Appendix 11 Data Processing Agreement

Data Processing Agreement

(the «Agreement» or the « DPA»)

between

AtB AS

(«AtB» or «Controller»)

and

XXXX

(«Consultant» or «Processor»)

1 The purpose of the DPA

The DPA shall ensure that all processing of personal data about the data subject (AtB´s customer) is in accordance with law and regulations, is not subject to unlawful processing and is accessible for anyone unauthorized to process the data.

Following the Framework Agreement for Analyses of Flexible transport (the «Contract») and as a part of the delivery, the processor will regularly process personal data on behalf of AtB. See this DPA item 3 for further information about the processing in question.

This DPA sets out the regulations for the processors processing of personal data on behalf of the Controller, such as collection, recording, organization, storage, disclosure or any combination of these. The DPA shall also set out the regulations of the Parties rights and obligations in connection with the processing of personal data.

The processing of personal data shall be in accordance with the at any time applicable legislation for processing of personal data, such as the Norwegian Personal Data Act (the "**Personal Data Act**") and the EU 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 (the "**General Data Protection Regulation**").

The DPA and the Contract between the Parties are mutual dependent, and cannot be terminated separately. The DPA may however – without termination of the Contract – be replaced by a new DPA, or supplied by specific instructions in regards to the processing of personal data.

The Processor is not entitled to any other processing than specified in this DPA. The Agreement will apply correspondingly as far as suitable for processing of data vital for the company.

Any obligations in the applicable regulations regarding the Processor shall apply even though it is not specifically mentioned in this DPA. To the extent that there is any conflict between the terms and conditions in this DPA and either the Personal Data Act or the General Data Protection Regulation, terms and conditions in the Personal Data Act or the General Data Protection Regulation shall prevail.

2 Definitions

Reference is made to the definitions in the underlying Contract. In addition, the following definitions shall apply:

Controller: means the legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data, i.e. AtB by the general manager, cf. GDPR article 4 (7).

Processor: means the legal person which processes personal data on behalf of the controller, cf. GDPR article 4 (8).

Vital Company data: Data significant to the Controllers business, such as strategies, contracts, prices, accounting data and/or similar documents.

Personal data: Any information relating to an identified or identifiable natural person, cf.GDPR article 4 (1).
Processing: Any operation which is performed on personal data, such as collection, recording, organization, storage and disclosure or any combination of use, cf. GDPR article 4 (2).

3 The Purpose and extent of the processing

3.1 General provisions

While working with directing of traffic and logistics, ticketing, reporting and control, the Processor will process personal data *on behalf of* the Controller in different ways.

The following personal data will be registered and stored by the Processor on behalf of the Controller:

- *A description of the type of personal data that will be registered and stored by the Processor on behalf of the Controller must be filled in here before signing of the Contract takes place.*

4 The Controller´s (AtB´s) duties

The Controller shall determine the processing of personal data under this Agreement. The Controller shall ensure that all processing of personal data is lawful, and that the processing is in accordance with applicable laws and regulations.

Unless otherwise stated in law, the controller is entitled to access to any personal data processed *on behalf of* the Controller. The Controller is entitled to access to the Processors IT-systems used for the processing of personal data, subject to the security of processing to ensure confidentiality, integrity and availability in the processing. The Processor is obliged to, if necessary, give the Controller necessary aid to provide access to the personal data.

The Controller is under a duty of confidentiality about any Vital company data exposed due to the assess given from the Consultant.

5 The Processor´s (Consultant´s) duties

5.1 The purpose of processing

The Processor shall process personal data *on behalf of* the Controller. The Consultant is not entitled to process any personal data on behalf of AtB for other purposes than defined in this DPA or according to supplementary instructions.

The Processor shall process personal data in accordance with and under the instructions given by the Controller and shall not process personal data to a greater extent than necessary to fulfil the Agreement with the Controller. The personal data can not be distributed or handed over, sold etc. to anyone for storage, arrangement or similar without a prior written consent from the Controller.

The Processor shall immediately notify the Controller if it becomes of the opinion that an instruction which has been given is not in compliance with the General Data Protection Regulation or other provisions regarding the safeguarding of personal information.

5.2 Duty to implement appropriate technical and organizational measures

The Processor confirms that it will implement and comply with appropriate technical and organizational measures in order to ensure necessary security of the information in accordance

with the Personal Data Act and the General Data Protection Regulation concerning protection of the rights of the data subject, including all demands subject to the GDPR article 32.

The measures shall ensure that regards to confidentiality, integrity and accessibility is implemented in the processing. This includes, depending on what is relevant, necessary measures in order to prevent incidental or illegal destruction or loss of data, non-authorised access to or the spreading of data, any other use of personal data which is not in accordance with the DPA, and measures in order to restore accessibility and access to personal data in the event of an occurrence.

The Processor shall assist the controller by appropriate technical and organizational measures for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in the GDPR Chapter III.

5.3 Access and rectification of data

If the Processor receive a request, such as a request for access to personal data, from a data subject (AtB´s customer) or others subject to the GDPR Chapter III, the Processor shall forward the request to AtB and assist the Controller with responding to the request.

If processed data has been incorrect, incomplete or unlawful, the Processor is obliged to correct the data, assist the Controller, and – as far as possible – ensure that the breach does not affect the data subject (AtB´s customer).

5.4 Duty to assist

The Processor shall, at the request of the Controller, assists the Controller in ensuring compliance with the obligations pursuant to the GDPR articles 32 to 36, such as:

- notifications to the supervisory/regulatory authorities (Datatilsynet) regarding breach of the personal data information security
- notifications to the registered person regarding breach of the personal data information security
- data impact assessments and/or prior consultations

5.5 Duty of confidentiality

The Processor is committed to confidentiality concerning all personal data it has access to under this DPA. The Processor shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The duty of confidentiality applies also after the expiry of the Agreement.

5.6 Codes of conduct

At the existence of approved codes of conduct (professional bodies) pursuant to the GDPR article 40, or certification pursuant to article 42 that the Processor has accepted to comply with or be certified by, the Processor is obliged to comply with such codes of conduct or meet the requirements for the certification.

5.7 Duty to maintain records of processing activities

The Processor shall maintain a record of processing activities performed on behalf of the Controller, to ensure that the Processor knows where the data is stored. The records shall contain information on the internal or external storage medium the data are stored.

The Processor shall register all authorized and unauthorized access to data. All inquiries which are made shall be registered in a manner which makes it possible to track them back to the individual user (i.e. employees at the Processor, sub-Consultants and the Controller).

The records shall at least contain the information required pursuant to the GDPR article 30. The Processor can at any time demand a copy of the records. The register/log shall be stored until it may be assumed that they are no longer needed.

6 Use of sub processor

The Processor shall *not* transfer any personal data that the Processor processes on behalf of the Controller to third party, without prior consent from the Controller. The Processor´s use of another processor shall be agreed with the Controller in writing before the processing commences.

It the Processor engages another processor to perform specific processing activities on behalf of the Controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to the GDPR article 28 (3) shall be imposed on that other processor by way of a contract or other legal act.

There shall be a DPA between the Processor and the sub processor. The DPA shall be approved by the Controller *before* any personal data are transferred. Where that other processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of that other processor's obligations.

7 Transfer to third countries

The Processor cannot – without written consent from the Controller – transfer any personal data under this Agreement to a third country and/or third persons outside EU/EEA which does not provide an adequate level of protection, cf. the GDPR chapter V.

8 Security measures

The Processor shall fulfill the security demands at any time set out in applicable legislation. The Processor shall implement appropriate technical and organizational measures regarding confidentiality, integrity and accessibility to ensure a level of security appropriate to the risk at processing of personal data.

(See Annex 4 to the Code of Conduct – Guide to information security.)

The Consultant shall document its routines and all measures which has been taken in order to fulfil its duties. This documentation shall, upon request, be made available to the Controller. The Processor shall assist, where needed, to ensure that the Controller is in compliance with the legal obligations.

The Processor shall take all measures required pursuant to the GDPR article 32. The Processor shall make available to the Controller all information necessary to demonstrate compliance with these obligations. The documentation shall be made available to the Controller upon request.

The Processor must ensure appropriate security on servers, databases and other equipment to prevent any unauthorized access to personal data processed on behalf of the Controller. This also applies to prints and forms filled in with personal data.

The Processor shall have a security management system to ensure fulfillment of the demands in the GDRP article 32. The Processor shall also establish and maintain necessary security measures revealed by risk assessments.

The Controller shall – upon request – be given access to the result of any risk assessments and security audits performed by the Processor.

The Processor shall immediately notify The Controller of any personal data breach. The notification shall at least contain a description of:

- the categories of personal data concerned,
- the extent of the breach,
- (if possible) the cause of the breach,
- the likely consequences of the personal data breach and the potential risk for the data subjects,
- the measures taken or proposed to be taken to address the personal data breach,
- Any other information necessary to ensure that AtB can fulfill its obligations

The result of the handling of the breaches shall be documented

To the extent it is required the Controller will notify the supervisory authority (Datatilsynet) cf. the GDPR article 33.

9 Audits

The Controller shall regularly audit/inspect the Processor's processing of personal data which belongs to the Controller. The Controller will normally provide a 3 days' notice before an audit, but may demand unannounced audits. The Processor shall provide necessary aid to the Controller, such as making all information necessary to document compliance with the obligations set out in the GDPR and this DPA accessible for the Controller. The Processor shall also make the audits possible and contribute at audits.

An audit may include revision of procedures, inspections, spot tests, more comprehensive local controls or other suitable measures to demonstrate that the obligations in the GDPR article 28 is fulfilled. Reference is made to Annex 4 to the Code of Conduct - «Guide to information security».

10 Confidentiality

The Parties shall treat all personal data with confidentiality. Employees and others who act on behalf of the Processor in connection with processing of personal information shall sign a confidentiality Agreement approved by the Controller, cf. Appendix 8.

Only the Processor's employees which has the need for access to systems and information in order to fulfil necessary tasks regarding the services have access to such systems and/or information. Signed confidentiality agreements shall be made available tothe Controller upon request. The duty of confidentiality applies also after the expiry of the Contract and the DPA.

11 Nonconformity

At any breach of the provisions in this DPA, the GDPR or other applicable regulation, the Controller may demand that further processing by the Processor or any sub processor shall cease with immediate effect, and may initiate necessary measures to protect the data.

A breach of the provisions in this DPA may be considered as material breach, cf. the provisions regarding breach in the Contract.

Any compensation claim resulting from one of the Parties' violation of law, regulations or obligations set out in this DPA shall be resolved in accordance with Article 82 of the GDPR. Item 6 in the Contract about the Consultant´s liability will also apply.

12 Duration of the DPA

The DPA is effective as long as the Processor continues to process personal data on behalf of the Controller, cf. this Agreement and the Contract, and until all personal data is returned or deleted, cf. item 13 in this DPA.

13 Storage, return and deletion at termination

The Processor shall not store any personal data longer than what is determined in Agreement with the Controller or following mandatory law, including Code of Conduct for electronic ticketing.

At termination of this DPA, the Processor shall at the choice of the Controller delete or return all the personal data (including copies of personal data) to the Controller after the end of the provision of services relating to processing under this agreement, and delete existing copies unless otherwise is agreed between the Parties in writing or required by mandatory law.

The Processor shall further, upon request, provide the Controller with prints, or in another suitable way make available all personal data in databases etc. that is under this DPA or the Contract.

At the termination of the DPA the Processor shall properly delete all documents, data, disks, CDs and other material containing personal data under this agreement. This also applies for any safety copies.

The Processor shall within 1- one - month confirm in writing that return and/or deletion is performed according to this DPA. Return and/or deletion shall be performed without cost for the Controller.

14 Compensation

The Processor shall perform any obligation under this DPA, law and regulations without compensation, unless otherwise agreed between the Parties.

15 Written information

Any information pursuant to this agreement shall be directed in writing to:
personvernombud@atb.no

16 Change of legislation etc.

At any changes and amendments in law or regulations, the Controller may demand an amendment to the agreement to ensure that it reflects any new obligations and demands.

17 Governing law and legal venue

This agreement is governed by Norwegian law, and the Parties choose Sør-Trøndelag tingrett as the legal venue. This also applies after termination of the agreement.

* * *

This agreement in 2 – two – originals, one to each Party.

Trondheim, xx.xx.2020

For AtB	**For Consultant**
(Controller)	(Processor)
……..	……
Name: Janne Solli	Name:
CEO	CEO