SUB DATA PROCESSING AGREEMENT

QualiWare ApS

Date: 28 May 2018

1 Parties

1.1 This agreement on collection, storage and use of documents and information (hereinafter the ”Sub Data Processing Agreement”) has been signed by and between

QualiWare ApS
Company reg. no. 30731557
Ryttermarken 15
DK-3250 Farum
Denmark
(hereinafter referred to as the ”Data Processor”)

and co-signed

[Customer name]
CVR.no. [No]
[Address]
DK-[Address]
Denmark
(hereinafter referred to as ”Sub Data Processor”)

(hereinafter jointly referred to as the ”Parties” and individually as ”Party”)

2 DEFINITIONS

2.1 Terms and expressions with capital first letters used in this Sub Data Processing Agreement shall have the meanings set out in the General Data Protection Regulation (EU Regulation 2016/679 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, hereinafter the "GDPR") or the meanings otherwise defined in this Sub Data Processing Agreement.

2.2 “Data Subject” shall mean the identified or identifiable natural person to whom Personal Data refers.

2.3 “Pre-approved Subcontractors” shall be the subcontractors of Sub Data Processor, stated in Appendix 1.

2.4 “Third party” shall mean a natural or legal person, public authority, agency or body other than the Data Subject, the Data Controller, Sub Data Processor, the Data Processor and

persons who, under the direct authority of the Sub Data Processor or Data Processor, are authorized to process Personal Data.

2.5 "Sales and Delivery Terms" shall mean the agreement on supply of IT services entered into by and between the Sub Data Processor and the Data Processor on the date:

3 SCOPE

3.1 This Sub Data Processing Agreement concerns the Parties' obligations in regards to processing of Personal Data.

3.2 Under this Sub Data Processing Agreement, the Data Processor shall solely or jointly with other parties decide for what purpose and by use of what tools Personal Data may be processed. Data Processor shall instruct the Sub Data Processor hereon.

3.3 This Sub Data Processing Agreement shall apply to all the Sub Data Processor's current and future deliveries under the Sales and Delivery Terms to all companies within Data Processor's group of companies, for whom the Sub Data Processor processes Personal Data.

3.4 This Sub Data Processing Agreement shall supplement and form part of the Sales and Delivery Terms. In case of any inconsistencies between this Sub Data Processing Agreement and the Sales and Delivery Terms, this Sub Data Processing Agreement shall prevail.

3.5 Until 24 May 2018 the Sub Data Processor shall comply with the Danish Act on Processing of Personal Data (law no. 421 of 31 May 2000 with amendments), including associated Danish executive orders.

3.6 As of 25 May 2018, the Sub Data Processor shall comply with the GDPR, including other applicable national Danish legislation issued according to the GDPR or as a supplement hereto.

3.7 Any Personal data processed pursuant to this Sub Data Processing Agreement is proprietary to the Data Processor.

4 PRIOR SPECIFIC OR GENERAL WRITTEN AUTHORISATION

4.1 Sub Data Processor shall process Personal Data on behalf of Data Processor. Data Processor has received its instructions in regards to the Personal Data from the Controller, which is a customer to the Data Processor.

4.2 Data Processor instructs the Sub Data Processor to process the Personal Data to provide its services under the Sale and Delivery Terms.

4.3 If the Sub Data Processor considers that any instructions from the Data Processor contravene or infringe statutory regulations, including the GDPR or other EU or applicable member state data protection provisions, the Sub Data Processor must notify the Data Processor hereof immediately.

4.4 The Sub Data Processor is not entitled to make use of Personal Data, information or otherwise provided by Data Processor, for purposes other than fulfilment of this Sub Data Processing Agreement. The Sub Data Processor may not use such Personal Data for historical, statistical, scientific or similar purposes, whether anonymized or in any other way.

5 GEOGRAPHICAL LIMITATIONS

5.1 The Sub Data Processor is not allowed to transfer, access, process or otherwise make available Personal Data in countries outside the EU/EEA.

5.2 The Sub Data Processor can transfer, access, process or otherwise make personal data available to Pre-Approved Subcontractors listed in Appendix 1. Any such agreements with Pre-Approved Subcontractors outside the EU or EEA shall – prior to any transfer of data - be entered into pursuant to the EU Commission's decision of 2010/87/EU regarding the standard model contract for transfer of personal data to countries outside the EU or EEA in addition to any permission from local authorities if legally required.

6 CONFIDENTIALITY

6.1 The Parties accept, both for the duration of this Sub Data Processing Agreement and subsequently, not to disclose any Confidential Information to a Third Party. This non-disclosure obligation shall not apply to information which (a) or (b) information which a Party document has been created by the Party itself.

6.2 "Confidential Information" means all information of a technical, business, infra structural or similar nature, irrespective of whether this information has been documented, except for information which is or will be made available in another way than through breach of this Sub Data Processing Agreement and all Personal Data.

6.3 The Parties shall ensure that employees and consultants who receive Confidential Information are obliged to accept a similar obligation regarding Confidential Information from the other Party and the cooperation in general in accordance with this Sub Data Processing Agreement.

6.4 The Sub Data Processor must further ensure that all people with access to Personal Data being processed on behalf of Data Processor are familiar with this Sub Data Processing Agreement and are subject to the provisions of this Sub Data Processing Agreement.

7 DATA PROCESSOR'S IT SECURITY POLICIES

7.1 The Sub Data Processor shall comply with Data Processor's IT Security Policies, stated in Appendix 2. Data Processor shall inform Sub Data Processor in writing each time a change has been made to the Data Processor's IT Security Policies before such changes takes effect. Upon written request, Data Processor shall inform Sub Data Processor of the content of any such changes made to the Data Processor's IT Security Policies.

7.2 The Sub Data Processor must always provide supervisory authorities and Data Processor with the necessary access to and insight into the Personal Data which is being processed and the systems used.

8 APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES

8.1 The Sub Data Processor must implement appropriate and reasonable technical and organizational measures to ensure a level of security that matches the risks of data processing for the processing of Personal Data which the Data Processor provides under this Sub Data Processing Agreement, including reasonably ensuring a) Pseudonymisation and encryption of Personal Data; b) continuous confidentiality, integrity, availability and robustness of the processing systems and services for which the Sub Data Processor is responsible; c) timely recovery of the availability of and access to Personal Data in case of a physical or technical incident; d) a procedure for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure processing security; e) that Personal Data is not accidentally or unlawfully destroyed, lost or impaired and against any unauthorized disclosure, abuse or in any other way is processed in violation of any applicable law on Personal Data.

8.2 The Sub Data Processor shall determine the appropriate level of technical and organizational measures. When determining this, the Sub Data Processor must particularly consider the risks related to the processing, i.e. the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Data which has been transmitted, stored or processed in any other way.

8.3 Sub Data Processor shall, upon prior written request from the Data Processor, and within reasonable time-limits provide the Data Processor with sufficient information to document that the abovementioned technical and organizational security measures have been taken.

9 TRANSPARENT INFORMATION AND COMMUNICATION

9.1 The Sub Data Processor must continuously report to Data Processor with the agreed contents, quality and frequency. The Sub Data Processor must immediately inform Data Processor of any development which may significantly impair the Sub Data Processor's current or future ability or possibility to comply with the Sub Data Processing Agreement.

9.2 The Sub Data Processor is obliged to inform Data Processor immediately, if the Sub Data Processor is not able to ensure the correct processing of Data Processors Personal Data in accordance with this Sub Data Processing Agreement.

10 DATA SUBJECTS RIGHTS

10.1 Sub Data Processor shall upon request from the Data Processor and without undue delay provide all reasonable requested information and assistance to the Data Processor in regards to the Data Subject's rights on the following items: (1) processing security known to the Sub Data Processor for any processing of Personal Data which is not provided directly by Sub Data Processor or a Pre-Approved Subcontractor, (2) notification to the supervisory authority of any Data Security Breach, (3) notification to the Data Subject of any Data Security Breach, (4) consequential analysis of data protection and (5) preliminary hearing.

10.2 Sub Data Processor shall also upon request from the Data Processor provide all reasonable requested information and assistance to the Data Processor in regards to the Data Subject's rights without undue delay on the following items: (1) the duty to inform when collecting Personal Data from the Data Subject, (2) the duty to inform if the Personal Data has not been collected from the Data Subject, (3) the Data Subject's right to access Personal Data, (4) the right to correct Personal Data, (5) the right to be deleted (»the right

to be forgotten«), (6) the right to limitation of processing; (7) the duty to notify in connection with corrections or deletions of Personal Data or limitations in the processing activity, (8) the right to data portability and (9) the right to object for processing of Personal Data.

11 DATA SECURITY BREACH

11.1 In case of a Data Security Breach for which the Sub Data Processor (or any Pre-Approved Subcontractor) is responsible, the Sub Data Processor shall as soon as practical possible, inform Data Processor hereof.

11.2 This notification must at least:

a) include a description of the nature of the Data Security Breach including, if possible, the categories and the estimated number of affected Data Subjects as well as the categories and estimated number of affected registrations of Personal Data,

b) include the name of and contact information for the data protection officer (DPO) or another point of contact where further information may be obtained,

c) describe the probable consequences of the Data Security Breach,

d) describe the measures taken by the Sub Data Processor or which the Sub Data Processor proposes are taken to handle the Data Security Breach including, if relevant, measures to limit the possible consequential damages.

11.3 The Sub Data Processor must document all Data Security Breaches, including the actual circumstances surrounding the Data Security Breach, its consequences and the remedial measures that have been taken.

11.4 This documentation must enable the regulatory authority to check that Sub Data Processor complies with its duty to inform of any Data Security Breach.

12 USE OF SUBCONTRACTORS

12.1 The Sub Data Processor may not use any subcontractors without Data Processor’s prior written approval.

12.2 Data Processor has provided its consent to Sub Data Processor using the Pre-Approved Subcontractors as subcontractors.

12.3 The Sub Data Processor must inform Data Processor of any plans to either add or replace Pre-Approved Subcontractors. No sub Sub Data Processor may be added to the list of the Pre-Approved Subcontractors without Data Processors prior written approval.

12.4 If the Sub Data Processor uses a subcontractor to carry out specific processing activities on behalf of Data Processor, the same data protection obligations as are described in this Sub Data Processing Agreement shall be imposed on the subcontractor in a written agreement.

12.5 If the subcontractor does not comply with the provisions of this Sub Data Processing Agreement, the Sub Data Processor will be liable for the subcontractor's actions or failures to act/breach on the same terms as for its own services.

12.6 The Sub Data Processor is obliged to inform its subcontractors of the provisions of this Sub Data Processing Agreement.

13 DELIVERY OF PERSONAL DATA

13.1 During the term of this Sub Data Processing Agreement, Data Processor has full access to any Personal Data being processed by the Sub Data Processor.

13.2 If Data Processor so requests, the Sub Data Processor is obliged to keep a back-up copy of Personal Data and additional information available in the Sub Data Processor's systems for up to 3 months after the expiry or termination of the Sub Data Processing Agreement. Provided such request has been made, the Data Processor may, until the expiration of such 3-month period and irrespective of the reason for the expiry of the Sub Data Processing Agreement, request for an access to any Personal Data and additional information recorded in such back-up copy.

13.3 Sub Data Processor may only disclose Personal Data and information to Data Processor and/or to a third party appointed by Data Processor.

13.4 The Sub Data Processor must upon Data Processor's written instructions delete Personal Data or any information which has come to the Sub Data Processor's possession under the Sub Data Processing Agreement.

14 COOPERATION WITH THE SUPERVISORY AUTHORITY

14.1 The Data Processor and the Sub Data Processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

15 COSTS

15.1 All costs, including costs related to revision, inspection and regular implementation of measures under applicable law and to fulfil the Sub Data Processor's obligations under this Sub Data Processing Agreement are included in any fees to be paid by the Data Processor under the Sales and Delivery Terms. Sub Data Processor shall not be entitled to receive any separately fees for the Sub Data Processor's fulfillment of such obligations.

16 EFFECTIVE DATE AND TERMINATION

16.1 The Sub Data Processing Agreement shall come into force on the date of the last party signing this Sub Data Processing Agreement.

16.2 The Sub Data Processing Agreement shall continue for as long as the Sales and Delivery Terms have not been terminated or expired.

16.3 Data Processor is always entitled to suspend the data processing by the Sub Data Processor under this Sub Data Processing Agreement.

17 CHANGES IN THE APPLICABLE DATA PROTECTION LEGISLATION

17.1 If a change in mandatory applicable data protection legislation applicable to Data Processor or to Sub Data Processor requires Sub Data Processor to (i) sign on to any additional documentation for mandatory data protection compliance purposes, or (ii) implement additional technical and organizational measures to the ones listed herein, or (iii) accept additional obligations to those set out herein, and such requirement mentioned in (i) - (iii) above cause additional costs or risks for Sub Data Processor, then the Parties agree to negotiate in good faith a fair adjustment of any applicable fees.

17.2 Section 17.1 shall apply accordingly, in case (i) the Data Processor instructs Sub Data Processor to undertake services not foreseen in this Sub Data Processing Agreement or (ii) where mandatory applicable data protection legislation applicable to Data Processor

or to Sub Data Processor or the relevant supervisory authority imposes obligations on Sub Data Processor in addition to those set out herein.

18 GENERAL TERMS

18.1 **Amendments.** The terms of this Sub Data Processing Agreement can only be amended by written agreement between the Parties.

18.2 **Independent Parties.** The Parties explicitly accept that the relationship between them is a customer-independent contractor relationship.

18.3 **Information.** The Parties are obliged to act loyally towards each other and to inform each other without undue delay about any changes that may affect this Sub Data Processing Agreement.

18.4 **Force majeure.** None of the Parties are responsible for any actions or failure to carry out measures to the extent that such actions or such failure is due to matters beyond a Party's reasonable control, including but not limited to war, uprisings, force majeure, strikes or other work stoppages (either in part or in whole), disturbances of the public telenet, disturbances of internet connections or similar evens, but only if said Party could not have predicted the event at the time of taking on the obligation. As long as such an event prevents a Party from performing said obligation, this must be suspended until such disturbance no longer exists.

18.5 **Notices.** All notices related to this Sub Data Processing Agreement must be made to the other Party either in person or by registered mail.

18.6 **Assignment.** Data Processor may, either in part or in whole, assign its rights and obligations under this Sub Data Processing Agreement to a third party. The Sub Data Processor may not assign its rights or obligations under this Sub Data Processing Agreement to a third party without the Sub Data Processor's prior written approval.

18.7 **Invalid condition.** If a condition or a provision in this Sub Data Processing Agreement is invalid, such invalidity shall not mean that the remaining part of this Sub Data Processing Agreement is invalid. If the applicable law on personal data is changed after the effective date of this Sub Data Processing Agreement, the Data Processor is obliged to accept such changes to this Sub Data Processing Agreement.

18.8 **Governing law.** This Sub Data Processing Agreement is governed by Danish law with the City Court of Copenhagen as its legal venue. United Nations Convention on Contracts for the International Sale of Goods (CISG) shall not apply to the Sub Data Processing Agreement.

19 Signature

Date: 28-05-2018	Date:
	

Appendix 1 - Pre-approved subcontractors:

Appendix 2 - Data Processors IT Security Policies

1 Access to Personal Data is restricted to persons who have a material need for access to Personal Data. Personal Data will only be accessed on a "need to know" basis.

2 Employees, who handle Personal Data, are instructed and trained in what they must do with Personal Data and how to protect Personal Data.

3 There must be as few people as possible with access to Personal Data, with due regard for the operation. However, there must be a sufficient number of employees to ensure the operation of the tasks concerned in case of sickness, holidays, staff replacement, etc. Personal Data will only be accessed on a "need to know" basis.

4 Personal data on paper - for example in cartons and binders- are kept closed and locked when not in use.

5 When documents (papers, charts, etc.) are discarded, shredding and other measures are used to prevent unauthorized access to Personal Data.

6 We use access codes to access PCs and other electronic equipment with Personal Data. Only those who need to have access will receive an access code and then only for the systems that they need to use. Those who have a password may not leave the code to others or leave it so others can see it. Checking of assigned codes must be done at least once every six months.

7 Unsuccessful attempts to access IT systems with Personal Data are detected and logged. If a specified number of consecutive rejected access attempts is detected, further tests must be blocked.

8 We have appointed a responsible person to monitor such inaccessible access attempts. Considering the technological development, software is available that can clarify who has attempted to gain access to personal data.

9 If Personal Data is stored on a USB key, Personal data must be protected, e.g. by use of a password and encryption key. Otherwise, the USB key must be stored in a locked drawer or cabinet. Similar requirements apply to the storage of personal data on other portable data media.

10 PCs connected to the Internet shall have an updated firewall and virus control installed. When connecting to WiFi, for free access, we ensure appropriate security measures considering the current state of technology development in the IT-area.

11 If sensitive personal data or social security numbers are sent by e-mail via the Internet, such e-mails must be encrypted. If you send Personal Data to us via email, please note that sending to us is not secure if your emails are not encrypted.

12 About the repair and service of data equipment containing Personal Data and when data media are to be sold or discarded, we take the necessary measures to prevent information from being disclosed to a third party.

13 In the situations where a computer is submitted for repair and where Personal Data is stored on such computer, we establish several access codes for different sections of the personal data. For example, a repairer will not need to be able to access Personal Data that may be on the computer. Such a multi-code scheme may help - but not eliminate - the risk of misuse of Personal Data. In addition, agreement and verification should ensure that repairers do not unduly access Personal Data, for example, by using confidentiality statements.

14 When we use an external data processing agent to handle Personal Data, a written Sub Data Processing Agreement is signed between us and the Sub Data Processor. This applies, for example, when we use an external document archive or if cloud systems are used in the processing of personal data - including communication with the customer. In the same way, a written agreement between us and our customer is always entered into if we act as Sub Data Processor. Sub Data Processing Agreements are also available electronically.

15 We have internal rules on information security. We have adopted internal rules on information security that contain instructions and measures which protect Personal Data from being destroyed, lost or modified, from unauthorized disclosure, and against unauthorized access or knowledge of them. We will ensure that collected Personal Data are treated with care and protected according to applicable safety standards. We have strict security procedures for collecting, storing and transferring Personal Data to prevent unauthorized access and compliance with applicable laws.

16 We have taken the necessary technical and organizational safeguards to protect your Personal Data from accidental or illegal destruction, loss or change, and against unauthorized disclosure, abuse or other actions contrary to applicable law.

17 The systems are located on servers in secured premises.

18 We use industry standards such as firewalls and authentication protection to protect your Personal Data.

19 All data transferred between client (browser and web app) and server(s) are encrypted according to the HTTPS protocol.

20 All facilities are locked and only staff members who have signed a declaration of confidentiality have access to the facilities. After the end of normal working hours, the facilities are locked. Access to the facilities is always carried out under the supervision of an employee.

21 All access to our premises is logged by electronic key or entered in the guestbook.

22 We take a backup of all databases and files on shared drives every night. The backup is stored on an internal server, partly on an external data centre.

23 We make the following types of backup:
a) Rolling backup. This method takes daily backup of all file and data updates and creates a backup of all new data. This creates a history of changes so that the ability to recover lost data is increased.
b) backup clone. This backup strategy creates a perfect copy of each device on the network
c) backup offsite. This backup ensures against data loss if backup is stored on site. All data and files are backed up and backup stored offsite.

24 All backup data and files are overwritten at 30-day intervals. It is not technically possible to complete deletion of individual files on a backup before such overwriting occurs. Thus, if you have request that we delete Personal Data, such Personal Data will be deleted in live environment, but will remain on backup until the specific backup is overwritten after 30 days. However, we have introduced internal processes and procedures to ensure that Personal Data is not reintroduced as live data by reloading data and files from a backup as Personal data has been deleted according to the "right to be forgotten."