall obtain verifiable informed consent of the End Users or be able to provide confirmation of any other applicable lawful basis for Processing, and shall maintain a record of each such consent and/or lawful basis. Upon reasonable written notice, Merchant shall provide information on the lawful basis as requested and where required by CMP, any Payment Network, regulator, or other competent authority.

## 4. Obligations of the Processor

### 4.1 Instructions

CMP shall Process Personal Data in accordance with this DPA and the Agreement, and for the purposes and in the manner specified by Merchant from time to time in the Agreement and further instructions within the scope of the Agreement.

### 4.2 Technical and Organizational Measures

4.2.1 Taking into account the state of the art, the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, CMP shall implement appropriate technical and organizational measures (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) to ensure a level of security appropriate to the risk. Up to date information regarding technical and organizational measures can be found on www.cm.com/trust-center/security/.

4.2.2 CMP shall test, assess and evaluate the effectiveness of technical and organizational measures for ensuring the security of the Processing on an ongoing basis. CMP shall continuously enhance and improve technical and organizational measures where appropriate.

### 4.3 Personnel requirements

CMP ensures that persons authorized to Process the Personal Data have committed themselves to confidentiality or

are under an appropriate statutory obligation of confidentiality. Access to Personal Data is restricted to personnel who require access in order to perform the CMP Services under the Agreement.

**4.4. Confidentiality**

CMP agrees that it shall maintain the Personal Data in confidence. In particular, CMP agrees that it shall not disclose any Personal Data supplied to CMP by, for, or on behalf of Merchant to any third party without Merchant's prior consent, except as foreseen and required for the performance of the CMP Services under the Agreement or mandatory law.

**4.5.Data Subject Rights**

4.5.1 Where Merchant so instructs CMP, CMP shall transfer, correct, delete or block Personal Data if Merchant receives a request from a Data Subject to exercise the 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 (“Data Subject Request”).

4.5.2 CMP shall notify Merchant if CMP receives a Data Subject Request. Taking into account the nature of the Processing, CMP shall assist Merchant, in responding to a Data Subject Request under the Applicable Data Protection Law. CMP shall assist Merchant to the extent CMP is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws.

**4.6 Assistance with Merchant’s compliance**

CMP shall provide to Merchant further assistance reasonably required to ensure compliance with Merchant's obligations under Data Protection Laws, including with respect to:

(a) data protection impact assessment, by providing such information and cooperation as Merchant may require for the purpose of assisting Merchant in carrying out a data protection impact assessment and periodic reviews to assess if the Processing of Personal Data is performed in compliance with the data protection impact assessment;

(b) prior consultation with a data protection supervisory authority regarding high risk Processing.

**4.7 Compliance, information, and audit**

4.7.1 CMP has obtained third-party certifications set forth in the Trust Center on the website of CMP, available at www.cm.com/trust-center/, which provides information on technical and organizational measures, privacy, compliance, risk management and data security. Upon Merchant’s written request, and subject to the confidentiality obligations set forth in the Agreement, CMP shall make available to Merchant, that is not a competitor of CMP (or Merchant’s independent, third-party auditor that is not a competitor of CMP) a copy of CMP’s then most recent third-party certifications and information regarding the IT architecture and security, as applicable and reasonably requested. Merchant is responsible for assessing the information that is made available by CMP and determining whether it meets Merchant’s requirements and obligations under Applicable Data Protection Laws. Merchant agrees that the information provided hereunder shall serve to fulfill the audit rights of Merchant under Applicable Data Protection Laws.

4.7.2 In the event the information provided by CMP is insufficient to prove compliance with this DPA, Merchant has the right to appoint an accredited external expert at most once per year to audit the procedures regarding the data Processing for Merchant. CMP will cooperate with such audit upon a reasonable prior written notice of no less than

ten Working Days. Merchant shall reimburse CMP for any time expended by CMP for any such audit at CMP's then-current professional services rates, which shall be made available to Merchant upon request. Before the commencement of any such audit, the Parties shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Merchant shall be responsible.

4.7.3 CMP is entitled to request that the external expert signs a confidentiality declaration in favor of CMP. The confidentiality declaration shall contain the terms and conditions that are usual for this type of declaration. Any report or statement provided by the external expert shall be made available to CMP. Merchant shall ensure that the audit hinders CMP 's operations as little as possible.

**4.8 Records**

CMP shall maintain complete, accurate and up to date records of Processing activities carried out on behalf of its Merchants.

**4.9 Affiliates and Sub-processors**

4.9.1 Some or all of CMP's obligations under the Agreement may be performed by affiliates of CMP. CMP is responsible for compliance of its affiliates with the Agreement.

4.9.2 Merchant acknowledges and agrees that (a) CMP's affiliates may be retained as Sub-processors; and (b) CMP and CMP's affiliates respectively may engage third-party Sub-processors in connection with the provision of the CMP Services. Provided always CMP or a CMP affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in the Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the CMP Service provided by such Sub-processor and CMP maintains an up to date list of Sub-processors. CMP's current list of Sub-processors is available on: www.CMP/trust-center/privacy/. CMP shall inform Merchant thirty (30) days prior to any changes with respect to the Sub-processor list. Within that timeframe, Merchant may object to the change to the Sub-processor list, provided such objection is submitted in writing and based on reasonable grounds with respect to Applicable Data Protection Laws. The Parties will make a good faith effort to resolve the Merchant's objection. If the objection is not resolved within thirty (30) days, either Party may terminate the Agreement.

4.9.3 CMP shall be responsible for each of its Sub-processors to the same extent CMP would be responsible if performing the services of each Sub-processor directly under the terms of the Agreement.

**4.10 Breach Notification**

In respect of a Personal Data Breach, CMP shall:

(a) notify Merchant of a Personal Data Breach involving CMP or a sub-contractor without undue delay (but in no event later than forty-eight hours after becoming aware of the Personal Data Breach).

(b) provide reasonable cooperation and assistance to Merchant in relation to any action to be taken in response to a Personal Data Breach under Applicable Data Protection Laws, such as Art. 33(3) and 34(3) GDPR, including regarding any communication of the Personal Data Breach to the Data Subject and data protection authorities.

CMP will promptly investigate a Personal Data Breach and take reasonable measures to identify its root cause(s) and prevent a recurrence. As information is collected or otherwise becomes available, unless prohibited by law, CMP will provide Merchant with a description of the Personal Data Breach, the type of data that was the subject of

the Personal Data Breach, and other information Merchant may reasonably request. The Parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected Data Subjects and/or the relevant data protection authorities.

## 5. Cross Border Data Transfer

To the extent that the engagement of a Sub-processor under art. 4.9 requires a cross border transfer mechanism under Applicable Data Protection Laws to lawfully transfer personal data from a jurisdiction (i.e., the European Economic Area, the United Kingdom or any other relevant jurisdiction) to a third party located outside of that jurisdiction the following terms shall apply. Merchant authorizes CMP to transfer Personal Data outside the jurisdiction in which CMP is located and the Personal Data was first received, provided that CMP shall ensure that such transfers will be executed in accordance with this DPA and a lawful data transfer mechanism that provides an adequate level of protection under Applicable Data Protection Laws.

## 6. Storage, retention, and deletion of Personal Data

CMP shall Process and retain data, including Personal Data, in accordance with Applicable Law, regulations, including but not limited to national telecom legislation and Applicable Data Protection Laws. The data, including Personal Data, submitted to the platform of CMP shall be Processed and stored in accordance with CMP's data retention policy. The Personal Data shall be retained for no longer than is necessary for providing the CMP Services under the Agreement, for the purposes as stated in the Agreement and as far as required and/or allowed under Applicable Law. CMP shall de-identify or depersonalize data into anonymized data after the applicable retention period. This results in data that includes no Personal Data or unique identifiers that could later be used to refer to the Personal Data to which the data was once associated.

## 7. Description of Processing

### 7.1 Nature and Purpose of Processing

CMP will Process Personal Data as necessary to perform the CMP Services pursuant to the Agreement, as further specified in the Agreement, and as further instructed by Merchant within the scope of the Agreement.

### 7.2 Duration of the Processing

CMP will process Personal Data for the duration of the Agreement and in accordance with clause 6 of this DPA.

### 7.3 Categories of Data Subjects

Merchant may submit data to CMP in using the CMP Service, the content of which is determined and controlled by Merchant in its sole discretion, and which may include, but is not limited to Personal Data relating to the categories of Data Subjects listed in Annex 1.

### 7.4 Type of Personal Data

Merchant may submit Personal Data to the CMP Services, the extent of which is determined and controlled by Merchant in its sole discretion, and which may include, but is not limited to the categories of Personal Data listed in Annex 1.

## Annex 1: Description of data subjects and categories of personal data

**Data Subjects:**

- (Potential) customers (who are natural persons) of Merchant or its Merchants;
- Employees, contractors, advisors, freelancers or persons hired by (customers of) Merchant;
- Contact persons of Merchant's prospects, customers and business partners;
- Merchant's users authorized by Merchant to use the CMP Services.

**Categories of personal data:**

- Customer's name;
- Customer's email and/or telephone number;
- Payment method;
- Card details;
- Consumption data;
- Transaction data;
- Data on fraud likelihood.