STANDARD CONTRACTUAL CLAUSES

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

between

[Customer]

(the data controller)

and

Sociuu ApS

CVR 37652210

Ryesgade 3B

2200 København N

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

2.1 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.

2.2 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).

2.3 "Personal data" means any information relating to an identified or identifiable natural person, see article 4(1) GDPR. If other confidential information than personal data is processed for the purpose of fulfilling the Clauses, e.g. information considered confidential according to the Financial Business Act, any reference to "personal data" shall include this other confidential information.

2.4 In the context of the provision of providing a software-as-a-service employee advocacy solution, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

2.5 The Clauses shall take priority over any similar provisions contained in other agreements between the parties. If further obligations for the data processor have been set out in another agreement between the parties, for example by Standard Contractual Clauses as referred to in article 46(2)(c) and (d) GDPR, these further obligations will apply in addition to the Clauses.

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

2.7 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.

2.8 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.

2.9 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.

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

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

2.12 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

3.1 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.

3.2 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".

3.3 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

4.1 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.

4.2 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.

4.3 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 or other law to which the data processor is subject.

4.4 The data processor cannot condition the full and unlimited compliance with the data controller's instruction on the data controller's payment of outstanding invoices etc., and the data processor has no right of retention in the personal data.

5 CONFIDENTIALITY

5.1 The data processor shall keep the personal data confidential.

5.2 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 shall be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

5.3 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.

5.4 If the data processor is a legal entity, these Clauses apply to any persons under the data processor's authority, and the data processor warrants that such persons with access to the personal data, comply with the Clauses.

5.5 The obligations of the data processor under Clause 5 shall persist without time limitation and regardless of whether the cooperation of the parties has been terminated.

6 SECURITY OF PROCESSING

6.1 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.

6.2 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.

6.3 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 activity entrusted to it by the data controller 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.

6.4 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.

6.5 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

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

7.2 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.

7.3 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 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). The data controller has the right to object to the use of a sub-processor without cause. The data processor must inform the data controller in writing of the discontinued use of a sub-processor. 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.

7.4 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.

7.5 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.

7.6 If the sub-processor does not fulfil his data protection obligations, the data processor shall remain 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

8.1 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.

8.2 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 in writing prior to processing unless that requirement prohibits such information on important grounds of public interest.

8.3 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

8.4 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.

8.5 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.

8.6 If the data controller in Appendix C.6 has instructed the data processor to transfer personal data to a third country, the data processor must ensure that the described legal basis for the transfer, e.g. Standard Contractual Clauses as referred to in article 46(2)(c) and (d) GDPR, has been concluded between the relevant parties.

9 ASSISTANCE TO THE DATA CONTROLLER

9.1 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

9.2 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, The Danish Data Protection Agency (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, The Danish Data Protection Agency (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.

9.3 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

10.1 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.

10.2 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.

10.3 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.

10.4 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

11.1 On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

11.2 The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

12 AUDIT AND INSPECTION

12.1 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.

12.2 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.

12.3 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

13.1 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

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

14.2 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.

14.3 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.

14.4 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.

14.5 Signature

On behalf of the data processor

Name	Per John Jensen
Position	CEO
Date	25/8 - 2024

Signature

15 DATA CONTROLLER AND DATA PROCESSOR CONTACTS/CONTACT POINTS

15.1 The parties may contact each other using the following contacts/contact points:

15.2 The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

On behalf of the Data controller:

[Customer]

On behalf of the Data processor:

Name	Emil Devantie
Position	CTO
Telephone	+45 29931249
E-mail	emil@sociuu.com

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 processor provides a employee advocacy platform, in which the data controller creates and maintains relevant information to the area. The data may only be processed by the data processor according to instructions from the data controller.

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 process' the data controllers' data in connection with the following tasks:

- Hosting of the employee advocacy platform
- Remote access related to debugging and upgrading the platform.
- Consultancy on the use of the platform

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

I: Name, Title, company subdivision/work group, work email address

II: Name, Title, company subdivision/work group, work email address

If Customer has Social Connect enabled, the following meta data will be processed in addition:

I & II: Socialmedia post engagement statistics, socialmedia post reactions, socialmedia post reshares

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

I: Current Customer employees

II: Former Customer employees

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 of personal data follows the length and the termination of the main agreement.

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	CVR	ADDRESS	DESCRIPTION OF PROCESSING	LOCATION(S) OF PROCESSING
T-Systems Intenational GmbH	118 645 675	Am Schiens 10, 39221 Bördeland, Germany And Lübecker Str. 2, 39124 Magdeburg, Germany	System processing and data storage	Germany
Flowmailer	62 15 48 85	Flowmailer B.V Van Nelleweg 1 3044 BC Rotter-dam, The Nether-lands	SMTP service	The Netherlands

The data controller has on the effective date of the Clauses authorised the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled 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.

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 following:

The data controller hereby instructs the data processor to process the data controller's personal data for operation of the employee advocacy platform, as a Software-as-a-service cf. the main agreement.

C.2. Security of processing

The data processor shall be entitled and under obligation to make decisions about the technical and organisational security measures that are to be implemented to establish the necessary (and agreed) level of data security.

In this connection, the data processor must assess the extent to which it is necessary to implement the measures in the following areas, cf. the information security standard ISO 27001:2013:

- Information security policies;
- Organization of information security;
- Personnel safety;
- Management of information assets;
- Access control;
- Cryptography;
- Physical protection and environmental protection;
- Reliability;
- Communication security;
- Acquisition, development and maintenance of systems;
- Supplier relations;
- Management of information security breaches;
- Emergency, emergency and re-establishment management; and
- Compliance with legal and contractual requirements.

However, the data processor must - in any case and as a minimum - implement the following measures, which have been agreed with the data controller:

(i) Based on the identified risks for the rights and freedoms of data subject pursuant to Article 32 GDPR and Clause 6.2., the data processor shall define a set of policies for security of processing, which must be approved by the data processor's management, published and communicated to the employees, any sub-processors and to the data controller;

(ii) The data processor shall require all employees and contractors to apply security of processing in accordance with the established policies and procedures of the organisation;

(iii) The data processor shall ensure that all employees, and where relevant contractors, receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function;

(iv) The data processor shall implement technical and organisational measures to ensure that its employees, any sub-processor's employees and external parties, are only granted access to personal data on a need-to-know basis, as relevant for their job function. Such measures must include identification and authorisation of persons who are granted access, along with regular reviews of the assigned access rights;

(v) The data processor shall log access to personal data. Such log information and logging facilities must be regularly reviewed and protected against unauthorised access;

(vi) Access to systems and applications associated with processing of personal data shall be controlled by a secure log-on procedure, and the data processor shall adopt a policy for the use of secret authentication information (passwords);

(vii) The data processor shall design and apply physical security and protection to locations where personal data is processed to prevent unauthorised access to or manipulation of personal data;

(viii) The data processor shall ensure that the transmission of personal data through external communication channels is encrypted by a strong encryption based on acknowledged algorithms;

(ix) The data processor shall implement measures and adopt policies to ensure that personal data is effectively deleted upon the expiration of the data controller's retention period;

(x) The data processor shall implement procedures for the management of removable media based on the type of personal data associated with the media and dispose of such media securely when no longer required;

(xi) The data processor shall implement technical and organisational measures that ensure correct and secure operation of facilities and systems associated with processing of personal data. Such measures must include protection against execution of malicious code on systems used for processing of personal data and regular backup of such systems;

(xii) The data processor shall adopt contingency plans and procedures to ensure the ability to restore the availability and access to personal data in a timely manner in the event of an incident; and

(xiii) The data processor shall adopt a policy for regular testing, assessment and evaluation of the effectiveness of the implemented technical and organisational measures.

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, by request of the data controller, and for payment, help fulfil the data controllers obligations in relation to the data subjects rights, including responding to right of access requests, the right to data portability, the right to rectification, the right to erasure, the right to restriction of processing, as well as the data controllers obligations to notify the data subjects of a security breach, in accordance with Chapter III of the General Data protection Regulation, as well as article 34.

The data processor must, for payment, assist the data controllers' obligations under articles 32-36 of the General Data Protection Regulation, on security of processing, personal data breach and any notification to the Supervisory authorities and the data subject. The data processor must under the same conditions assist the data controller with data protection impact assessments.

C.4. Storage period/erasure procedures

Personal data is stored in accordance with the data controller's retention period, as the data controller is in full control of deletion functionalities.

Upon termination of the provision of personal data processing services, the data processor shall either delete the Personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5. Processing location

Subject to Clause 7, processing of the personal data under the Clauses cannot be performed at other locations than the following:

Sociuu ApS

Ryesgade 3B
2200 København N
Denmark

Refer to the list in Annex B.1 above.

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 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

To ensure the data processor's compliance with the GDPR, the applicable EU or Member State data protection provision and the Clauses, the data controller shall annually obtain information from the data processor concerning the data processor's obligations in relation to the personal data processing services with which the data processor has been assigned.

Based on the results of such information, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller or the data controller's representative shall in addition have access to inspect, includ-ing physically inspect, the places, where the processing of personal data is carried out by the data pro-cessor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required.

The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

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

The data processor shall, on the basis of an assessment of the risks to the rights and freedoms of the data subjects related to the specific processing activities to be carried out by sub-processor, determine how the data processor will audit sub-processors' compliance with the GDPR, the applicable EU or Member State data protection provisions and any Clauses which the data processor has agreed with the sub-processor.

Further, the data processor shall determine how often the data processor will audit those sub-processors.

Subsequently, the data processor shall audit those sub-processors according to the determined extent and at the determined intervals to ensure that those sub-processors comply with the GDPR, the applicable EU or Member State data protection provisions and any Clauses which the data processor has agreed with the sub-processor.