Data Processing Agreement

(version July 1, 2020)

[Name of customer]
[Address]

Central Business Register (CVR/VAT) no.: INSERT
(the "Data Controller")

and

any.cloud a/s
Islands Brygge 41
2300 Copenhagen S
Denmark

Central Business Register (CVR/VAT) no.: DK31161509
(The "Data Processor")

(jointly the "Parties" and individually a "Party")

have entered the following data processing agreement (the "Agreement") on the Data Processor's processing of personal information on behalf of the Data Controller:

1. BACKGROUND, PURPOSE AND SCOPE

1.1 As part of the Data Controller's entering into an agreement on the delivery of services, as described in appendix 1 of the Agreement, the Data Processor processes personal information for which the Data Controller is responsible.

1.2 The Data Processor must comply with the legislative requirement from time to time for data processors, including from 25 May 2018, the General Data Protection Regulation (Regulation (EU) 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) with related acts and secondary national legislation.

1.3 It is a requirement in the personal data legislation that the Data Controller and the Data Processor enter into a written agreement on the processing to be performed; a so-called "data processing agreement". The Agreement constitutes such data processing agreement.

2. PERSONAL INFORMATION COVERED BY THE AGREEMENT

2.1 This Agreement and related instruction cover all types of personal data as described in appendix

1 to the Agreement.

3. GEOGRAPHIC REQUIREMENTS

3.1 The processing of personal data performed by the Data Processor according to agreement with the Data Controller, may only be performed by the Data Processor or data sub processors, see clause 5, within the European Economic Area (EEA). The Data Processor is in no way entitled to have data processing performed outside the EEA without the written consent of the Data Controller, unless required under EU law or the national law of the member states which the data processor is subject to; in such case, the Data Processor informs the Data Controller about this legal claim before processing unless the said law prohibits such notification for the purpose of important societal interests.

4. INSTRUCTION

4.1 The scope of the tasks which the Data Controller must provide and support means that under the Parties' agreement, various forms of processing of personal data will be performed. The various forms of data processing of personal data are described in appendix 1 to the Agreement.

4.2 The Data Processor only acts according to documented instruction from the Data Controller. The Data Processor must ensure that the entrusted personal data is not used for other purposes or processed in other ways than what appears from the Data Controller's instruction. All the described actions necessary for the processing of the Contract are considered documented. However, other processing may take place if required under EU law or the national law of the member states which the Data Processor is subject to; in such case, the Data Processor informs the Data Controller about this legal claim before processing unless the said law prohibits such notification for the purpose of important public interests.

4.3 If, in the Data Processor's opinion, an instruction is contrary to the legislation, the Data Processor must inform the Data Controller to that effect.

4.4 This Agreement and related instruction cover the categories of the data subjects specified in appendix 1.

4.5 If the processing of personal data with the Data Processor is performed in full or in part by the use of remote connection, including home offices, the Data Processor must establish guidelines for the employees' processing of personal data when using remote connection which must also comply with the requirements specified in the Agreement.

4.6 To the extent possible, the Data Processor must assist the Data Controller in complying with the Data Controller's obligations to reply to requests about exercise of the rights of the data subject, including on access, rectification, limitation or erasure if the relevant personal information is processed by the Data Processor. If the Data Processor receives such communication from the data subject, the Data Processor informs the Data Controller to that effect.

4.7 The Data Controller is liable for all the Data Processor's costs for such assistance, see clause 4.6, including for the data sub-processor. The Data Processor's assistance is invoiced at the Data Processor's hourly rate applicable from time to time for such work.

5. USE OF A DATA SUB-PROCESSOR

5.1 The Data Controller grants the Data Processor consent to use data sub-processors, provided that the conditions specified in the Agreement have been complied with. The Data Processor informs the Data Controller of such data sub-processors.

5.2 The data sub-processor is subject to the instruction of the Data Processor. The Data Processor has entered into a written data processing agreement with the data sub-processor in which it has been ensured that the data sub-processor fulfils requirements corresponding to those required from the Data Processor by the Data Controller under the Agreement.

5.3 Costs incidental to the establishment of the contractual relationship with a data sub-processor, including costs for preparation of a data processing agreement and any establishment of a basis for transfer to third countries, are paid by the Data Processor and are thus of no concern to the Data Controller.

5.4 If the Data Controller wants to instruct data sub-processors directly, this should only be done after discussion with and via the Data Processor. If the Data Controller instructs data sub-processors directly, the Data Controller must, no later than simultaneously, inform the Data Processor of the instruction and the basis thereof. Where the Data Controller instructs data sub-processors directly, a) the Data Processor is released from any liability, and any result of such instruction is solely the liability of the Data Controller, b) the Data Controller is liable for any cost which the instruction may result in to the Data Processor, including the Data Processor is entitled to invoice the Data Controller with its usual hourly rate for all working time which such direct instruction may entail for the Data Processor, and c) the Data Controller is itself liable vis-à-vis data sub-processors for any cost, remuneration or other payment to the data sub-processor which the direct instruction may entail.

5.5 The Data Processor presently uses the data sub-processors specified in appendix 1 to the Agreement to handle the technical operation of the services.

5.6 On conclusion of this Agreement, the Data Controller accepts that the Data Processor is entitled to change sub-data processor on the condition that a) any new data sub-processor complies with similar conditions required in this clause 5 from the present data sub-processor and that b) no later than on the commencement of such data sub-processors processing of personal data which the Data Controller is responsible for, the Data Processor is informed by the Data Controller of the identity of the new data sub-processor.

5.7 If the Data Controller does not want that the Data Processor uses a new data sub-processor as notified, see clause 5.6, the Data Controller must object in writing to the Data Processor against the use of such new data sub-processor no later than 14 days after receipt of the information, see clause 5.6. In case the Data Processor does not find itself able to comply with any objection from the Data Controller against a new data sub-processor, the Data Controller must be informed as soon as possible, and in such case the Data Controller can terminate the Hosting Agreement to expire at the date stated in clause 5.6.

6. PROCESSING AND DISCLOSURE OF PERSONAL DATA

6.1 The Data Controller warrants to have the required authority to process the personal data comprised by this Agreement.

6.2 The Data Processor may not without the written consent of the Data Controller disclose information to a third party unless such disclosure follows from the legislation or from a binding request from a court or other data protection authority, or appears from this Agreement.

7. SAFETY

7.1 The Data Processor must make appropriate technical and organisational security measures against personal data being accidentally or unlawfully destroyed, lost or impaired, and coming to the knowledge of a third party, is abused or otherwise processed contrary to the law, see clause 1.2 above.

7.2 Data processor is a certified ISO 27001 with a valid certificate and must comply with the requirements for security specified in the ISO standards at all times. Further, according to clause 7.1, the Data Processor must implement and retain the security measures described in appendix 2 and otherwise comply with the demands made in the Contract. The security demands made in appendix 2 constitute the Data Controller's requirements in relation to security conditions with the Data Processor.

7.3 The Data Processor is always entitled to implement alternative security measures provided that such security measures as a minimum comply with or offer more security than the security measures described in the Hosting Certificate and appendix 2, see clause 7.2, and otherwise meet the security requirements in the Contract. The Data Processor cannot make any impairments of the security matters without the Data Controller's previous written approval.

7.4 If the Data Processor is established in another EU member state, the provisions regarding security measures provided in the laws of the EU member state in which the Data Processor is established must also apply to the Data Processor. If the Data Processor is established in another EU member state, the Data Processor must thus comply with both security measures covered by the applicable legislation in Denmark and security requirements in the Data Processor's home country. The same applies to sub-data processors.

7.5 The Data Processor must, according to agreement with the Data Controller, to the extent possible assist the Data Controller with ensuring observance of the obligations in article 32 of the regulation (taking of appropriate technical and organisational measures), 34 (communication to the data subjects about personal data breaches), 35 (carrying out of an impact assessment concerning data protection) and 36 (prior consultation). In this connection the Data Processor is entitled to invoice the Data Controller at its usual hourly rate for all the Data Processor's working hours which such agreement may entail for the Data Processor, and the Data Controller is liable for any payment to the data sub-processor.

7.6 If the specifications in clause 7.5 lead to tighter security measures relative to what has already been agreed by the parties in this Agreement, the Data Processor implements, where possible, such measures on the condition that the Data Processor receives payment for this, see clause 7.7 below.

7.7 Costs incidental to such implementation of measures, see clause 7.6, are paid by the Data Controller and are thus of no concern to the Data Processor. The Data Processor is also entitled to invoice the Data Controller at its usual hourly rate for all the Data Processor's working hours which such implementation may entail for the Data Processor, and the Data Controller is liable for any payment to the data sub-processor.

8. RIGHT OF MONITORING

8.1 At the request of the Data Controller, the Data Processor must provide the Data Controller with sufficient information for the Data Controller to ensure that the Data Processor complies with article 28 of the General Data Protection Regulation and this Agreement.

8.2 To the extent that the Data Controller also wants this to comprise the processing performed by data sub-processors, the Data Processor is informed thereof. Accordingly, the Data Processor will obtain sufficient information from the data sub-processor.

8.3 If the Data Controller wants to monitor as specified in this clause 8, the Data Controller must always give the Data Processor notice of at least 30 days in such connection.

8.4 The Data Processor must once a year at the request of the Data Controller arrange that a generally recognised and independent third party provides a security audit report prepared in compliance with a recognised auditing standard (e.g. ISAE 3402 with a frame of reference to ISO 27002:2014 or similar), to the Data Controller on observance of the security measures requirements in compliance with the Data Processor's certification with BFIH, see clause 7.3 above and appendix 2 of the Agreement. As a member of BFIH, the Data Processor is certified once a year to use the Hosting Certificate, which i.a. contains an ISAE 3402 with a frame of reference to ISO 27002. On the Data Processor's submission of a copy of the updated Hosting Certificate and related ISAE 3402 declaration with a frame of reference to ISO 27002, the Data Processor complies with the requirement in this provision.

8.5 The Data Controller is entitled to receive a copy of an annual security audit report describing the security conditions with the sub-data processor and which has been prepared in accordance with an acknowledged auditing standard (e.g. ISAE 3402 with a frame of reference to ISO 27002:2014 or similar) by a generally known and independent third party which is engaged in such matters. A copy of such safety audit report is sent on request to the Data Controller when the Data Processor has received such report from the sub-data processor.

8.6 If the Data Controller wants to have prepared other or further security audit report in addition to those mentioned in clauses 8.4 and 8.5, or monitoring of the Data Processor's or the data sub-processor's personal data processing is otherwise wanted, including if the Data Controller wants a security audit report prepared at a specific time, this is agreed in detail with the Data Processor. The Data Controller or the data sub-processor may always demand that such a security audit report is prepared in accordance with an acknowledged auditing standard (e.g. ISAE 3402 with a frame of reference to ISO 27002:2014 or similar) by a generally known and independent third party which is engaged in such matters.

8.7 The Data Controller pays all costs related to the monitoring of security conditions, as stated in clause 8.6, with the Data Processor and in relation to the data sub-processor, including that the Data Processor is entitled to invoice the Data Controller at its usual hourly rate for all the Data Processor's working hours which such monitoring may entail for the Data Processor, and the Data Controller is liable for any payment to the data sub-processor.

9. PERSONAL DATA, SECURITY BREACH

9.1 If the Data Processor becomes aware of such a personal data security breach, which means a security breach resulting in accidental or unlawful destruction, loss, change, unauthorised disclosure of or access to personal data, which has been transmitted, kept or otherwise processed, the Data Processor is obliged without undue delay to attempt to localise such breach and seek to mitigate damage occurred to the extent possible, and to the extent that it is possible to restore any lost data.

Costs related hereto are carried by the Data Processor, except in cases where the breach(es) of security can be proven to be caused by the Data Controller’s use of 3rd party software (including operating systems) or security breaches with the Data Controller in which access was forced to the Data Processor.

9.2 The Data Processor is further obliged, without undue delay, to notify the Data Controller after having become aware that breach of the personal data security has occurred. The Data Processor must then without undue delay, to the extent possible, provide written notification to the Data Controller, which to the extent possible must contain:

a) A description of the nature of the breach, including the categories and the approximate number of affected data subjects and registrations of personal data.

b) Name of and contact information of the data protection officer.

c) A description of the likely consequences of the breach.

d) A description of the measures made by the Data Processor or the sub-data processor or suggested to be made to handle the breach, including measures to mitigate its potential adverse effects.

9.3 If it is not possible to provide the information in clause 9.2 together, the information may be provided in steps without undue further delay.

9.4 Similarly, data sub-processors are under an obligation to inform the Data Processor in accordance with clauses 9.2 and 9.3 without undue delay.

10. DUTY OF CONFIDENTIALITY

10.1 The Data Processor must keep personal data confidential, and is thus only entitled to use the personal data as part of performing its obligations and rights under the Agreement. The Data Processor must ensure that the employees and any others, including data sub-processors, who are authorised to process the data covered in the Agreement, are under a duty of confidentiality. Such confidentiality also applies after expiry of the Agreement.

11. PRECEDENCE

11.1 Unless otherwise set out in the Agreement, provisions in the Agreement take precedence in relation to similar provisions in other agreements between the parties, including the Contract.

12. TERM AND TERMINATION OF THE DATA PROCESSING AGREEMENT

12.1 The Agreement enters into force on the Parties' signatures.

12.2 In the event that the Contract terminates, irrespective of the reason, this Agreement also terminates.

12.3 The Agreement cannot be terminated individually, but can be replaced by another data processing agreement about the same matters. If not, the Data Processor is bound by this Agreement as long as the Data Processor processes personal data on behalf of the Data Controller.

12.4 The Data Controller must as soon as possible and no later than 14 days after expiry of the Contract inform the Data Processor in writing whether the Data Processor must return or delete the personal data processed. 30 days after termination of the Hosting Agreement, the Data Processor is entitled to erase all personal information which has been processed under the terminated Contract on behalf of the Data Controller. However, the Data Processor may always keep the processed data if that follows from EU law or the national law of the member states. Any costs incurred by this are to be covered by the Data Controller.

13. SIGNATURE

13.1 The above is accepted with effect from the Parties' signatures.

13.2 This Agreement has been signed in two similar copies, of which each Party keeps one.

14. APPENDICES

Appendix 1:	Description of the background for and the purpose of the Agreement etc.
Appendix 2:	Description of security measures

Place and date

[name of the signor]
For the Data Controller

____

Place and date
Copenhagen, on dd.mm.yy

Adrian Frimodt-Møller
For the Data Processor

____