DATA PROCESSING AGREEMENT

between

PBL Medlemsservice AS co. reg. no. 884071232

the Data Processor

and

the Customer:

_____

the Data Controller

This agreement on the processing of personal data must be observed by the Data Processor as a consequence of having concluded an agreement with the Data Controller for the utility rights to one or more of our digital PBL Mentor solutions.

1. Purpose of the Agreement

The Data Processor processes personal data on behalf of the Data Controller on the basis of the above preamble.

PBL Member Service develops, operates and maintains PBL Mentor's services, along with the provision of service and support. PBL Member Service may, as part of the service and maintenance activities, user support, troubleshooting or other similar one-off assignments, require access to details in the system involving the processing of personal data.

The purpose of the processing, its duration and nature, as well as the types of personal data to be processed and categories of data subjects are set out in the appendix to this Agreement.

The Agreement shall ensure that personal data is processed in accordance with the requirements valid at any time for processing personal data. This includes the European Parliament's and Council's Regulation 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, GDPR) of 27 April 2016 and the Data Protection Act (hereinafter "data protection law").

The Data Processor shall process personal data in the manner described in the Agreement, or otherwise in a manner as agreed in writing between the Data Processor and Data Controller.

Terms and definitions used in the Agreement shall have the same understanding as under data protection law.

2. The rights and duties of the Data Controller The duties of the Data Processor

The Data Processor confirms that it will put in place suitable technical and organisational measures that ensure that all processing under this Agreement meets the requirements of personal data law and protection of the data subject's rights, including observation of all requirements set out under Article 32 GDPR. See also the additional duties under clause 4.

The Data Processor undertakes to provide the Data Controller with access to its security documentation and with assistance such that the Data Controller can fulfil its own responsibility according to the laws and regulations.

The Data Controller has the right, unless otherwise agreed or as required by law, to access and inspect the personal data being processed and the systems used for this purpose. The Data Processor undertakes to provide the assistance in such cases.

The Data Processor has a duty of confidentiality with respect to documentation and personal data which employees may have access to under this Agreement. This provision continues to apply beyond the end of the Agreement.

The Data Processor shall assist the Data Controller in answering requests from data subjects, having regard for the nature of the processing and, the extent possible, assist with suitable technical and organisational measures. This applies both to requests from data subjects for the exercise of their rights in pursuant to Chapter 3 GDPR and assisting the Data Controller in ensuring duties linked to data security are complied with. The same applies to assistance in assessing the impact on data protection as well as prior consultation as set out in Articles 32 to 36 GDPR, having regard for the nature of the processing and the information available to the Data Processor. If standards of conduct pursuant to Article 40 GDPR have been laid down or an approved certification scheme pursuant to Article 42 GDPR, which the Data Processor has undertaken to observe or be certified to, the Data Processor is obliged to comply with such standards of conduct or certification requirements.

The Data Processor must keep records (a log) of the processing activities it carries out on behalf of the Data Controller, which must contain, as a minimum, the information set out under Article 30 GDPR. The Data Controller may at any time request a copy of such records.

The Data Processor shall make available to the Data Controller all information that is necessary to demonstrate that the duties set out in this clause 2 have been fulfilled and facilitate and assist with audits, including inspections, performed by the Data Controller or another auditor mandated by the Data Controller. This also applies to providing access to security documentation. The Data Processor has direct responsibility with respect to the relevant supervisory authorities.

The Data Processor has an duty of confidentiality regarding personal data that employees may have access to as a result of the Agreement and processing of the personal data and must ensure that persons who are authorised to process the personal data undertake to observe confidentiality in processing the data or are subject to a suitable statutory duty of confidentiality. This provision also applies beyond the end of the Agreement.

The Data Processor shall not provide data or information to a third party without the explicit consent of the Data Controller. Enquiries to the Data Processor shall be forwarded by the Data Processor to the Data Controller as soon as possible.

The Data Processor shall immediately inform the Data Controller if instructions in the opinion of the Data Processor contravene GDPR or other legislation.

3. Use of subprocessors

The Data Processor shall only use subsuppliers for processing personal data (subprocessors) who have been approved in writing by the Data Controller and who have confirmed that they will put in place suitable technical and organisational measures that ensure that all processing under this Agreement meets the requirements under GDPR and protection of the data subject's rights.

The Data Controller grants the Data Processor general permission to use subprocessors to process personal data under the Agreement. In the event the Data Processor plans to use other subprocessors or replace subprocessors, the Data Processor shall inform the Data Controller of the plans and, in so doing, give the Data Controller the opportunity to object to such changes.

Subprocessors shall be subject to the same data protection duties as those specified in the Agreement, whereby subprocessors shall provide sufficient guarantees that technical and organisational measures will be implemented to ensure the processing meets legitimate requirements. If a subprocessor does not fulfil its data protection duties and the requirements under the Agreement, the Data Processor shall be fully responsible with respect to the Data Controller for ensuring that the subprocessor does fulfil its duties.

4. Security and deviations

The Data Processor shall observe the requirements on security measures set out in GDPR. The Data Processor shall be able to document procedures and other measures for meeting these requirements. The documentation shall be made available at the Data Controller's request.

Security audits must be conducted at regular intervals and the parties shall agree on the dates for such audits. The audit may include a review of procedures, random sample checks, more extensive local checks and other suitable control measures. It shall be agreed that it is the Data Processor's duty to cover any use of resources linked with conducting such an audit.

In the event of a security or personal data breach, the Data Processor shall notify the Data Controller without undue delay. As a minimum, notification of the breach must contain:

1. A description of the nature of the personal data breach, including, if possible, the categories and the approximate number of affected data subjects and the categories and the approximate number of affected personal data records.
2. The name and contact details of the data protection officer or another contact point from where more information can be obtained.
3. A description of the probable consequences of the personal data breach.
4. A description of the measures which have been taken or are proposed to manage the personal data breach, including, if applicable, measures to limit any possible damage resulting from the breach.

If it is not possible to provide the information in the initial notification, the information must be provided in phases as soon as it is available.

The Data Controller is responsible for reporting the breach to the supervisory authority. The Data Processor shall not send such a report or contact the supervisory authority unless the Data Controller has instructed such an action.

5. Transfer of personal data abroad

Personal data shall solely be transferred to a country outside the EU/EEA (third country) on documented instructions from the Data Controller. The Data Processor shall, therefore, not transfer or permit persons in a third country access to personal data in any way without the Data Controller having given explicit, written approval and prior documented instructions on the transfer or access. Consent and instructions must specify which countries it is permitted to transfer the data to. In addition to consent and instructions, the requirements governing the security and protection of the data subjects' rights under GDPR must be observed when transferring data to a third country.

6. Duration of the Agreement, order to stop, duties upon cessation/termination

The Agreement is valid for as long as the Data Processor processes or has access to personal data on behalf of the Data Controller.

The Data Controller may require that the Data Processor stops further processing of the data with immediate effect.

The Data Processor shall, on the Data Controller's instructions, erase or return all personal data to the Data Controller once the services linked to the processing have been supplied. In addition, existing copies shall be erased, unless there is a legitimate requirement for the continued storage of the personal data. This also applies to any backup copies, although it is sufficient here to overwrite the copies using established backup procedures.

The Data Controller shall receive a written confirmation from the Data Processor that all personal data has been returned or erased according to the Data Controller's instructions and that the Data Processor is no longer in possession of any copy, printouts or any other form of the personal data.

7. Other rights and duties

Other rights and duties are derived from the Master Agreement that applies between the Data Processor and Data Controller on the services that make the processing of personal data and this Agreement necessary. The same contact personnel apply to the Agreement as to the Master Agreement.

This Agreement shall not extend the Data Controller's sanction opportunities, including the liability to pay damages for the Data Processor, besides that derived from the Master Agreement.

In the event the Master Agreement is assigned to other parties, this Agreement shall be assigned accordingly.

Bodø, 30. 11 2018

the Data Processor	**Data Controller**
_____	_____
Direktør PBL Medlemsservice AS,	
Ole Reidar Sollund	

Appendix

Purpose of the processing

PBL Mentor comprises three digital solutions:

- PBL Mentor HMS
- PBL Mentor Kidplan
- PBL Mentor Frisk

PBL Mentor HMS:
Its purpose is to act as the business's HSE manual, internal control system, and staff and managers' handbook.

PBL Mentor Kidplan:
Its purpose is to act as the business's communication solution for parents and guardians. This solution comprises a website solution and various digital tools so that the daycare centre can communicate and share information with the children's parents/guardians.

PBL Mentor Frisk:
The purpose of this module is to generate absence statistics if employees are absent due to illness. The system is also designed to store follow-up notes in connection with follow-up discussions with an employee on sick leave.

Duration of the processing

The Data Processor and stores and processes personal data for as long as the customer relationship lasts.

Types of personal data to be processed

PBL Mentor HMS:

The following personal data shall be processed: Name, email address and telephone number of everyone with access to the solution.

PBL Mentor Kidplan:

Name and email address of all employees with user access to the solution.

Name, email address, home address and telephone number of parents and guardians with access to the solution from the daycare centre.

Name, date of birth, photo, attendance records, day reports and other possible sensitive health details of children, if the daycare centre makes use of the children's folder functionality.

PBL Mentor Frisk:

Name and email address of the solution's administrator (the daycare centre's staff manager).

Name, date of birth, absence history and any sensitive follow-up notes in connection with an absence due to illness follow-up.

Categories of data subjects

PBL Mentor HMS:

The business's employees.

PBL Mentor Kidplan:

The daycare centre's employees, children and parents and guardians.

PBL Mentor Frisk:

The business's employees.

Subprocessors upon commencement of the Agreement

PBL Mentor stores all data in its own database located in Bodø. No data is supplied to a third party or shared with other companies outside PBL.