Data Processing Agreement

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the “GDPR”)

Between a customer of Crispa (the “Data Controller”)

and

Crispa Technologies ApS
Company registration (CVR) number: 43 24 44 77
Applebys Plads 7
1411 Copenhagen K
Denmark

(the “Data Processor”)

Each a “Party”; together the “Parties”

HAVE AGREED on the following contractual clauses (the “Clauses”) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

Table of Contents

Preamble

1. These Clauses set out the rights and obligations of the Data Controller and the Data Processor when processing personal data on behalf of the Data Controller.

2. The Clauses have been designed to ensure the Parties' compliance with Article 28(3) of the GDPR.

3. In the context of the provision of the Crispa platform and associated accounting services, the Data Processor will process personal data on behalf of the Data Controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the Parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the Data Controller's conditions for the Data Processor's use of sub-processors and a list of sub-processors authorised by the Data Controller.

8. Appendix C contains the Data Controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the Data Processor and how audits of the Data Processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both Parties.

11. The Clauses shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the GDPR or other legislation.

The rights and obligations of the Data Controller

1. The Data Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR, the applicable EU or Member State data protection provisions and these Clauses.

2. The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The Data Controller shall be responsible for ensuring that the processing of personal data which the Data Processor is instructed to perform has a legal basis.

The Data Processor acts according to instructions

1. The Data Processor shall process personal data only on documented instructions from the Data Controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the Data Controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The Data Processor shall immediately inform the Data Controller if instructions given by the Data Controller, in the opinion of the Data Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

Confidentiality

1. The Data Processor shall only grant access to the personal data being processed on behalf of the Data Controller to persons under the Data Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn if access is no longer necessary.

2. At the request of the Data Controller, the Data Processor shall demonstrate that the concerned persons under the Data Processor's authority are subject to confidentiality obligations.

Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and 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, the Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The Data Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following: pseudonymisation and encryption of personal data; the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the Data Processor shall also independently evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Data Controller shall provide the Data Processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations pursuant to Articles 32–36 of the GDPR.

Use of sub-processors

1. The Data Processor shall meet the requirements of Article 28(2) and (4) of the GDPR in order to engage another processor (a "sub-processor"). The Data Processor shall not engage another processor without prior specific or general written authorisation from the Data Controller. In the case of general written authorisation, the Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of sub-processors, thereby giving the Data Controller the opportunity to object to such changes.

2. Where the Data Processor engages a sub-processor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in these Clauses shall be imposed on that sub-processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. The Data Processor shall remain fully liable to the Data Controller for the performance of the sub-processor's obligations.

3. The sub-processors approved by the Data Controller are listed in Appendix B.

Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the Data Processor shall only occur on the basis of documented instructions from the Data Controller and shall always take place in compliance with Chapter V of the GDPR.

2. In case transfers to third countries or international organisations, which the Data Processor has not been instructed to perform by the Data Controller, are required under Union or Member State law to which the Data Processor is subject, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless the law prohibits such information on important grounds of public interest.

3. The Data Processor shall ensure that personal data is transferred on the basis of an adequacy decision pursuant to Article 45 GDPR, or subject to appropriate safeguards pursuant to Article 46 GDPR, or on the basis of binding corporate rules pursuant to Article 47 GDPR, or pursuant to the derogations for specific situations set out in Article 49 GDPR.

Assistance to the Data Controller

1. Taking into account the nature of the processing, the Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.

2. The Data Processor shall assist the Data Controller in ensuring compliance with Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to the Data Processor.

Notification of personal data breach

1. In the event of a personal data breach concerning data processed by the Data Processor on behalf of the Data Controller, the Data Processor shall without undue delay notify the Data Controller of the breach. Such notification shall, at a minimum, describe the nature of the personal data breach, the likely consequences of the personal data breach and the measures taken or proposed to be taken by the Data Processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

2. Where and in so far as it is not possible to provide all information at the same time, the information may be provided in phases without undue further delay.

Erasure and return of data

1. On termination of the provision of personal data processing services, the Data Processor shall, at the choice of the Data Controller, delete or return all the personal data to the Data Controller and delete existing copies unless Union or Member State law requires storage of the personal data.

2. The Data Processor shall document the deletion of data in accordance with the instructions of the Data Controller.

Audit and inspection

1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and are imposed directly on the Data Processor by Article 28 of the GDPR.

2. At the Data Controller's request, and at the Data Controller's expense, the Data Processor shall also allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The Parties shall agree on the scope, method, timing and duration of the audits in accordance with Clause C.7.

The Parties' agreement on other terms

The Parties may agree other clauses concerning the provision of the data processing service provided that such clauses do not directly or indirectly contradict the Clauses or prejudice the fundamental rights or freedoms of the data subjects. Such additional terms are set out in Appendix D.

Commencement and termination

1. These Clauses shall become effective when signed by both Parties.

2. The Clauses shall apply for the duration of the provision of personal data processing services. The Clauses shall remain in force until the personal data processed on behalf of the Data Controller has been deleted or returned in accordance with Clause 11.

Data Controller and Data Processor contacts

The Parties may contact each other using the contact details provided in Appendix A and Appendix C.

Appendix A – Information about the processing

A.1 The purpose of the Data Processor's processing of personal data on behalf of the Data Controller

The Crispa platform enables companies to connect their banking and financial systems, automate bookkeeping and forecasting, and access real-time reporting and key metrics. The purpose of the processing is therefore to deliver accounting, forecasting and related financial management services to the Data Controller, including the generation of monthly P&L statements, calculation of metrics such as gross margin, customer acquisition cost (CAC) and net revenue retention (NRR), runway predictions and team planning.

A.2 The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing)

Collecting, organising, storing and analysing financial transaction data and supporting documents; processing bank feeds and invoices; categorising expenditures and revenues; generating accounting reports and forecasts; issuing notifications to the Data Controller regarding key financial events or expiring items; and enabling controlled sharing of financial data with authorised third parties such as auditors, investors or accountants.

A.3 The processing includes the following types of personal data about data subjects

Name, e-mail address, telephone number, residential or business address, user account credentials, job title; bank account identifiers or tokens; transaction details (amounts, dates, merchant descriptions); payroll and compensation data; invoice and receipt information containing personal details; communications metadata (e.g., sender and recipient email addresses); and any other personal data uploaded by the Data Controller to the Crispa platform.

A.4 Processing includes the following categories of data subject

Employees, officers and directors of the Data Controller, contractors, business owners, customers of the Data Controller, and other individuals whose personal data is contained in financial transactions or documents processed via the Crispa platform.

A.5 The Data Processor's processing of personal data on behalf of the Data Controller may be performed when the Clauses commence. Processing has the following duration

The Data Processor shall process personal data for as long as the Data Controller subscribes to the Crispa platform and associated accounting services or until otherwise instructed by the Data Controller.

Appendix B – Authorised sub-processors

B.1 Approved sub-processors

NAME	COMPANY INFORMATION	ADDRESS	DESCRIPTION OF PROCESSING
Amazon Web Services EMEA SARL	Company registration number: B-93815	38 Avenue John F. Kenn edy, L-1855 Luxembourg	Hosting of data and infrastructure services used to operate the Crispa platform.
Google LLC (Google Workspace)	N/A	1600 Amphitheatre Parkway, Mountain View, California 94043, USA	Email and productivity applications for internal communication and collaboration of Crispa personnel.
Dropbox, Inc.	N/A	1800 Owens Street, San Francisco, CA 94158, USA	Cloud storage and file sharing services used by Crispa to store documents and backups.
Superhuman Labs, Inc.	N/A	548 Market St, #39105, San Francisco, CA 94104, USA	Email client used by Crispa employees for efficient email management.
Plaid, Inc.	N/A	1098 Harrison Street, San Francisco, CA 94103, USA	Financial services platform for connecting bank accounts and retrieving transaction data used in the Crispa accounting services.
OpenAI, LLC	N/A	3180 18th Street, San Francisco, CA 94110, USA	Artificial intelligence services used to provide natural language processing and generative features within the Crispa platform.
Anthropic	N/A	548 Market St, San Francisco, CA 94104, USA	Artificial intelligence services used for advanced AI features such as summarisation or reasoning in the Crispa platform.
Perplexity AI, Inc.	N/A	115 Sansome Street, 9th Floor, San Francisco, CA 94104, USA	AI search and question-answering services used to enhance insights and analytics within the Crispa

			platform.

B.2 Prior notice for the authorisation of sub-processors

There are no sub-processors that require longer notice periods beyond what is stipulated in Clause 7.3 of these Clauses.

Appendix C – Instruction pertaining to the use of personal data

C.1 The subject of/instruction for the processing

The Data Processor's processing of personal data on behalf of the Data Controller shall be carried out by the Data Processor performing the services and functionalities of the Crispa products as agreed with the Data Controller. The data entered into the Crispa system is controlled by the Data Controller.

C.2 Security of processing

The level of security shall take into account the sensitivity of the personal data processed in the Crispa platform, which includes financial transaction details and personal information as described in Appendix A. The Data Processor maintains a high level of security controls in accordance with industry best practices. The security measures and description of the hosting and operational setup are described in Crispa's security overview documentation provided separately to the Data Controller.

C.3 Assistance to the Data Controller

Crispa builds, maintains and hosts the products used by the Data Controller. Crispa assists the Data Controller as far as possible with information and access to data, logs and infrastructure so that the Data Controller can comply with GDPR obligations, including responding to data subject requests and performing data protection impact assessments.

C.4 Storage period/erasure procedures

Data retention periods and policies depend on the different data subjects and areas of the platform. Some data remains in the system for the full duration of the engagement between Crispa and the Data Controller, while other data is deleted automatically.

- Log files may contain IP addresses, email addresses and other personal information. Logs are kept for up to 120 days depending on the infrastructure component.
- Transactional data in the platform: names, companies and the structure of the company are documented in Crispa's platform and are not automatically deleted; documents uploaded by users are deleted within 30 days after users instruct deletion.
- Backups are kept for 30 days and may contain current and former Data Controller data. Backups are always encrypted.

Upon termination of the provision of personal data processing services, Crispa will extract data and send it to the Data Controller and delete any personal data within 30 days after the termination date.

C.5 Processing location

Processing of personal data under the Clauses is performed at Crispa's primary and secondary data centres and office locations.

- Primary data centre: Amazon Web Services in Frankfurt, Germany (main hosting of data and application).
- Secondary data centre: Amazon Web Services in Dublin, Ireland (backup of data).
- Crispa's office locations: currently at Applebys Plads 7, 1411 Copenhagen K, Denmark (administration, support and development).

C.6 Instruction on the transfer of personal data to third countries

If the Data Controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the Data Processor shall not be entitled to perform such transfer within the framework of these Clauses.

C.7 Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

If required by the Data Controller, the Data Processor shall, at the Data Controller's expense, obtain an inspection report from an independent third party concerning the Data Processor's compliance with the GDPR. Such inspection cannot be performed more than once a year. The inspections of the Data Processor and sub-processors are limited by the availability and access that is possible. For example, it is not possible to perform a physical inspection of the Data Processor's data centre provider Amazon Web Services or other current and future sub-processors.

Any audits and inspections that the Data Processor obtains at its own initiative and cost concerning the Data Processor's compliance with the GDPR will be shared with the Data Controller in the form of main conclusions and plans for mitigating relevant risks.

The results and reports from audits and inspections are confidential and cannot be shared with any third parties unless with written consent or required by law.

C.8 Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

Not applicable.

Appendix D – The Parties' terms of agreement on other subjects

Not applicable.