DATA PROCESSER AGREEMENT

Competella PC Reception
Ver. 1.0

Standard Contractual Clauses

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

Between

Customer (the data controller)

and

Nuuday A/S
CVR 40 07 52 91
Teglholmsgade 1
2450 København SV
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

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. The provisions have been entered into as a supplement to the "General Terms and Conditions for the delivery and operation of Nuuday Business Services" (the Main Agreement) according to which the data processor processes personal data on behalf of the data controller in accordance with these Provisions. The newest version of the Clauses shall be available at tdc.dk/vilkaar.

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

5. Five 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. Appendix E contains specification of Technical and organisational Security measures as referred to in appendix C.2.

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

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

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.

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 as documented in appendices A and C, unless required to do so by Union or Member State law to which the processor is subject.

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;

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

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 requires 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 notification of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform the data controller of any intended changes concerning the addition or replacement of sub-processors at least 14 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). 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.

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.

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.

6. 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.

7. 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, The Danish Data Protection Agency, 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, 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 36 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.

5. Signature

   The provisions form part of the Main Agreement and must therefore not be signed.

15. Data controller and data processor contacts/contact points

The data processor's data protection adviser can be contacted by e-mail: dpo@nuuday.dk

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:

- Competella is an attendant / switchboard and contact solution placed on top of Skype for business.

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):

- Competella is providing easy and intuitive call handling functionality, so users / agents can easily process their needs with for handle phone calls, transfer to available and correct colleagues.

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

- Name
- Phone number
- Organisation
- Mail address
- Department
- Call handling
- Status / presence / free-busy
- Call history
- Call statistics

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

- Customers employees
- Persons who a call is done wit

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:

- Until termination of contract between customer and Nuuday A/S of delivering the service 'Competella PC Reception'

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
Competella Sweden AB (HQ)	Org. No. 556781-5070	Fleminggatan 48 112 33 Stockholm +46 8 465 010	Service and support

Upon the entry into the agreement, the data controller has approved the use of the above-mentioned sub-data processors for the described processing activity. The data processor is entitled to use other sub-data processors after the notification about these new sub-data processors has been publicly available on tdc.dk/vilkaar/ for at least 14 days before the sub-data processor is used.

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:

- Delivery, support and hosting of Competella PC Reception

C.2. Security of processing

I addition to the security measures described under Clause 6 the data processor shall adhere to the security measures described in Appendix E Security Controls.

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:

- As the data processor provides a self-service solution, the data controller has the ability to fulfil the data subject's rights as set out in Chapter III of the General Data Protection Regulation. If the data controller requests additional assistance in this regard, the data controller will be billed by the data processor at the usual hourly rate

C.4. Storage period/erasure procedures

- Upon termination of the processing of personal data for the data controller, data shall, in accordance with the agreement with the data controller, been:
    - Deleted if this is not in conflict with other legislation.

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:

- Nuuday datacenter – Interxion, Industriparken 20A, 2750 Ballerup

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

The personal data may not be transferred to a non-EU/EEA country unless prior written approval to such transfer has been explicitly granted by the data controller. If required by law or upon the data controller's request, the data processor shall enter into the EU Commission's Standard Contractual Sections (or subsequent versions thereof) for the transfer of personal data from data controllers to data processors located in non-EU/EEA countries in accordance with the EU 95/46 Data Protection Directive as specified in the EU Commission's Decision of 5 February 2010 as amended. If, following the application of the General Data Protection Regulation, cf. above, or upon the data controller's request, new versions of the standard contractual clauses must be adopted, the data processor must conclude such new clauses, either as new agreements or in replacement of already existing agreements. The data processor must at all times ensure that a transfer is lawful, and that all required approvals and notifications to the relevant supervisory authority regarding such transfer have been adequately obtained and made.

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 annually provide, free of charge, a statement of assurance from an independent third party concerning the Data Processor's compliance with the Data Protection Regulation, data protection provisions of other Union or national law of the Member States and these Provisions for the Data Controller.

The audit statement shall be published at https://tdc.dk/vilkaar subsection 14. Revisionserklæring.
If the data controller requests further information in connection with an audit of the data processor, the data processor must give the data controller access to these against payment of the data processor's reasonable costs in connection therewith.

In addition, the data controller or a representative of the data controller has, against payment of the data processor's reasonable costs in connection therewith, access to carry out inspections, including physical inspections, with the premises from which the data processor processes personal data, including physical locations and systems used to or in connection with the treatment. Such inspections may be carried out whenever the Data Controller deems it necessary.

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

N/A

Appendix D The parties' terms of agreement on other subjects

1. Confidentiality

1.1 Notwithstanding the contents of the Clauses, the Main Contract is confidential between the Parties to the effect that any sub-processors may only be informed of the contents of the Clauses and only to the extent necessary.

2. Instruction

2.1 The data processor must immediately inform the data controller if the data processor processes fully or partially the personal data in a way that may cause liability for the data controller. If so, the data processor must provide information on the matter, including on concerned data subjects, the personal data, the purpose of the processing and all other information requested by the data controller

3. Information

3.1 To the extent relevant, the data controller must inform the data processor of any legislation other than the general personal data legislation in the EEA, as for example any special, local requirements for the storage of personal data in the country of the data controller. If such special legislation flows down and imposes more obligations on the data processor than the general personal data legislation, the data controller shall indemnify the data processor for increased, documented additional costs for any such adaption. In that respect, no consideration shall be taken to the circumstances of other customers, including any payments made by such customers.

4. Liability and indemnity

4.1 This clause 4 supplements the provisions on liability of the Main Contract

4.2 In the event that liability to pay damages, compensation, tort or the like to data subjects, other relevant data subjects or third parties, has been imposed on the data processor due to violations of data protection legislation, this Agreement, privacy notices or instructions to the data processor or the like, and the data controller is fully or partly responsible for such violation, the data controller shall indemnify the data processor with a proportionate share of the amount (including any related costs or fees) corresponding to the proportionate share of liability that is incumbent on the data controller.

4.3 If the data processor has been imposed to pay an administrative fine, fines or the like to public authorities, the state treasury or the Danish Labour Court (Arbejdsretten) or the like, due to a violation of data protection legislation, the Clauses, privacy notices, instructions to the data processor, or the like, and the data controller is fully or partly responsible for such violation, the data controller shall indemnify the data processor with a proportionate share of the amount (and any related costs and fees) corresponding to the proportionate share of liability that is incumbent on the data controller.

4.4 The data controller shall take all steps necessary to defend any claim of infringement or alleged infringement of applicable data protection legislation.

4.5 This clause 4 is not subject to any limitations on liability or payment of damages set out in the Main Contract.

5. Fees to the Data Processor

5.1 The data controller shall also indemnify the data processor for significantly increased, documented additional costs due to changes in current legislation, including interpretations thereof. In that respect, no consideration shall be taken to the circumstances of other customers, including any payments made by such customers.

6. Severability

6.1 Should any provision of the Clauses be held to be unenforceable, illegal or invalid, such provision may by good faith negotiations or interpretation be replaced by provisions that to the widest extent possible gives effect to the intent and enforcement of the original provisions. If that is not possible, such term or provision shall to that extent be deemed not to form part of the Clauses. All other terms and conditions of the Clauses shall remain in full force and effect.

Appendix E Technical and organisational Security measures

(Based upon Technical and organisational Security controls from Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement)

Procedures and controls to be complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

1. Written procedures shall be in place which include a requirement that security measures agreed are established for the processing of personal data in accordance with the data processer agreement. Assessments shall made on a regular basis – and at least once a year – as to whether the procedures should be updated.
2. The data processor shall have performed a risk assessment and based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller.
3. For systems and databases used in the processing of personal data, antivirus software has to be installed and updated on a regular basis.
4. External access to systems and databases used in the processing of personal data shall takes place through a secured firewall.
5. Internal networks shall be segmented to ensure restricted access to systems and databases used in the processing of personal data.
6. Access to personal data shall be isolated to users with a work-related need for such access.
7. For the systems and databases used in the processing of personal data, system monitoring (syslog) shall be established.
8. Effective encryption shall be applied when transmitting confidential and sensitive personal data through the internet or by email.
9. Logging shall be established in systems, databases and networks handling and or transmitting confidential and sensitive personal data:
    - Activities performed by system administrators and others with special privileges
    - Security incidents include:
        i. Changes to log settings, including disabling logging
        ii. Changes in system rights for users
        iii. Failed log-on attempts on systems, databases, and networks
        iv. Log information is protected against tampering and technical errors and is reviewed on an ongoing basis.

    Log data shall be protected against manipulation and technical errors and are reviewed regularly.
10. Personal data used for development, testing or similar activity shall always be (if possible) in pseudonymised or anonymised form. Such use may only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.
11. The technical measures established shall be tested in vulnerability scans on a regular basis or when major changes have been implemented.
12. Changes to systems, databases or networks shall be made consistently with established procedures that ensure maintenance using relevant updates and patches, including security patches.
13. A formalised procedure shall be in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.
14. Access to systems and databases involving high risks for data subjects shall be authorised use two-factor authentication.
15. Physical access safeguards shall be established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.

Procedures and controls to be complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

1. Management of the data processer shall have approved a written information security policy that has been communicated to all relevant stakeholders, including data processer's employees. The IT security policy shall be based on a risk assessment performed. Assessments shall be made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.
2. Management of the data processer shall ensure that the information security policy does not conflict with data processing agreements entered into.
3. The employees of data processer shall be screened as part of the employment process. Such screening comprises, as relevant:
    - References from former employers
    - Certificates of criminal record
    - Driver´s license
4. Upon appointment, employees shall sign a confidentiality agreement. In addition, the employees shall be introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.
5. For resignations or dismissals, the data processor shall have implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.
6. Upon resignation or dismissal, employees shall be informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by data processer for the data controllers.
7. Awareness training shall be provided to data processer's employees on a regular basis with respect to general IT security and security of processing related to personal data.