

Document V210101

STRICTLY CONFIDENTIAL - LEGAL PRIVILEGE

DATA PROCESSING AGREEMENT

Between [CUSTOMER]

and Sociuu ApS

This data processing agreement (the "Agreement") is entered into between:

- (A) The [Customer], using the Sociuu software platform in accordance with agreed GTC "General Terms and Conditions)
- (B) Sociuu ApS, a company incorporated in Denmark under the register no. 37652210 at the Danish Business Authority, at Ryesgade 3 B, DK-2200 København K.

- The Customer and the Supplier hereinafter collectively referred to as the "Parties" and separately as a "Party"

1. SCOPE OF THE AGREEMENT

- 1.1. This Agreement forms part of the agreement between the Customer and the Supplier to reflect the parties' agreement with regard to the processing of personal data.
- 1.2. The Supplier acts as a data processor for the Customer, as the Supplier process personal data for the Customer as set out in Annex 1.
- 1.3. The personal data to be processed by the Supplier concerns the categories of data, the categories of data subjects and the purposes of the processing set out in Annex 1.
- 1.4. "Personal data" means any information relating to an identified or identifiable natural person, see article 4(1) of Regulation (EU) 2016/679 of 27 April 2016 (the General Data Protection Regulation "GDPR"). If other confidential information than personal data is processed for the purpose of fulfilling the Agreement, e.g. information considered confidential according to the Financial Business Act, any reference to "personal data" shall include the other confidential information.

2. PROCESSING OF PERSONAL DATA

- 2.1. Instructions: The Supplier is instructed to process the personal data only for the purposes of providing the data processing services set out in Annex 1. The Supplier may not process or use the Customer's personal data for any other purpose than provided in the instructions, including the transfer of personal data to any third country or an international organisation, unless the Supplier is required to do so according to Union or member state law. In that case, the Supplier shall inform the Customer in writing of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
- 2.2. If the Customer in the instructions in Annex 1 or otherwise has given permission to a transfer of personal data to a third country or to international organisations, the Supplier must ensure that there is a legal basis for the transfer, e.g. the EU Commission's Standard Contractual Clauses for the transfer of personal data to third countries.
- 2.3. If the Supplier considers an instruction from the Customer to be in violation of the GDPR, or other Union or member state data protection provisions, the Supplier shall immediately inform the Customer in writing about this.
- 2.4. If the Supplier is subject to legislation of a third country, the Supplier declares not to be aware of the mentioned legislation preventing the Supplier from fulfilling the Agreement, and that the Supplier will notify the Customer in writing without undue delay, if the Supplier becomes aware of that such hindrance is present or will occur.

3. THE SUPPLIER'S GENERAL OBLIGATIONS

- 3.1. The Supplier must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- 3.2. The Supplier shall implement appropriate technical and organisational measures to prevent that the personal data processed is
 - (i) accidentally or unlawfully destroyed, lost or altered,
 - (ii) disclosed or made available without authorisation, or

- (iii) otherwise processed in violation of applicable laws, including the GDPR.
- 3.3. The Supplier must also comply with the special data security requirements that apply to the Customer, see Annex 1, and with any other applicable data security requirements that are directly incumbent on the Supplier; including the data security requirements in the country of establishment of the Supplier, or in the country where the data processing will be performed.
- 3.4. The appropriate technical and organisational security measures must be determined with due regard for
- (i) the current state of the art,
 - (ii) the cost of their implementation, and
 - (iii) 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.
- 3.5. The Supplier shall upon request provide the Customer with sufficient information to enable the Customer to ensure that the Supplier complies with its obligations under the Agreement, including ensuring that the appropriate technical and organisational security measures have been implemented.
- 3.6. The Supplier shall in December each year at its own cost obtain and forward documentation regarding the Supplier's compliance with the data security requirements under the Agreement. The documentation must be forwarded to the Customer by 31 December of the pertinent year.
- 3.7. Furthermore, the Customer is entitled at its own cost to appoint an independent expert who shall have access to the Supplier's data processing facilities and receive the necessary information in order to be able to audit whether the Supplier complies with its obligations under the Agreement, including ensuring that the appropriate technical and organisational security measures have been implemented. The expert shall upon the Supplier's request sign a customary non-disclosure agreement, and treat all information obtained or received from the Supplier confidentially, and may only share the information with the Customer.
- 3.8. The Supplier must provide information related to the provision of the services to authorities or the Customer's external advisors, including auditors, if this is necessary for the performance of their duties in accordance with Union or member state law.
- 3.9. The Supplier must give authorities who by union or member state law have a right to enter the Customer's or the Customer's supplier's facilities, or representatives of the authorities, access to the Supplier's physical facilities against proper proof of identity.
- 3.10. The Supplier must without undue delay after becoming aware of the facts in writing notify the Customer about:
- (i) any request for disclosure of personal data processed under the Agreement by authorities, unless expressly prohibited under Union or member state law,
 - (ii) any suspicion or finding of (a) breach of security that results in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the Supplier under the Agreement, or (b) other failure to comply with the Supplier's obligations under Clause 3.2 and 3.3, or
 - (iii) any request for access to the personal data received directly from the data subjects or from third parties.
- 3.11. Taking into account the nature of the processing the Supplier must promptly assist the Customer with the handling of any requests from data subjects under Chapter III of the GDPR, including requests for access, rectification, blocking or deletion. The Supplier must also assist the controller by implementing appropriate technical and organisational measures, for the fulfilment of the Customer's obligation to respond to such requests.
- 3.12. The Supplier must assist the Customer with meeting the other obligations that may be incumbent on the Customer according to Union or member state law where the assistance of the Supplier is implied, and

where the assistance of the Supplier is necessary for the Customer to comply with its obligations. This includes, but is not limited to, at request to provide the Customer with all necessary information about an incident under Clause 3.10 (ii), and all necessary information for an impact assessment in accordance with article 35 and 36 of the GDPR.

- 3.13. Any services from the Supplier as set out in clause 3.7 to 3.9 and 3.11 to 3.12 are billable and will be charged in accordance with the price list made available to the Customer upon concluding this agreement.
- 3.14. In Annex 1, the Supplier has stated the physical location of the servers, service centers etc. used to provide the data processing services. The Supplier undertakes to keep the information about the physical location updated by providing a prior written notice of two months to the Customer. This does not require a formal amendment of Annex 1, prior written notice by mail or email suffices.

4. SUBSUPPLIERS

- 1. The Supplier may engage a sub-supplier. At the time of the Agreement, the Supplier uses the sub-suppliers set out in Annex 2. The Supplier undertakes to inform the Customer of any intended changes concerning the addition or replacement of a sub-supplier by providing a prior written notice of two months to the Customer. The Customer may object to the use of a sub-supplier without cause if such objection is relevant and reasoned in regards to data protection issues. If the objection is relevant and reasoned the Supplier will suggest two new sub-suppliers in order for the Customer to accept one of them. The Supplier must inform the Customer in writing of the discontinued use of a sub-supplier.
- 2. Prior to the engagement of a sub-supplier, the Supplier shall conclude a written agreement with the sub-supplier, in which at least the same data protection obligations as set out in the Agreement shall be imposed on the sub-supplier, including an obligation to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR.
- 3. The Customer has the right to receive a copy of the Supplier's agreement with the sub-supplier as regards the provisions related to data protection obligations. The Supplier shall remain fully liable to the Customer for the performance of the sub-supplier's obligations. The fact that the Customer has given consent to the Supplier's use of a sub-supplier is without prejudice for the Supplier's duty to comply with the Agreement.

2. CONFIDENTIALITY

- 2.1. The Supplier shall keep personal data confidential.
- 2.2. The Supplier shall not disclose the personal data to third parties or take copies of personal data unless strictly necessary for the performance of the Supplier's obligations towards the Customer according to the Agreement, and on condition that whoever personal data is disclosed to is familiar with the confidential nature of the data and has accepted to keep the personal data confidential in accordance with this Agreement.
- 2.3. If the Supplier is a legal entity all terms of the Agreement apply to any of the Supplier's employees and the Supplier must ensure that its employees comply with the Agreement.
- 2.4. The Supplier must limit the access to personal data to employees for whom access to said data is necessary to fulfil the Supplier's obligations towards the Customer.
- 2.5. The obligations of the Supplier under Clause 5 persist without time limitation and regardless of whether the cooperation of the Parties has been terminated.
- 2.6. The Customer shall treat confidential information received from the Supplier confidentially and may not unlawfully use or disclose the confidential information.

3. AMENDMENTS AND ASSIGNMENTS

- 3.1. The Parties may at any time agree to amend this Agreement. Amendments must be in writing.

- 3.2. The Supplier may not assign or transfer any of its rights or obligations arising from this Agreement without the Customer's prior, written consent.

4. TERM AND TERMINATION OF THE AGREEMENT

- 4.1. The Agreement enters into force when signed by both Parties and remains in force until terminated by one of the Parties.
- 4.2. Each party may terminate the Agreement upon 3 months written notice.
- 4.3. Regardless of the term of the Agreement, the Agreement shall be in force as long as the Supplier processes the personal data, for which the Customer is data controller.
- 4.4. In case of termination of the Agreement, regardless of the legal grounds therefore, the Supplier must provide the necessary transition services to the Customer. The Supplier is obliged to assist in a loyal way and as fast as possible with transferring the personal data to another supplier or return them to the Customer.
- 4.5. On the Customer's request the Supplier shall immediately transfer or delete (including anonymise) personal data, which the Supplier is processing for the Customer, unless Union or member state law requires storage of the personal data.
- 4.6. The Supplier is under no circumstances entitled to condition the full and unlimited compliance with the Customer's instructions on the Customer's payment of outstanding invoices etc., and the Supplier has no right of retention in the personal data.

5. PRIORITY

- 5.1. If any of the provisions of the Agreement conflict with the provisions of any other written or oral agreement concluded between the Parties, then the provisions of the Agreement shall prevail. However, the requirements in Clause 3 do not apply to the extent that the Parties in another agreement have set out stricter obligations for the Supplier. Furthermore the Agreement shall not apply if and to the extend the EU Commission's Standard Contractual Clauses for the transfer of personal data to third countries are concluded and such clauses set out stricter obligations for the Supplier and/or for sup-suppliers.
- 5.2. This Agreement does not determine the Customer's remuneration of the Supplier for the Supplier's services according to the Agreement.

- 0 -

For and on behalf of the Customer

Date:

Name:

Title:

For and on behalf of the Supplier

Date: 4/1 - 2021

Name: Per John Jensen

Title: CEO

ANNEX 1

This Annex constitutes the Customer's instruction to the Supplier in connection with the Supplier's data processing for the Customer, and is an integrated part of the Agreement.

The processing of personal data

a) Purpose and nature of the processing operations

The Supplier is providing an employee-advocacy it-solution for the Customer. The operation which is performed on the categories of personal data are: use, storage and consultation.

b) Categories of data subjects

I. Current Customer employees

II. Former Customer employees

c) Categories of personal data

Re b) I: Name

Re b) II: Title

Re b) III: Company subdivision/work group

Re b) IV: Work e-mail address

d) Special categories of data

Re b) I: None

e) Location(s), including name of country/countries of processing

Sociuu ApS, Ryegade 3 B, DK-2200 Copenhagen, Denmark, EU.

Amazon Web Services Inc., Frankfurt, Germany, EU



ANNEX 2

Subsuppliers

Amazon Web Services Inc., EU Datacenter - Frankfurt, Germany

- 0 -

A handwritten signature in black ink, located in the bottom right corner of the page. The signature is stylized and appears to be a combination of letters, possibly 'R' and 'A'.