CAPP & CO

DATA PROTECTION POLICY

1. DEFINITIONS AND INTERPRETATION

This Policy is subject to and should be read in accordance with Capp & Co Limited ("**Capp**")'s standard terms (the "**Terms**") and any document entitled "Capp & Co Order" attached to those Terms or which otherwise references those terms (the "**Order**") entered into between Capp and the client specified in the Order (the "**Client**").

In this Policy, the following terms shall have the following meanings:

"**controller**", "**processor**", "**data subject**", "**personal data**", "**processing**" (and "**process**") and "**special categories of personal data**" shall have the meanings given in Applicable Data Protection Law; and

"**Applicable Data Protection Law**" shall mean:

(i) prior to 25 May 2018, the EU Data Protection Directive (Directive 95/46/EC); and

(ii) on and after 25 May 2018, the EU General Data Protection Regulation (Regulation 2016/679).

2. RELATIONSHIP OF THE PARTIES

The Client appoints Capp as a processor to process the personal data relevant to the Order(s) (the "**Data**") for the purposes described in these Terms (or as otherwise agreed between the parties) (the "**Permitted Purpose**"). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

3. INTERNATIONAL TRANSFERS

Capp shall not transfer the Data outside of the European Economic Area ("**EEA**") unless it has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law.

4. CONFIDENTIALITY OF PROCESSING

Capp shall ensure that any person it authorises to process the Data (an "**Authorised Person**") shall protect the Data in accordance with Capp's confidentiality obligations under these Terms.

5. SECURITY

Capp shall implement the technical and organisational measures set out in the Annex to:

(i) protect the Data from accidental or unlawful destruction; and

(ii) prevent loss, alteration, unauthorised disclosure of, or access to, the Data,

(a "**Security Incident**").

6. SUBCONTRACTING

The Client consents to Capp engaging third party subprocessors to process the Data for the Permitted Purpose provided that Capp:

(i) maintains an up-to-date list of its subprocessors at https://www.capp.co/capp-policies, which it shall update with details of any change in subprocessors at least 10 days prior to any such change;

(ii) imposes data protection terms on any subprocessor it appoints that require it to protect the Data to the standard required by Applicable Data Protection Law; and

(iii) remains liable for any breach of this Clause that is caused by an act, error or omission of its subprocessor.

The Client may object to Capp's appointment or replacement of a subprocessor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to the Client's ability to comply with Applicable Data Protection Laws. In such event, Capp will either not appoint or replace the subprocessor or, if this is not possible, the Client may suspend or terminate the relevant Order(s) (without prejudice to any fees incurred by the Client prior to suspension or termination).

7. COOPERATION AND DATA SUBJECTS' RIGHTS

Capp shall provide reasonable and timely assistance to the Client (at the Client's expense) to enable the Client to respond to:

(i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable) in accordance with its Data Subject Rights Management Policy which can be found at https://www.capp.co/capp-policies; and

(ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data.

In the event that any request, correspondence, enquiry or complaint is made directly to Capp, Capp shall promptly inform the Client providing full details of the same.

8. DATA PROTECTION IMPACT ASSESSMENT

If Capp believes or becomes aware that is processing of the Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall inform the Client and provide reasonable cooperation to the Client (at the Client's expense) in connection with any data protection impact assessment that may be required under Applicable Data Protection Law.

9. SECURITY INCIDENTS

If it becomes aware of a confirmed Security Incident, Capp shall inform the Client without undue delay and shall provide reasonable information and cooperation to the Client so that the Client can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Law. Capp shall further take reasonably necessary measures and actions to remedy or mitigate the effects of the Security Incident and shall keep the Client informed of all material developments in connection with the Security Incident.

10. DELETION OR RETURN OF PERSONAL DATA

Subject to the provisions of the Terms, upon termination or expiry of the relevant Order(s), Capp shall (at the Client's election) destroy or return to the Client all Personal Data in its possession or control. This requirement shall not apply to the extent that Capp is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which Personal Data Capp shall securely isolate and protect from any further processing except to the extent required by law.

11. AUDIT

The Client acknowledges that Capp is regularly audited against *ISO 27001 and ISO 9001* standards by independent third-party auditors. Upon request, Capp shall supply a summary copy of its audit report(s) to the Client, which reports shall be subject to the confidentiality provisions within these Terms.

ANNEX

SECURITY MEASURES

Capp currently observes the security practices described in this Appendix 2. Notwithstanding any provision to the contrary otherwise agreed to by Client, Capp may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalised terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: Capp hosts its Service with outsourced cloud infrastructure providers. Additionally, Capp maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement.

Capp relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: Capp hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type III and ISO 27001 compliance, among other certifications, as per https://www.rackspace.com/en-nl/compliance/soc

Authentication: Capp has implemented a strong password policy for its Service. Customers who interact with the Service must authenticate before accessing its Service.

Authorisation: Customer data is stored in multi-tenant storage systems accessible to customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure.

The authorisation model in each of Capp products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customisation options. Authorisation to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key.

ii) Preventing Unauthorised Product Use

Capp implements industry standard access controls and detection capabilities for the internal networks that support its Service.

Security reviews of code stored in Capp source code repositories is performed, checking for coding best practices and identifiable software flaws.

iii) Limitations of Privilege & Authorisation Requirements

Product access: A subset of Capp employees have access to the product and to personal data via controlled interfaces, based on a business need to know. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role.

Code of conduct: All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: Capp makes HTTPS encryption (also referred to as SSL or TLS) mandatory on every one of its login interfaces. Capp HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Capp stores user passwords following policies that follow industry standard practices for security.

c) Input Control

Detection: Capp has designed its infrastructure to log extensive information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Capp personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Capp maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Capp will take appropriate steps to minimize damage or unauthorized disclosure.

Communication: If Capp becomes aware of unlawful access to data stored within its products, Capp will notify those affected promptly per the GDPR requirements described in Article 34.