Data Processing Agreement

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

between

The Partner

(the data controller)

and

Kanpla ApS
CVR: 40369813
Søndergade 44, 3.
8000 Aarhus C
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.

1. Table of Contents

2. Preamble 3

3. The rights and obligations of the data controller 3

4. The data processor acts according to instructions 4

5. Confidentiality 4

6. Security of processing 4

7. Use of sub-processors 5

8. Transfer of data to third countries or international organisations 6

9. Assistance to the data controller 7

10. Notification of personal data breach 8

11. Erasure and return of data 8

12. Audit and inspection 8

13. The parties' agreement on other terms 9

14. Commencement and termination 9

15. Data controller and data processor contacts/contact points 9

Appendix A Information about the processing 10

Appendix B Authorised sub-processors 11

Appendix C Instruction pertaining to the use of personal data 12

Appendix D The parties' terms of agreement on other subjects ..... **Error! Bookmark not defined.**

2. Preamble

1. These Contractual Clauses (the 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 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In the context of the provision of a digital platform and app, 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 General Data Protection Regulation (the GDPR) or other legislation.

3. 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 (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

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

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. 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.

5. 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, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. 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:
   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. 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 from the data controller – 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 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

   The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 14-days notice in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

3. 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 the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, 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 Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

4. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

5. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

6. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. 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 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, is required under EU 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 that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. 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, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, Datatilsynet, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, Datatilsynet, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to 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.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities,

with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

15. Data controller and data processor contacts/contact points

1. The data processor may be contacted at the following contacts:

Name	Peter Bæch
Position	CEO
Telephone	+45 93 92 04 12
E-mail	pb@kanpla.dk

2. The data controller is obligated to continuously inform the data processor about changes regarding contact persons.

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 is:

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is to provide a digital platform and app, along with associated services, to the Data Controller. This includes registering user information, storing data, providing support for system usage, assisting in data transfer, copying, or deletion, and taking backups of agreed-upon data.

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):

The Data Processor's processing of personal data on behalf of the Data Processor primarily involves:

- Collection
- Registration
- Deletion

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

General personal data:

- Name
- Address
- Email address
- Position / title
- Company • Employee number
- Dietary preferences / diet
- Phone number
- Payment information

Sensitive personal data:

- Information about allergens (Data can be transferred voluntary for the user)

A.4. Processing includes the following categories of data subject:

Canteen guests (employees, customers, and possibly other visitors).

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 processing is not time-limited upon entering into the provisions, as the processing continues until the agreement between the parties for the provision of a digital platform and app ceases.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	ADDRESS	DESCRIPTION OF PROCESSING
Google Cloud Platform	Server located at Frankfurt, Germany (europe-west3), samt enkelte funktioner i St. Ghislain, Belgium (europe-west1)	Used for storage, hosting and processing of the data.
Intercom R&D Unlimited Company	2nd Floor, Stephen Court, 18-21 Saint Stephen's Green, Dublin	Chatsupport integration.
Reepay A/S	Pilestræde 28a, 2. sal, 1112 København K, Danmark. Server located at AWS Ireland	Used for facilitating secure payment.
Elastic NV	Keizersgracht 281, Amsterdam. Server located at GCP - Belgium (europe-west1)	Used for statistics and tickets.
Mailjet SAS	4, rue Jules Lefebvre, 75009 Paris, France. Server located at GCP - Belgium (europe-west1) and Germany (europe-west3).	Mailsystem to ensure newsletters and updates on the application.

The data controller shall on the commencement of the Clauses authorise the use of the above-mentioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

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

The Data Processor must provide written notice to the Data Controller of any planned changes regarding the addition or replacement of subprocessors, with a minimum of 14 days' prior written notice. This allows the Data Controller the opportunity to object to such changes before using the respective subprocessor(s). The Data Processor notifies the Data Controller via email to the contact person at the Data Controller, as specified in Clause 16 of the provisions.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The Data Controller hereby instructs the Data Processor to process the Data Controller's information for the purpose of delivering the Data Processor's digital platform and app

C.2. Security of processing

The level of security shall take into account:

The processing involves a significant amount of general personal data, and therefore, a standard security level needs to be established.

The Data Processor is then entitled and obligated to make decisions regarding the technical and organizational security measures to be implemented in order to establish the necessary (and agreed-upon) security level.

However, the Data Processor shall, in any case and at a minimum, implement the following measures, as agreed upon with the Data Controller:

IT Security Policy

The Data Processor must have information security policies and procedures in place that are reviewed annually and approved by the Data Processor's management.

The Data Processor must have procedures for development/change management that are based on privacy-by-default and standard settings.

Where necessary, the Data Processor must conduct a risk assessment of the processing activities involving personal data. The risk assessment should consider the integrity, confidentiality, and availability of the data subject's information.

Password Policy and User Management

The Data Processor must have password policies and user management policies for regular accounts and stricter guidelines for administrative and service accounts. These policies should be reviewed annually and approved by the Data Processor's Tech Lead.

Access is granted based on the principle of "least privileged access." This means that access is only given to users who have a necessary need for it.

Portable Media

The Data Processor must have procedures for managing portable and storage media, including the disposal of media that is no longer in use, in order to prevent unauthorized access.

Mobile Devices and Remote Workstations

There must be supporting security measures to manage risks associated with the use of mobile devices and access to remote workstations at the Data Processor's organization.

Overview of IT Assets

The Data Processor must maintain an updated list of IT assets, including PCs and servers where the Data Controller's data is stored.

Handling of Employees - Before, During, and After Employment

Education and Awareness

The Data Processor must provide relevant training and ensure that new employees at the Data Processor receive the Data Processor's information security policies and policies for the processing of personal data. Employees should be aware of these policies in their work organization.

The Data Processor must ensure that all employees handling personal data are bound by the necessary confidentiality obligations.

Access Rights

The Data Processor must have procedures for managing users and their roles and permissions. The Data Processor should clarify the responsibility for assigning roles and permissions, including during employment and after termination, to ensure that conflicting functions and responsibilities are separated to prevent potential security breaches.

Data Breaches and Incident Management

Data Breaches

The Data Processor must ensure the separation of development, testing, and production environments to mitigate the risk of data breaches.

Incident Management

The Data Processor must have procedures for handling data breaches, including when and how to report them to the Data Processor, as well as the classification of data breaches. The data breach procedures should be tested at least once a year.

Logging
The Data Processor logs the use of the Data Processor's IT systems.

The Data Processor must set up alarms that alert the Data Processor in case of suspicious behavior.

Physical Security

The Data Processor must have procedures in place for physical security to ensure that unauthorized individuals do not have access to personal data.

Servers and other equipment where personal data is processed must be located in locked rooms.

Server rooms must be protected against fire and theft.

Endpoint Security

Antivirus and Firewall

The Data Processor must have appropriate antivirus programs and firewalls to protect against hacker attacks, malware, and other malicious programs and codes.

Updates

Systems where personal data is processed must be regularly updated to minimize the risk of programming errors and vulnerabilities in the Data Processor's IT security.

TLS Encryption

The Data Processor must have TLS or equivalent encryption to protect information, whether at rest or during transmission, including the use, maintenance, and protection of encryption keys throughout their lifecycle. Additionally, encryption must be used in accordance with relevant agreements, legislation, industry standards, and regulatory recommendations.

Backup

The Data Processor must perform backups of personal data belonging to the Data Controller.

The Data Processor must conduct tests of implemented IT security measures, including logs and backups.

Retention Period/Deletion Routine

Personal data stored in backups is retained for 30 days, after which it is overwritten by the Data Processor.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

The Data Processor must implement processes that support the Data Controller in fulfilling the rights of the data subjects according to Chapter 3 of the Data Protection Regulation.

The Data Processor must take immediate action to reduce or eliminate identified vulnerabilities.

The Data Processor must review its own logs to confirm whether data has been accessed by unauthorized individuals and, upon request from the Data Controller, provide these logs.

The Data Processor must be able to provide lists of affected data subjects, enabling the Data Controller to identify and notify them.

The Data Processor cannot demand separate payment for assistance in fulfilling its obligations (e.g., if the Data Processor wants to change information texts, update contact information, retrieve data for access requests, delete data, etc.).

The Data Processor must provide risk assessments, impact assessments, and/or assist the Data Controller in preparing such assessments for the respective system.

C.4. Storage period/erasure procedures
Personal data shall be stored throughout the duration of the cooperation between the parties, after which the Data Processor shall return them to the Data Controller unless instructions for deletion have been given before then.

Upon termination of the service regarding the processing of personal data, the Data Processor shall either delete or return the personal data in accordance with Clause 11.1 of the Terms, unless the Data Processor, upon instruction from the Data Controller and after signing these Terms, has changed the Data Controller's original choice. Such changes shall be documented and stored in writing, including electronically, in connection with the Terms.

C.5. Processing location
Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller’s prior written authorisation:

Denmark and the agreed locations for subprocessors specified in Annex B without the prior written approval of the Data Controller.

C.6. Instruction on the transfer of personal data to third countries
The Data Processor is not entitled to transfer personal data to insecure third countries without the explicit prior written approval of the Data Processor. Any transfer of personal data to insecure third countries must comply with the conditions of the General Data Protection Regulation, including, if necessary, by using the EU Commission's Standard Contractual Clauses for third-country transfers as adopted by the EU Commission on June 4, 2021.

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 within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller’s audits, including inspections, of the processing of personal data being performed by the data processor

The Data Processor shall, at its own expense, obtain an ISAE 3000 assurance report every three years. The report includes an independent auditor's statement, management's statement, system description, and, finally, the Data Processor's control objectives, controls, tests, and results thereof.

Based on the results of the assurance report, the data controller is entitled to request further measures to ensure compliance with the General Data Protection Regulation, data protection provisions in other EU law, or national law of member states and these provisions.

The independent third party shall treat any information obtained from or received from the Data Processor confidentially and may only disclose its findings to the data controller. The Data Processor shall receive a copy of the expert's report and be entitled to use it as documentation

for other clients to the extent relevant. The assurance report shall be promptly provided to the data controller for information purposes.

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

The Data Processor shall monitor and control the subprocessors using the necessary means to assess whether the subprocessor complies with its obligations.

Upon request from the data controller, the Data Processor shall promptly provide the data controller with a copy of such statement received from the subprocessor or make it available to the data controller in another manner. If not provided, the Data Processor shall promptly provide a written account to the data controller outlining the main features of such statement upon receipt.