Data Processing Agreement

This Data Processing Agreement forms part of the Service Agreement of [insert date of signature of the Service Agreement] and is entered into between:

1) Mintra Trainingportal AS, a Norwegian company with registration number 943 098 557, Mintra Training Portal Ltd, a company registered in UK with registration number 362194 including affiliate in Dubai, Mintra Asia Pacific Pte Ltd, a company registered in Singapore with registration number 201427343E, and Atlas Knowledge Ltd., a company registered in UK with registration number 01231037 ("**Data Processor**"); and

2) Name of organisation: _____
Registration number: _____
("**Data Controller**")

1. Background

1.1 The Data Processor Processes Personal Data on behalf of the Data Controller.

1.2 This Data Processing Agreement governs the Processing of Personal Data that the Data Processor performs on behalf of the Data Controller under the Service Agreement. The Data Processor shall process Personal Data only in accordance with the listed and agreed specified purposes under this Data Processing Agreement.

1.3 The Norwegian Personal Data Act with Regulations, and EU Regulation 2016/679, contains requirements for the governing of the relationship between the Data Processor and the Data Controller, and for the security and organizational measures that must be implemented to ensure lawful and secure processing of Personal Data. This Data Processing Agreement has therefore been entered into to ensure that Personal Data is processed only in accordance with applicable laws and regulations, and only upon instructions from the Data Controller.

1.4 In case there is a contradiction between terms in this Data Processing Agreement and the Service Agreement, the Service Agreement shall prevail.

2. Definitions

2.1 **GDPR** (General Data Protection Regulation) means EU Regulation 2016/679.

2.2 **Personal Data** means any information relating to an identified or identifiable natural person, Article 4 (1) of the GDPR.

2.3 **Data Subject(s)** means any information relating to an identified or identifiable natural person of whom the Data Controller has Personal Data.

2.4 **Processing** means any operation or set of operations which is performed on Personal Data, cf. Article 4 (2) of the GDPR.

2.5 **Third Country** means countries outside the EU/EEA which are not considered to ensure adequate level of protection for the Processing of Personal Data.

3. Processing of Personal Data

3.1 *Personal Data to be processed*

(a) The Data Processor delivers

- ☐ OCS
- ☐ Trainingportal
- ☐ Trainingportal IDV

to the Data Controller and will Process Personal Data on behalf of the Data Controller in this regard. The categories of Personal Data to be Processed pursuant to this Data Processing Agreement are specified in Annex 1.

3.2 *Purpose of the Processing of Personal Data*

(a) The purpose of the Data Processor's Processing of Personal Data pursuant to this Data Processing Agreement is personnel administration, as well as e-learning and training management services, in addition to system service and security improvements.

4. Data Controller's Obligations

4.1 The Data Controller confirms that:

(a) There is adequate basis for the Processing of Personal Data;

(b) The Data Controller is entitled to and responsible for the legality of the transfer of Personal Data to the Data Processor;

(c) The Data Controller is responsible for the accuracy, integrity, content, reliability and legality of the Personal Data being Processed; and

(d) The Data Controller has notified the Data Subjects in accordance with the current statutory requirements.

4.2 The Data Controller shall ensure that Personal Data is processed in accordance with the GDPR, respond to the Data Subjects' inquiries and ensure that adequate technical and organizational measures are taken to secure the Personal Data Processed, cf. Article 32 of the GDPR.

4.3 The Data Controller is obliged to report nonconformity to the relevant supervisory authorities and, if applicable, to the Data Subject without undue delay in accordance with applicable legislation.

5. Data Processor's Obligations

5.1 *Basic Obligations*

(a) Data Processor shall only process Personal Data upon, and in accordance with, instructions from the Data Controller and in accordance with the GDPR.

(b) The Data Processor shall not process Personal Data without prior written agreement with the Data Controller or written instructions from the Data Controller beyond what is necessary for the purposes specified in this Data Processing Agreement.

(c) The Data Processor shall assist the Data Controller, taking into account the nature of the processing and the information available to the Data Processor, in ensuring compliance with the obligations pursuant to the GDPR Article 32 to 36, and further make available to the Data Controller all information necessary to demonstrate that the Data Controller complies with the obligations laid down in the GDPR Article 28.

(d) The Data Processor shall notify the Data Controller if the Data Processor receives instructions from the Data Controller that violates the GDPR.

5.2 *Data Security*

(a) The Data Processor shall ensure, through planned, systematic, organizational and technical measures, adequate data security in relation to confidentiality, integrity and availability in the Processing of Personal Data in accordance with Article 32 of the GDPR.

(b) The measures and the internal control documentation are made available to the Data Controller on request.

(c) In the assessment of the technical and organizational measures to be implemented, the Data Processor shall consider:

- Best practice
- The cost of implementation
- The nature and extent of the Processing
- The context and purpose of the Processing
- Seriousness of the risk that the Processing of Personal Data entails for the Data Subject's rights

(d) The Data Processor shall consider:

- Implementation of pseudonymisation and encryption of Personal Data
- The ability to ensure ongoing confidentiality, integrity, availability and robustness of systems for Processing and services

- The ability to restore availability and access to Personal Data on time in case of physical or technical incidents
- A process for regular testing, assessment and evaluation of the effectiveness of technical and organizational measures for the security of the Processing

5.3 *Inquiries from Data Subjects*

(a) The Data Processor shall implement technical and organizational measures to assist the Data Controller in responding to inquiries regarding the exercise of the Data Subjects' rights.

5.4 *Assistance to Data Controller*

(a) Data Processor shall provide assistance in such a way that the Data Controller can safeguard its own liability according to law and regulation, assisting the Data Controller in:

- Implementing technical and organizational measures as mentioned above,
- Observing duty of notification to supervisory authorities and Data Subjects as a result of non-conformity,
- Performing assessment of data privacy implications ("DPIA, Data Privacy Impact Assessments"),
- Performing preceding discussions with supervisory authorities when an assessment of data privacy implications makes it necessary,
- Notifying the Data Controller if the Data Processor believes that a Data Controller's instruction is in violation of applicable data privacy regulations.

(b) Such assistance as mentioned above shall be carried out to the extent required by the Data Controller's needs, the nature of the Processing and the information available to the Data Processor. The Data Processor is entitled to charge the Data Controller for such assistance according to the Data Processor's standard hourly rates.

5.5 *Procedures and notification at security breaches*

(a) Any use of information systems and Personal Data in violation of established procedures, instructions from the Data Controller or applicable law regarding the processing of personal data, as well as security breaches, shall be treated as non-conformity.

(b) The Data Processor shall have procedures and systematic processes to follow up non-conformity, including the reestablishment of the normal state, elimination of the cause of the non-conformity, and preventing recurrence.

(c) The Data Processor shall without undue delay notify the Data Controller of a security breach, and of any violation of this Data Processing Agreement or accidental, unlawful or unauthorized access, use or disclosure of Personal Data, or that Personal Data may

have been compromised or that the integrity of the Personal Data may have been violated.

(d) The Data Processor shall provide the Data Controller with all necessary information to enable the Data Controller to comply with applicable law and enable the Data Controller to answer inquiries from data protection authorities. The Data Controller shall report nonconformities to the Data Protection Authority in accordance with applicable legislation.

5.6 *Procedures for deletion*

(a) Personal Data shall be deleted when this is no longer necessary in order to achieve the purpose for which it was collected. The Data Controller shall define the deletion procedures and the Data Processor shall follow and perform them.

5.7 *Deletion upon termination*

(a) Upon termination of the Service Agreement, the Data Processor shall without undue delay cease Processing of Personal Data on behalf of the Data Controller. As such, the Data Processor shall upon instruction from the Data Controller, delete all Personal Data contained in the Data Processor's possession in connection with Processing under this Data Processing Agreement.

5.8 *Confidentiality*

(a) The Data Processor has confidentiality in relation to Personal Data. The Data Processor shall ensure that anyone performing work for the Data Processor, either employees or hired staff, who have access to or are involved in the Processing of Personal Data under the Service Agreement (i) are subject to confidentiality and (ii) are notified of and comply with the obligations under this Data Processing Agreement. Confidentiality also applies after the Service Agreement has been terminated.

5.9 *Annual security audits*

(a) The Data Controller has the right to conduct an annual audit of the Data Processor's Processing of Personal Data. The Data Processor shall facilitate such audit. The Data Controller is entitled to demand a security audit performed by an independent third party. The third party concerned will prepare a report that will be delivered to the Data Controller on request. The Data Controller shall pay the costs associated with an annual audit. If an audit reveals significant breaches of the obligations by the Data Processor under the Data Processing Agreement, the Data Processor shall pay for the Data Controller’s reasonable costs accrued from the audit.

(b) The Data Processor will regularly perform security audits on systems, etc. that are relevant to the Processing of Personal Data covered by this Data Processing Agreement. The Data Controller shall have access to reports that document security audits.

6. Use of Sub-Processors

6.1 *Use of Sub-processors*

(a) The Data Processor has the Data Controller's general authorisation for the engagement of Sub-processors. The Data Processor shall inform the Data Controller (by updating the Mintra website and thereby providing the Data Controller notice of that update) of any changes concerning the addition or replacement of Sub-processors at least thirty (30) calendar days after the information is publicized on the website, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of such Sub-processors. If the Data Controller in due time formally objects in writing to the engagement of such Sub-processors, the Parties shall discuss in good faith to find an appropriate solution and/or new Sub-Processor that are acceptable for both Parties. If the Parties are unable to reach an agreement within thirty (30) calendar days from the Data Processor's notice to the Data Controller of intended changes, the Data Processor is entitled to terminate both the Data Processing Agreement and the Service Agreement, in full or in part, at its own discretion and without any obligations, financial commitments or any other liability towards the Data Controller. The list of Sub-processors already authorised by the Data Controller is in Annex 1.

6.2 *Agreement with Sub-processors*

(a) The Data Processor shall ensure that Sub-processors do not Process Personal Data covered by the Service Agreement in any way other than what is necessary to provide the service, and that the Personal Data is not left to others for Processing without this being in accordance with this Data Processing Agreement or agreed in advance in writing with the Data Processor.

(b) The Data Processor shall ensure that any agreement with a Sub-processor contains the necessary provisions regarding the Processing of Personal Data in accordance with Article 28 of the GDPR. The Data Processor is responsible for the Sub-processor's Processing Personal Data in accordance with the requirements of the GDPR.

6.3 *Sub-processors outside the EU/EEA*

(a) If the Data Processor is to enter into an agreement with Sub-processors in countries outside the EU/EEA, this should only be done according to EU's standard agreements for transfer of personal data to third countries. The same applies even if Personal Data is kept or stored in the EU/EEA when personnel with access to the data are located outside the EU/EEA. The Data Controller gives the Data Processor the authorization to enter into such standard agreements with Sub-processors in accordance with this section 6.

7. Duration and Liability

7.1 This Data Processing Agreement shall apply from the date it has been signed by both parties until the Service Agreement expires or until the Data Processor's obligation to perform services under the Service Agreement is terminated for any reason.

7.2 Upon termination of this Data Processing Agreement, Personal Data and other data shall be deleted, if not return in standardized format and medium has been agreed in writing. The Data Processor and its Sub-processors shall immediately stop processing personal data from the date specified by the Data Controller.

7.3 As an alternative to returning Personal Data (or other data), the Data Controller may, in its sole discretion, instruct the Data Processor in writing that all or part of the Personal Data (or other data) shall be deleted by the Data Processor, unless prescriptive legislation prevents the Data Processor from such deletion.

7.4 The Data Processor is not entitled to retain a copy of Personal Data or other data provided by the Data Controller in connection with the Customer Agreement or this Data Processing Agreement in any format, and any physical and logical access to such Personal Data or Data shall be deleted.

7.5 The Parties shall revise this Data Processing Agreement in the event of relevant changes to applicable laws.

7.6 The Parties' liability for damage suffered by a data subject or other natural persons which is due to a violation of the Norwegian Personal Data Act, including GDPR, will follow the provisions of article 82 of the GDPR. Any recourse claims for damages from the Data Controller to the Data Processor which are arising from article 82 in the GDPR, shall, in the aggregate, be limited to the lower of 1) an amount equivalent to the consideration invoiced by the Data Processor to the Data Controller during the last 12 months prior to the date of the claim, or 2) the liability cap stated in the Service Agreement.

7.7 The Parties are individually liable for administrative fees imposed pursuant to article 83 of the General Data Protection Act.

8. Choice of Law and Legal Venue

8.1 This Data Processing Agreement shall be subject to and interpreted in accordance with Norwegian law. Each Party may require a legal dispute under this Data Processing Agreement to be resolved before the Norwegian courts of law.

8.2 The venue shall be the legal venue of the Data Processor.

9. Appendices

9.1 Annex 1: Overview of Personal Data being Processed and Sub-processors.

10. Signatures

	Data Processor	**Data Controller**
Signature:		Signature: _____
Name:	Scott Irving Kerr	Name: _____
Title:	CEO	Title: _____
Date:	31.8.2020	Date: _____

Data Protection Officer Contact Details

	Data Processor	**Data Controller**
Name:	Kami Faust	Name: _____
Email:	kami.marie.faust@mintra.com	Email: _____

If the Data Protection Contact changes it is up to the Data Controller to inform Mintra Group.

11. Annex 1

11.1 *Categories of Personal Data*

(Dependant on the Mintra Group product used, please adjust categories of personal data processed)

- Contact information, such as telephone number and e-mail address
- Employment information, such as title
- ID data, such as name and social security number
- Next of kin information
- Economic information, such as salary
- Technical information, such as IP address and log file
- If Trainingportal Identification Verification module is purchased the following Personal Data is processed:
  - (i) Biometric identification data, such as face recognition
  - (ii) Other identification data provided by the government, such as passport, Identity card, drivers licence

11.2 *Categories of Data Subjects*

(Dependant on the Mintra Group product used, please adjust categories of personal data processed)

- Employees
- Contracted personnel

11.3 *Sub-processors*

(Categories of personal data and agreement see Appendix 1 within Annex 2, EU's standard agreement)

- Rackspace, UK – Hosting provider
- Amazon, Ireland – Hosting provider
- Dominus Software, Poland – Software developer
- New Verve Consulting, UK – Hosting provider
- RDU, UK – Testing, special project for proctoring