

Data Processing Agreement

(Latest version September 2023)

Parties of the agreement:

PBL Mentor AS - reg.no. 884 071 232
(Here on after referred to as the Data Processor)

and

Customer - reg.no. xxx xxx xxx
(Here on after referred to as the Data Controller)

jointly referred to as the Parties.

Place and date:

Contracting parties

[Name of the signatory on behalf of the Data Controller]
[Name of the signatory on behalf of the Data Processor]


For the Data Controller	For the Data Processor
<div></div> <div>Signature</div>	<div>Stephan Skjelvan</div> <div></div> <div>Signature</div>

TABLE OF CONTENTS:

1	Purpose of this Data Processing Agreement	3
2	Definitions	3
3	Rights and obligations of the Data Controller	4
4	Instructions from the Data Controller to the Data Processor	4
5	Confidentiality and duty of secrecy	5
6	Assistance to the Data Controller	5
7	Security of processing	6
8	Notification of breach of personal data security	6
9	Use of Subprocessor.....	7
10	Transfer of personal data to countries outside the EEA	8
11	Audit	9
12	Erase and return of information	9
13	Breach and suspension order	10
14	Duration and expiry	10
15	Governing law and legal venue	10

1 Purpose of this Data Processing Agreement

- 1.1 This Agreement (the “Data Processing Agreement”) sets out the Parties’ rights and obligations when the Data Processor processes personal data on behalf of the Data Controller, as part the services delivered under the Main Agreement. The purpose of the Data Processing Agreement is to ensure that the Parties comply with the Applicable Privacy Policy.

The Data Processing Agreement comprises this document, as well as Appendices A, B, C and D.

- 1.2 In the event of conflict between the terms of the Main Agreement and the Data Processing Agreement, the terms of the Data Processing Agreement will take precedence regarding matters specifically related to the processing of personal data. In the event of any conflict between the Data Processing Agreement and its Appendices, the Appendices will take precedence.

- 1.3 **Appendix A** of The Data Processing Agreement includes a detailed description of the processing that is to take place, as well as the purpose of processing, categories of personal data and data subjects, rules for erasure/deletion and return, and the Parties’ designated contact persons, as well as which underlying agreement(s) the processing of personal data is related to (see the definition of the Main Agreement below).

- 1.4 **Appendix B** of The Data Processing Agreement includes conditions for the use of Subprocessors, as well as a list of approved Subprocessors.

- 1.5 **Appendix C** of the Data Processing Agreement contains specific instructions for the processing of personal data under the Main Agreement, including security measures and the Data Controller’s right of access to and audit of the Data Processor and any Subprocessors, as well as sector-specific provisions concerning the processing of personal data.

- 1.6 **Appendix D** of the Data Processing Agreement contains changes to the standard text and any subsequently agreed changes to the Data Processing Agreement.

2 Definitions

Applicable Privacy Policy: The applicable versions of the EU’s General Data Protection Regulation (2016/679) (“GDPR”) and the Norwegian Act on the Processing of Personal Data of 15.06.2018 (the Personal Data Act) with related regulations etc., and any other relevant legislation concerning the processing and protection of personal data, as specified in Appendix C, section C.7.

Main Agreement: One or more agreements between the Data Controller and the Data Processor concerning the provision of services which entail the processing of personal data, as specified in Appendix A. The Data Processing Agreement may apply to several underlying agreements.

Subprocessor: A company or person used by the Data Processor as a subcontractor for the processing of personal data under the Main Agreement.

Article 4 of GDPR will apply to privacy policy terms not defined in this agreement.

3 Rights and obligations of the Data Controller

The Data Controller is responsible for the processing of personal data in accordance with the Applicable Privacy Policy. The Data Controller must specifically ensure that:

- i. the processing of personal data is for a specified and explicit purpose and is based on valid legal grounds
- ii. the data subjects have received the necessary information concerning the processing of the personal data
- iii. the Data Controller has carried out adequate risk assessments; and
- iv. the Data Processor has at all times, adequate instructions and information to fulfil its obligations under the Data Processing Agreement and the Applicable Privacy Policy.

4 Instructions from the Data Controller to the Data Processor

- 4.1 The Data Processor shall process the personal data in accordance with the Applicable Privacy Policy and the Data Controller's documented instructions, cf. section 4.2. If other processing is necessary to fulfil obligations to which the Data Processor is subject under applicable law, the Data Processor must notify the Data Controller to the extent this is permitted by law, cf. Article 28 (3) (a) of GDPR.
- 4.2 The Data Controller's instructions are stated in the Main Agreement and the Data Processing Agreement with Appendices. The Data Processor must notify the Data Controller immediately if the Data Processor believes the instructions conflict with the Applicable Privacy Policy, cf. Article 28 (3) (h) of GDPR.
- 4.3 The Data Processor must be notified of any changes to the instructions by updating Appendix D, and changes must be implemented by the Data Processor by the date agreed between the Parties or, if no specific date has been agreed, within a reasonable time. The Data Processor may require the Data Controller to pay documented costs accrued in connection with the implementation of such changes, or the proportional adjustment of the

remuneration under the Main Agreement if the amended instructions entail additional costs for the Data Processor. The same applies to additional costs that accrue due to changes in the Applicable Privacy Policy which concern the activities of the Data Controller.

5 Confidentiality and duty of secrecy

- 5.1 The Data Processor must ensure that employees and other parties who have access to personal data are authorised to process personal data on behalf of the Data Processor. If such authorisation expires or is withdrawn, access to the personal data must cease without undue delay.
- 5.2 The Data Processor shall only authorise persons who need access to the personal data in order to fulfil their obligations under the Main Agreement, the Data Processing Agreement and any other processing that is necessary to fulfil obligations to which the Data Processor is subject, in accordance with applicable law, see section 4.1, last sentence.
- 5.3 The Data Processor must ensure that persons authorized to process personal data on behalf of the Data Controller are subject to obligations of confidentiality either by agreement or applicable law. The obligations of confidentiality shall survive the duration of the Data Processing Agreement and/or employment relationship.
- 5.4 At the request of the Data Controller, the Data Processor shall document that the relevant persons are subject to said obligations of confidentiality see section 5.3.
- 5.5 Upon the expiry of the Data Processing Agreement, the Data Processor is required to discontinue all access to personal data that is processed under the agreement.

6 Assistance to the Data Controller

- 6.1 When requested, the Data Processor shall assist the Data Controller with the fulfilment of the rights of the data subjects under Chapter III of the GDPR through appropriate technical or organisational measures. The obligation to assist the Data Controller solely applies insofar as this is possible and appropriate, taking into consideration the nature and extent of the processing of personal data under the Main Agreement.
- 6.2 Without undue delay, the Data Processor shall forward all enquiries that the Data Processor may receive from the data subject concerning the rights of said data subject under the Applicable Privacy Policy to the Data Controller. Such enquiries may only be answered by the Data Processor when this has been approved in writing by the Data Controller.
- 6.3 The Data Processor must assist the Data Controller in ensuring compliance with the obligations pursuant to Articles 32-36 of GDPR, including providing assistance with personal data impact assessments and prior consultations with the Norwegian Data Protection

Authority, in view of the nature and extent of the processing of personal data under the Main Agreement.

- 6.4 If the Data Processor, at the request of the Data Controller, provides assistance as described in sections 6.1 or 6.3, and the assistance goes beyond what is necessary for the Data Processor to fulfil its own obligations under the Applicable Privacy Policy, the Data Processor may claim all documented costs related to the assistance be reimbursed. The assistance will be reimbursed in accordance with the price provisions of the Main Agreement.

7 Security of processing

- 7.1 The Data Processor shall implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Data Processor must, as a minimum, apply the measures specified in Appendix C of the Data Processing Agreement.

- 7.2 The Data Processor shall carry out risk assessments to ensure that an appropriate security level is maintained at all times. The Data Processor must ensure regular testing, analysis and assessment of the security measures, in particular with regard to ensuring sustained confidentiality, integrity, availability and robustness in processing systems and services, and the ability to quickly restore the availability of personal data in the event of an incident.

- 7.3 The Data Processor must document the risk assessment and security measures and make them available to the Data Controller on request, and also allow for the audits agreed between the Parties, cf. section 11 of the Data Processing Agreement.

8 Notification of breach of personal data security

- 8.1 In case of a personal data breach, the Data Processor shall without undue delay, notify the Data Controller in writing of the breach, and in addition provide the assistance and information necessary for the Data Controller to be able to report the breach to the supervisory authorities in line with the Applicable Privacy Policy.

- 8.2 Notification in accordance with section 8.1 must be given to the Data Controller's point of contact in accordance with Appendix C, section C.9, and must:

- a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories of and approximate number of personal data records concerned
- b. state the name and contact details of the data protection officer or other contact point from where more information can be obtained

-
- c. describe the likely consequences of the personal data breach; and
 - d. describe the measures taken or proposed by the Data Controller to address the breach, including where appropriate, measures to mitigate possible adverse effects.

If necessary, information may be given in phases without any further undue delay.

- 8.3 The Data Processor shall implement all necessary measures that may reasonably be required to rectify and avoid similar personal data breaches. As far as possible, the Data Processor must consult the Data Controller concerning the measures to be taken, including assessment of any measures proposed by the Data Controller.
- 8.4 The Data Controller is responsible for notifying the Data Protection Authority and the data subjects affected by the personal data breach. The Data Processor may not inform third parties of any breach of personal data security unless otherwise required under applicable law or in accordance with the express written instructions of the Data Controller.

9 Use of Subprocessor

- 9.1 The Data Processor may only use Subprocessors with the prior general or specific written authorisation of the Data Controller, in accordance with Appendix B of the Data Processing Agreement. For an overview of approved Subprocessors, see Appendix B of the Data Processing Agreement.
- 9.2 If a Data Processor engages a Subprocessor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in this Data Processing Agreement shall be imposed on the Subprocessor by way of written agreement. See section 9.7 concerning the use of standard third-party services.
- 9.3 The Data Processor may only engage Subprocessors who provide appropriate technical and organisational measures to ensure that the processing fulfils the requirements in accordance with the Applicable Privacy Policy. The Data Processor must assess and verify that satisfactory measures have been taken by the Subprocessors. Upon request, the Data Processor must be able to submit reports from such assessments to the Data Controller.
- 9.4 If the Data Controller objects to changes in the use of Subprocessors pursuant to Appendix B, section B.1 of the Data Processing Agreement, the Parties must negotiate in good faith with the aim of reaching a reasonable solution to how the further delivery of the services under the Main Agreement is to take place, including the distribution of any costs between the Parties. The parties must come to an agreement before changes in the use of Subprocessors can be made.

-
- 9.5 If the Subprocessor fails to fulfil its data protection obligations, the Data Processor shall remain liable to the Data Controller for the performance of the Subprocessor's obligations in the same way as if the Data Processor himself was responsible for the processing.
- 9.6 The Data Processor is obligated, on request, to disclose agreements with Subprocessors to the Data Controller. This solely applies to the parts of the agreement that are relevant to the processing of personal data, and subject to any statutory or regulatory limitations. Commercial terms and conditions are not required to be submitted.
- 9.7 If the Data processor uses a subcontractor that provides standardised third-party services, the Parties may agree that the subcontractor's standard data processing agreement will be used and applied directly to the Data Controller as in a direct data processing relationship (i.e., not as a Subprocessor) under the following terms:
- The Data Controller must expressly accept under the Main Agreement that the standardised third-party services are provided on the subcontractor's standard terms
 - The Data processor must follow up on the standard terms on behalf of the Data Controller
 - The standard terms must fulfil the requirements in the Applicable Privacy Policy.

The Data Processor must follow up the data processing agreement with the subcontractor on behalf of the Data Controller, unless otherwise agreed in each individual case.

10 Transfer of personal data to countries outside the EEA

- 10.1 Personal data may only be transferred to a country outside the EEA ('Third country') or to an international organisation if the Data Controller has approved such transfer in writing and the terms in section 10.3 are fulfilled. Transfer includes, but is not limited to:
- a) processing of personal data in data centres, etc. located in a Third Country, or by personnel located in a Third Country (by remote access)
 - b) assigning the processing of personal data to a Subprocessor in a Third State; or
 - c) disclosing the personal data to a Data Controller in a Third Country, or in an international organisation.
- 10.2 The Data Processor may nonetheless transfer personal data if this is required by applicable law in the EEA area. In such cases, the Data Processor must notify the Data Controller, to the extent permitted by law.
- 10.3 Transfer to Third Countries or international organisations may only take place if there are the necessary guarantees of an adequate level of data protection in accordance with the

Applicable Privacy Policy. Unless otherwise agreed between the Parties, such transfer may only take place on the following grounds:

- a) a decision of the European Commission concerning an adequate level of protection in accordance with Article 45 of GDPR; or
- b) a Data Processing Agreement which incorporates standard personal data protection provisions as specified in Article 46 (2) (c) or (d) of the GDPR (EU model clauses); or
- c) binding corporate rules in accordance with Article 47 of GDPR.

10.4 Any approval by the Data Controller for the transfer of personal data to a Third Country or international organisation must be stated in Appendix B of the Data Processing Agreement.

11 Audit

11.1 Upon request, the Data Processor shall make available to the Data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and this Data Processing Agreement.

11.2 The Data Processor shall allow and contribute to inspections and audits carried out by or on behalf of the Data Controller. The Data Processor shall also allow and contribute to inspections conducted by relevant supervisory authorities. The Data Controller's review of any Subprocessor shall be conducted by the Data Processor, unless otherwise specifically agreed. Specific procedures for conducting audits are stated in Appendix C, section C.5.

11.3 If an audit reveals a breach in the obligations in the Applicable Privacy Policy or the Data Processing Agreement, the Data Processor must rectify the breach as soon as possible. The Data Controller may require the Data Processor to temporarily stop all or part of the processing activities until the breach has been rectified and approved by the Data Controller.

11.4 Each Party shall pay its own costs associated with an annual audit. If an audit reveals significant breaches of the obligations under the Applicable Privacy Policy or the Data Processing Agreement, the Data Processor shall pay for the Data Controller's reasonable costs accrued from the audit.

12 Erasure and return of information

12.1 Upon the expiry of this Data Processing Agreement, the Data Processor is obligated to return and erase all personal data processed on behalf of the Data Controller under the Data Processing Agreement, in accordance with the provisions of Appendix C, section C.6. This also applies to any back-up copies.

12.2 The Data Controller will determine how any return of personal data is to take place. The Data Controller may require return to take place in a structured and commonly used machine-readable format. The Data Controller will pay the Data Processor's documented

costs associated with the return unless this is included in the remuneration under the Main Agreement.

- 12.3 If a shared infrastructure or back-up is used and direct erasure is not technically possible, the Data Processor must ensure that the personal data is made inaccessible until it has been overwritten.
- 12.4 The Data Processor must confirm in writing to the Data Controller that the data has been erased or made inaccessible, and shall, upon request document how this has taken place.
- 12.5 Further provisions concerning erasure and return are stated in Appendix C.

13 Breach and suspension order

- 13.1 In the event of breach of the Data Processing Agreement and/or Applicable Privacy Policy, the Data Controller and relevant supervisory authorities may order the Data Processor to cease all or part of the processing of the data effective immediately
- 13.2 If the Data Processor fails to comply with its obligations pursuant to this Data Processing Agreement and/or Applicable Privacy Policy, this shall be deemed a breach of the Main Agreement, and the obligations, deadlines, sanctions and limitations of liability in the Main Agreement's regulation of the Supplier's breach will be applied, unless otherwise expressly agreed between the Parties in Appendix D.

14 Duration and expiry

- 14.1 The Data Processing Agreement will come into effect from the date it is signed by both Parties. The Data Processing Agreement shall apply for as long as the Data Processor processes personal data on behalf of the Data Controller. It shall also apply to any personal data held by the Data Processor or any of its Subprocessors after the expiry of the Main Agreement.
- 14.2 The rules concerning termination specified in the Main Agreement shall also apply to the Data Processing Agreement, to the extent this is applicable. The Data Processing Agreement may not be terminated if the Main Agreement is in effect unless it is replaced by a new Data Processing Agreement.

15 Governing law and legal venue

The Data Processing Agreement is governed by Norwegian law. Disputes will be resolved in accordance with the provisions of the Main Agreement, including any provisions concerning legal venue.

APPENDICES TO THE DATA PROCESSING AGREEMENT

THIS DOCUMENT CONSTITUTES THE FOLLOWING APPENDICES:

APPENDIX A – INFORMATION REGARDING THE PROCESSING

APPENDIX B - CONDITIONS FOR THE DATA PROCESSOR'S USE OF SUB-PROCESSORS

APPENDIX C - INSTRUCTIONS REGARDING THE PROCESSING OF PERSONAL DATA

APPENDIX D - CHANGES TO THE STANDARD TEXT OF THE DATA PROCESSING AGREEMENT AND SUSEQUENT CHANGES AFTER ENTERING INTO THE AGREEMENT

A.	Information about the processing	3	
A.1	The Main Agreement and the purpose of the processing of personal data	3	
A.2	The Data Processor's processing of personal data on behalf of the Data Controller .	3	
A.3	Types of personal data	4	
A.4	Categories of data subjects	4	
A.5	Duration of processing	5	
B.	Conditions for the Data Processor's use of and changes in any Subprocessors.....	5	
B.1	The Data Controller's approval of the use of Subprocessors.....	5	
B.2	Approved Subprocessors.....	7	
C.	Instructions concerning the processing of personal data.....	8	
C.1	Scope and purpose of processing.....	8	
C.2	Security of processing.....	8	
C.2.1	Specification of security level	8	
C.2.2	Information security management system.....	9	
C.3	Documentation.....	9	
C.4	Transfer of personal data - Location for processing and access	9	
C.5	Auditing and supervision procedures.....	10	
C.6	Erase and return of personal data upon the expiry of the agreement	11	
C.7	Sector-specific provisions concerning the processing of personal data	11	
C.8	Contact details.....	12	
D.	Changes to the standard text of the Data Processing Agreement and changes after the establishment of the agreement		13

A. INFORMATION ABOUT THE PROCESSING

A.1 The Main Agreement and the purpose of the processing of personal data

The Data Processor's processing of personal data on behalf of the Data Controller pertains to the delivery of services as described in the Main Agreement.

The Main Agreement is the following agreement(s) entered into between the Parties:

PBL Mentor Kidplan, communication system

The purpose of the processing is as follows:

Its purpose is to act as the business's communication system for parents and legal guardians. This solution consists of a website and various digital tools which the kindergarten can use to communicate and share information with the children's parents and legal guardians.

A.2 The Data Processor's processing of personal data on behalf of the Data Controller

The Data Processor's processing of personal data on behalf of the Data Controller concerns (nature of the processing):

- Name and email address of all employees with user access to the system.
- Name, email address, home address and telephone number of parents and legal guardians with access to the system.
- Name, date of birth, photo, attendance records, day reports and other possible sensitive health details of children will be registered if the kindergarten makes use of the function in "children's folder".
- SMS and e-mail sent from the solution.

A.3 Types of personal data

The processing concerns the following types of personal data concerning the data subjects (several options are possible):

<input checked="" type="checkbox"/>	<i>Special categories of personal data in accordance with Article 9 (1) of GDPR:</i> The communication system has a function called "Children's folder" which provides the opportunity to make notes in free text or save documents on each individual child.
<input type="checkbox"/>	<i>Other information subject to a special need for protection:</i> <i><Enter type, e.g. national identity number, financial details, performance assessments in employment relationships, etc.></i>
<input checked="" type="checkbox"/>	<i>Other personal data:</i> Employees: Name, email address, mobile phone number and type of position. Children: Name, date of birth and associated department in the kindergarten. Guardian: Name, e-mail address, mobile phone number and residential address.

A.4 Categories of data subjects

The processing concerns the following categories of data subjects:

The kindergartens employees, children, parents and legal guardians.

A.5 Duration of processing

Processing of personal data by the Data Processor under the Main Agreement may commence when the Data Processing Agreement has entered into force. The processing has the following duration (select one option):

<input checked="" type="checkbox"/>	The processing is not limited in time and lasts until the expiry of the Main Agreement.
<input type="checkbox"/>	The processing is limited in time and applies until <i><state date or criterion for termination, such as the conclusion of a project. Note that the processing may not normally be concluded before the Main Agreement expires >.</i>

On expiry (of the Main Agreement or the processing), personal data must be returned and erased in accordance with section 12 of the Data Processing Agreement and the instructions in Appendix C.

B. CONDITIONS FOR THE DATA PROCESSOR'S USE OF AND CHANGES IN ANY SUBPROCESSORS

B.1 The Data Controller's approval of the use of Subprocessors

When entering into the Data Processing Agreement, the Data Controller approves the use of the Subprocessors listed in section B.2. Note that parent and sister companies and subsidiaries of the Data Processor are also considered to be Subprocessors if they contribute to the delivery of services and process personal data.

The following is agreed concerning changes in the use of Subprocessors:

<input checked="" type="checkbox"/>	The Data Processor may use a Subprocessor from the same Group (parent or sister company or subsidiary) that is established in a country within the EEA. The Data Processor must inform the Data Controller in advance of the use of any such Subprocessor. (This option can be combined with one of the other options.)
<input checked="" type="checkbox"/>	The Data Processor may make changes to the use of Subprocessors provided that the Data Controller is notified and is given the opportunity to object to the

	<p>changes. Any such notification must be received by the Data Controller no later than one month before the change enters into force, unless otherwise agreed in writing between the Parties. Changes that entail the transfer of personal data to countries outside the EEA (third countries) still require written approval pursuant to section 10 of the Data Processing Agreement.</p> <p>If the Data Controller opposes the change, the Data Processor must be notified as soon as possible. The Data Controller may only object to the change on reasonable and justifiable grounds.</p>
<input type="checkbox"/>	<p>The Data Processor may only make changes to the use of Subprocessors with the specific prior written approval of the Data Controller. The Subprocessor may not process personal data under the Main Agreement before such approval has been granted. Approval shall not be unreasonably withheld.</p>

B.2 Approved Subprocessors

The Data Controller has approved the following Subprocessors:

Name	Reg. no.	Address	Description of processing	Processing location	Contact details	Special categories of personal data
<i>LinkMobility</i>	992 434 643	Langkaia 1 0150 OSLO	<i>SMS from Kidplan. See Linkmobility's information on privacy: https://linkmobility.no/brukerstotte/</i>	<i>All data is stored on LinkMobility's servers.</i>	support.norway@linkmobility.com +47 22 99 44 00	
<i>Mailgun</i>		San Antonio HQ 112 E Pecan St. #1135 San Antonio, TX 78205	<i>For notifications and newsletters, we use the 3rd party service MailGun to distribute the emails. We use the strictest settings for deleting e-mail at MailGun, i.e. they only process it for dispatch purposes and are deleted after a maximum of 72 hours.</i>	<i>Sending emails takes place through Mailgun's servers located in the EU.</i>	https://www.mailgun.com/contact/support	
<i>Microsoft corporation</i>		One Microsoft Way, Redmond WA, USA 9805	<i>File storage of documents and images, database storage of information stored in PBL Mentor HMS.</i>	<i>Data storage takes place at Microsoft's data centers in Norway. Microsoft is listed as an approved supplier on dataprivacyframework.gov, so personal data can be transferred to it as if it were a European business.</i>	https://www.microsoft.com/nb-no/trust-center/privacy	

The Data Processor may not use the individual Subprocessor for any other processing than as agreed or allow another Subprocessor to perform the processing described in cases other than as described in Appendix B, section B.1 concerning the replacement of a Subprocessor.

C. INSTRUCTIONS CONCERNING THE PROCESSING OF PERSONAL DATA

C.1 Scope and purpose of processing

The personal data may only be processed within the scope and for the purpose described in the

- Main Agreement
- Data Processing Agreement with appendices

The Data Processor does not have the right to use the personal data other than to the extent necessary to fulfil its obligations under the Data Processing Agreement and may not process this data for the Data Processor's own purposes.

C.2 Security of processing

C.2.1 *Specification of security level*

A specific risk assessment based on an assessment of the scope of the personal data that is processed, the type of information and the nature of the processing, determines that the processing (select one option):

☒ Requires a high security level. Reason:

The system allows the data controller to enter sensitive information.
The purpose of processing sensitive information is to be able to provide a kindergarten with good quality and safety. If, for example, a child has an allergy or intolerance, this is something that is important for the kindergarten to have information about. This is authorized with reference to § 23 of the Kindergarten Act, as well as art. 9 of the regulation. Here both letters A and B will be relevant. After risk assessment, we have built in a solution for two-factor authentication in the system. This is to prevent unauthorized persons from gaining access to information if the username and password gets lost.

☐ Does not require a high security level. Reason:

C.2.2 Information security management system

The Data Processor must have an appropriate system for managing information security. The Data Processor must establish and manage adequate security measures to protect information security concerning the processing of personal data, including (several options are possible):

<input type="checkbox"/>	Security requirements as described in the Main Agreement: <i><Insert reference to specific regulation in the Main Agreement></i>
<input checked="" type="checkbox"/>	Security requirements as described below: The data processor has its own system for risk assessments.

C.3 Documentation

The Data Processor shall document the procedures and measures taken to fulfil the requirements arising from the Applicable Privacy Policy and the Data Processing Agreement, including the information security requirements. This documentation must be stored and updated for the duration of the Data Processing Agreement and shall be made available to the Data Controller or supervisory authorities on request.

C.4 Transfer of personal data - Location for processing and access

Without the prior written approval of the Data Controller, processing of the personal data covered by the agreement may not take place at or with access from other locations than those specified in Appendix B.2. By location is meant:

- Place from where it is possible to access the personal data (access)
- Place where the personal data is handled (processed)
- Place where the personal data is stored

This limitation does not apply to parent and sister companies and subsidiaries of the Data Processor that are established within the EEA. At the request of the Data Controller, the Data Processor must, however, be able to document where the personal data is processed at any time.

C.5 Auditing and supervision procedures

In order to monitor compliance with the Applicable Privacy Policy and the Data Processing Agreement, the following has been agreed (several options are possible):

<input checked="" type="checkbox"/>	<p>The Data Controller has the right to conduct audits at the Data Processor's place of business in order to verify the Data Processor's compliance with its obligations under this Data Processing Agreement or the Applicable Privacy Policy.</p> <p>Such audits shall:</p> <ul style="list-style-type: none"> • Be subject to reasonable advance notice and shall be performed no more than once per year, unless a security breach at the Data Processor or other special circumstances justify more frequent audits • Take place during normal working hours and without unnecessary disruption of the Data Processor's work-related activities • Be performed by employees of the Data Controller or by third parties who are approved by the Parties and are subject to an obligation of confidentiality. <p>The Data Processor shall make available the necessary resources reasonably required in order to perform the audit.</p> <p>The Data Controller shall cover the costs of any third parties used to conduct the audit. Each Party will cover their own costs pertaining to the performance of the audit. If the audit reveals significant breaches of the obligations under the Applicable Privacy Policy or the Data Processing Agreement, the Data Processor must nonetheless cover the Data Controller's reasonable costs ensuing from audit.</p>
<input type="checkbox"/>	<p>The Data Processor will engage an external auditor to verify that security measures have been put in place and are working as intended. This audit must:</p> <ol style="list-style-type: none"> i. take place once a year, ii. be performed in accordance with recognised verification standards, such as ISAE 3402, and iii. be performed by an independent third party with sufficient knowledge and experience. <p>The reports must be submitted to the Data Controller on request.</p> <p>The Data Processor must also provide the information and assistance necessary for the Data Controller to be able to comply with its obligations under the Applicable Privacy Policy.</p>
<input type="checkbox"/>	<p>Third-party audits may be submitted, where standardised third-party services are provided by a Subprocessor, as long as the audit took place in accordance with generally recognised principles and by a certified auditor.</p>

<input type="checkbox"/>	<i><Insert any other audit procedures, including any special or deviating procedures for audits of Subprocessors that the Parties have agreed on></i>
--------------------------	---

C.6 Erasure and return of personal data upon the expiry of the agreement

The Parties have agreed on the following regarding erasure/return of personal data (select one option):

<input checked="" type="checkbox"/>	All personal data processed under this Data Processing Agreement must be erased without undue delay and no later than within 90 calendar days of the expiry of the Main Agreement. The same applies to any other relevant information managed on behalf of the Data Controller.
<input checked="" type="checkbox"/>	<p>All personal data processed under this Data Processing Agreement, and any other relevant information managed on behalf of the Data Controller, must be returned upon the expiry of the Main Agreement.</p> <p>Within 30 calendar days after return has taken place, the Data Processor is required to erase all personal data and other relevant information managed on behalf of the Data Controller.</p> <p>Return must take place as follows:</p> <p>Agreement between the data processor and the data controller.</p>
<input type="checkbox"/>	<i><Insert any other agreed procedures for erasure or return></i>

C.7 Sector-specific provisions concerning the processing of personal data

<Insert any sector-specific provisions concerning the processing of personal data to be covered by "Applicable Privacy Policy"; see section 2 of the Data Processing Agreement.>

C.8 Contact details

For any enquiries pursuant to this Agreement, such as notification of breach of personal data security or a change in the use of Subprocessors, the following channels must be used:

At the Data Controller

Security breach:

Phone:

E-mail:

Other enquiries:

Name:

Position:

Phone:

E-mail:

At the Supplier

Security breach:

Phone: 00 47 75 55 37 86/ 00 47 93 25 12 21

E-mail: stephan@mentorpluss.no

Other enquiries:

Navn: Marianne Amundsen Bergrud

Stilling: Product manager PBL Mentor AS

Telefon: 00 47 75 55 37 81/ 00 47 99 50 74

27 E-post: marianne@mentorpluss.no

**D. CHANGES TO THE STANDARD TEXT OF THE DATA PROCESSING AGREEMENT
AND CHANGES AFTER THE ESTABLISHMENT OF THE AGREEMENT**