Data Processing Agreement

between

[Fill in name of customer] (hereinafter "**the Controller**")	
Customer's legal name and enterprise registering no.:	
Address:	
Represented by:	
Signature:	
Title:	
Date:	

and

d2o (hereinafter "**the Processor**")	
Supplier's legal name and enterprise registering no.:	Deadline2online AS (981693302)
Address:	Postboks 2719 Solli, 0204 Oslo
Represented by	Hoang N. Nguyen
Signature:	
Title:	Chief Operating Officer
Date:	

for the processing of personal data (Personal Data)

1. Background and Purpose

The purpose of this Data Processing Agreement (DPA) is to set out the rights and obligations of the parties concerning the data processing operations carried out under the Main Service Agreement (MSA). In the event of inconsistency between the MSA and this DPA on matters concerning data protection, the DPA shall prevail.

The Parties commit to comply with the Norwegian Data Protection Act and the Regulation (EU) 2016/679 of 27 April 2016 (the GDPR regulation).

2. Description of processing activities

The nature and purpose of processing: The Processor operates a software-as-a-service (SaaS) platform (called PMI), which includes labour forecasting, scheduling, and budget/forecast deviation analysis and reporting.

Pursuant to the MSA the Controller is granted a license to access and use PMI and d2o Academy, a learning management system. In providing the service, the Controller authorises the Processor to process Personal Data which are submitted to and stored in PMI and d2o Academy by the Controller.

The Personal Data processed are limited to: First name, last name, e-mail, job title and employee number.

The categories of Data Subjects are limited to: End-users of PMI, employees and contractors of Processor.

3. Duration of DPA

This DPA shall enter into force May 25th, 2018 and will remain in force as long as the Processor processes Personal Data on behalf of the Controller under the MSA.

4. Obligations of the Processor

4.1 Processing

The Processor agrees to:

a. secure that the processing of Personal Data is in accordance with the GDPR regulation, and process the data only for the sole purpose(s) stipulated in the MSA;

b. only process the Personal Data in accordance with the documented instructions of the Controller listed in Appendix 1 to the present DPA. If the Processor deems an instruction of the Controller to be in violation of the GDPR regulation, it shall immediately inform the Controller thereof. In addition, if the Processor is required to transfer Personal Data to a country or to an international organisation under EU law or the law of the Member State to which it is subject, it must inform the Controller of this legal obligation before processing, unless the law in question prohibits such information for important reasons of public interest;

c. secure the confidentiality of Personal Data processed in the framework of the present DPA;

d. ensure that those who are authorised to process the Personal Data by virtue of the present DPA:
    i. commit themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
    ii. receive necessary training on the subject of Personal Data protection;

e. take into account, with regard to its tools, products, applications or services, the principles of data protection by design and of data protection by default.

4.2 Use of Subprocessor

4.2.1 The Processor agrees and warrants to remain liable to Controller for the subcontracted processing services of any of its direct or indirect subprocessors under this Agreement. The Processor shall maintain an up-to-date list of the names and location of all subprocessors used for the processing of Personal Data under this DPA (see Appendix 3). The Processor shall update the list (which is published on Wiki, the online user guide made available in PMI) of any subprocessor to be appointed at least 30 days prior to the date on which the subprocessor shall commence processing Personal Data. The Controller may sign up to receive email notifications of any such changes. The Processor agrees to sign agreements with its subprocessors which are in compliance with the regulation in this DPA. The same data protection obligations as set out in the DPA or other legal act between the controller and the processor as referred to in GDPR article 28 paragraph 3 shall be imposed on the Subprocessor by way of a contract, 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 GDPR.

4.2.2 In the event that the Controller objects to the Processing of its Personal Data by any newly appointed subprocessor as described in Section 4.2.1, it shall inform the Processor immediately. In such event, the Processor will either:

a. instruct the subprocessor to cease any further processing of the Controller's Personal Data, in which event the MSA shall continue unaffected, or
b. allow the Controller to terminate the MSA (and any related services agreement with the Processor) immediately and provide it with a pro rata reimbursement of any sums paid in advance for services to be provided but not yet received by the Controller as of the effective date of termination.

4.3 Right of information for Data Subjects

In case the data collection is done by the Processor, it shall provide the Data Subjects of the processing activities information regarding the Personal Data which it processes. The formulation and format of information shall be as approved by the Controller (upon proposal of the Processor) prior to data collection.

4.4 Exercise of rights of Data Subjects

Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in GDPR Chapter III.

The Controller shall, as far as the GDPR allows, handle all contact with the Data Subject. In case a Data Subject contacts the Processor for the exercise of their right of access, right of rectification, right of erasure and objection, right to restriction of processing, right to data portability, right not to be subject to a decision based solely on automated processing (including profiling), the Processor shall upon receipt without undue delay forward the requests to Controller's PMI Super-user and the contact person of the Controller under this DPA.

To the extent the Controller, in its use of PMI services, does not have the ability to address a Data Subject request, the Processor shall upon Controller's request provide commercially reasonable assistance to facilitate such Data Subject request to the extent the Processor is legally permitted to do so and provided that such Data Subject request is exercised in accordance with the GDPR regulation.

4.4 Notification of a Personal Data breach

In the event of (i) a Personal Data breach, (ii) breach of this DPA, or (iii) breach of the GDPR regulation, the Processor shall promptly notify the Controller's PMI Super-user and the contact person of the Controller under this DPA in writing. In respect of a Personal Data breach, the Processor will make it best endeavour to give such notification no later than 36 hours after the Processor became aware of it.

Such notification shall – wherever relevant – include:

a. describe the nature of the Personal Data breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
b. if possible, the identities of the affected Data Subjects;
c. communicate the name and contact details of the data protection officer or other contact point of the Processor where more information may be obtained;
d. describe the likely consequences of the Personal Data breach;
e. describe the measures taken or proposed to be taken to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.
f. include other information required for the Controller to comply with applicable data protection law.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

4.5 Obligation of assistance

The Processor will, insofar it is commercially reasonable, cooperate with the Controller to carry out a data protection impact assessment.

The Processor will, insofar it is commercially reasonable, cooperate with the Controller to consult the supervisory authority prior to processing.

The Processor will assist the Controller in ensuring compliance with the obligations pursuant to GDPR Articles 32 to 36 taking into account the nature of processing and the information available to the processor.

4.6 Security measures

The Processor shall implement all technical and organisational security measures necessary to ensure the protection, confidentiality and particular handling of the Personal Data as required under GDPR, i.a. by taking all measures required pursuant to GDPR Article 32 and other GDPR regulations (see also Appendix 2), including but not limited to:

a. the pseudonymisation and encryption of Personal Data;
b. the ability to ensure the 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.

4.7 Return or deletion of Personal Data

Upon termination of the performance of the services relating to the processing of Personal Data, the Processor will up to thirty (30) days following such termination permit the Controller to export its Personal Data, at its expense, in accordance with the capabilities of the service. Following such period, the Processor shall have the right to delete all Personal Data stored or processed by Processor on behalf of Controller in accordance with Processor's deletion policies and procedures. Data Controller expressly consents to such deletion or anonymization. Once deleted or anonymized, the Processor will inform the Controller in writing.

The Processor will at the choice of the Controller, delete or return all the personal data to the Controller after the end of the provision of services relating to processing, and delete existing copies unless law requires storage of the personal data.

4.8 Data protection officer

The Processor will keep the Controller informed of the name and contact details of its data protection officer, in case where it has designated one in accordance with Article 37 of the GDPR regulation. This is published on Wiki, the online user guide made available in PMI. The Controller may sign up to receive email notifications of any such changes.

4.9 Records of processing activities

The Processor shall maintain a record of processing activities on behalf of the Controller containing:

a. the name and contact details of the Processor and the Controller on behalf of which the Processor is acting, and, where applicable, of the Controller's or the Processor's representative, and the data protection officer;
b. the categories of processing carried out on behalf of the Controller;
c. where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
d. where possible, a general description of the technical and organisational security measures inter alia as appropriate, including but not limited to:
    i. the pseudonymisation and encryption of Personal Data;
    ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

iii. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4.10 Audit and Documentation

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the GDPR obligations as requested by the Controller from time to time, and shall allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

The Processor shall cover all costs associated with audits and is entitled to charge separately the Controller the costs, including internal resources (at the rates stipulated in the MSA) it incurs in conjunction with its assistance with such audits.

5. Obligations of the Controller

As part of the Controller receiving the service under the MSA, the Controller agrees to:

a. take sole responsibility for the accuracy of Personal Data and the means by which such Personal Data is acquired and the Processing of Personal Data by the Controller, including instructing processing by the Processor in accordance with this DPA, is and shall continue to be in accordance with all the relevant provisions of the GDPR regulation, particularly with respect to the security, protection and disclosure of Personal Data;

b. that the Controller will inform its Data Subjects about its use of data processors to Process their Personal Data, including Data Processor; and

c. that it shall respond in reasonable time and to the extent reasonably practicable to enquiries by Data Subjects regarding the Processing of their Personal Data by Data Controller, and to give appropriate instructions to the Processor in a timely manner; and

d. that it shall respond in a reasonable time to enquiries from a Supervisor regarding the Processing of relevant Personal Data by the Controller.

e. if appropriate, participate the processing, including conducting audits and inspections at the Processor

6. Limitation on liability

6.1 UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY (WHETHER IN CONTRACT, TORT, NEGLIGENCE OR OTHERWISE) WILL EITHER PARTY TO THIS DPA, OR THEIR AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SERVICE PROVIDERS, SUPPLIERS OR LICENSORS BE LIABLE TO THE OTHER PARTY OR ANY THIRD PARTY FOR ANY LOST PROFITS, LOST SALES OR BUSINESS, LOST DATA (BEING DATA LOST IN THE COURSE OF TRANSMISSION VIA DATA CONTROLLER'S SYSTEMS OR OVER THE INTERNET THROUGH NO FAULT OF DATA PROCESSOR), BUSINESS INTERRUPTION, LOSS OF GOODWILL, OR FOR ANY TYPE OF INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, CONSEQUENTIAL OR PUNITIVE LOSS OR DAMAGES, OR ANY OTHER LOSS OR DAMAGES INCURRED BY THE OTHER PARTY OR ANY THIRD PARTY IN CONNECTION WITH THIS DPA, OR THE SERVICES, REGARDLESS OF WHETHER SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF OR COULD HAVE FORESEEN SUCH DAMAGES.

6.2 NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS DPA OR THE MSA, DATA PROCESSOR'S AGGREGATE LIABILITY TO DATA CONTROLLER OR ANY THIRD PARTY ARISING OUT OF THIS DPA AND ANY LICENSE, USE OR EMPLOYMENT OF THE SERVICE, SHALL IN NO EVENT EXCEED THE LIMITATIONS SET FORTH IN THE MSA.

6.3 FOR THE AVOIDANCE OF DOUBT, THIS SECTION SHALL NOT BE CONSTRUED AS LIMITING THE LIABILITY OF EITHER PARTY WITH RESPECT TO CLAIMS BROUGHT BY DATA-SUBJECTS.

7. Law and venue

This DPA shall be governed by the laws of Norway, and the venue is in Norway where the Processor has its domicile.

Appendix 1: Controller's instructions

Any relevant instruction by the Controller comprised in the underlying MSA commercial agreement between the Controller and the Processor relating to the processing activities set out in section 2 hereof, will be considered to be incorporated herein by reference. All Personal Data shall be processed only to the extent allowed under applicable law.

Appendix 2: Technical and organisational and security measures

The Processor, when Processing Personal Data on behalf of the Controller in connection with the PMI service, shall implement and maintain the following technical and organizational security measures for the processing of Personal Data ("Security Standards"):

1. **Physical Access Controls:** The Processor shall take reasonable measures to prevent physical access, such as security personnel and secured buildings and factory premises, to prevent unauthorized persons from gaining access to Personal Data, or ensure Subprocessor operating data centres on its behalf are adhering to such controls.
2. **System Access Controls:** The Processor shall take reasonable measures to prevent Personal Data from being used without authorization. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.
3. **Data Access Controls:** The Processor shall take reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access; and, that Personal Data cannot be read, copied, modified or removed without authorization in the course of Processing.
4. **Transmission Controls:** The Processor shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so data submitted or stored in connection with the use of PMI service cannot be read, copied, modified or removed without authorization during electronic transmission or transport.
5. **Input Controls:** The Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom data has been entered into data processing systems, modified or removed. The Processor shall take reasonable measures to ensure that (i) the Personal Data source is under the control of the Controller; and (ii) Personal Data integrated into the service is managed by secured transmission from the Controller.
6. **Data Backup:** Back-ups of the databases in the service are taken on a regular basis, are secured, and encrypted to ensure that Personal Data is protected against accidental destruction or loss' when hosted by the Processor.
7. **Logical Separation:** Data from different the Processor's subscriber environments is logically segregated on the Processor's systems to ensure that Personal Data that is collected for different purposes may be Processed separately.

Appendix 3: Subprocessors

Company name	Company address	Processing location	Change
~~Ahot AB~~	~~Vegagatan 10 and 413 09 Göteborg~~	~~Sweden~~	
Claes Nilsson Elautomation AB	Box 69, 161 26 Bromma	Sweden	
d2o LLC	1560 Sawgrass Corporate Parkway, 4th Floor, Fort Lauderdale, FL-33323	USA	
Hubconsult Ltd	Unit B, 23/F., North Cape Commercial Building, 388 King's Road, North Point,	Hong Kong	
Konsulent R. Gule	Randulf Hansens vei 13, 4870 Fevik	Norway	
LeBon Co., Ltd	2/108 Road 8, Ward Binh Hung Hoa, Binh Tan District, Ho Chi Minh City	Vietnam	
Microsoft Azure	1, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521	North Europe/ Ireland	
QT-DATA INC.	81 - 325 5th Avenue North, Saskatoon, SK, S7K 2P7	Canada	
Smart IT AS	Grindalsvegen 3, 2406 Elverum	Norway	
Webhuset AS	Postboks 610 Sentrum, 5806 Bergen	Norway	
Zendesk, Inc KaHot WalkMe, Inc.	1019 Market Street, San Francisco, CA 94103 USA AVENUE DE BELMONT 42, CH-1820 MONTREUX 525 Market Street, 37th Floor, San Francisco, CA 94105	Ireland SWITZERLAND USA	 Added 01/08/18 Added 01/08/19