Data Processing Agreement

between

[company name]
[company registration number]
[address]
[zip code and city]
[country]

hereinafter referred to as the "Controller"

and

BDO AS
Org.nr. 993,606,650
Munkedamsveien 45A
0250 OSLO
Norway

hereinafter referred to as the "Processor"

each of which is a "Party" and together constitutes the "Parties".

1. About the data processing agreement

The parties have entered into an agreement to [insert a brief description of the services BDO will deliver] (the "Engagement Agreement").

The purpose of this agreement (the "Data Processing Agreement") is to stipulate the rights and obligations of the Parties when the Processor processes personal data on behalf of the Controller in connection with providing the services as described in the Engagement Agreement.

The Data Processing Agreement shall ensure that the requirements of the EU General Data Protection Regulation 2016/679 (GDPR), the Personal Data Act (personopplysningsloven) and associated legislation are complied with. GDPR and the Personal Data Act with associated legislation are hereinafter jointly referred to as the "Data Protection Regulation".

The Data Processing Agreement is included as an appendix to the Engagement Agreement between the Controller and the Processor. In case of conflict between the Processor Agreement and other agreements between the Parties, the provisions of the Data Processing Agreement shall take precedence if the conflict concerns the processing of personal data. However, this does not apply to written instructions given pursuant to the Data Processing Agreement.

The Data Processing Agreement does not exempt the Processor from obligations imposed on the Processor under the Data Protection Regulation or other legislation.

2. Description of the processing

The purpose of the Processor's processing of personal data is [insert purpose].

The Processor may process personal data about the following categories of data subjects:

- [Insert who the personal data relates to, such as the client's employees, etc.]

The Processor may process the following types of personal data about the data subjects:

☐ **Special categories of personal data according to Article 9 of the GDPR:**

[Specify type, such as information regarding health or trade union membership]

☐ **Other personal data worthy of special protection:**

[Specify type, such as social security number or information about income and debt]

☐ **Other personal data:**

[Specify type, such as name, telephone number, email address, education, and employment details, including position, title or working hours]

3. Rights and obligations of the controller

The Controller is responsible for ensuring that the processing of personal data takes place in accordance with the GDPR, other relevant legislation and the Data Processing Agreement. Among other things, the Controller is obliged to ensure that there is a valid legal basis for the processing that the Processor shall carry out pursuant to the Data Processing Agreement.

The Controller has both a right and a duty to determine the purpose of the processing and the means to be used.

The Controller shall provide the Processor with instructions on how the personal data shall be processed pursuant to the Data Processing Agreement. These instructions are part of the Data Processing Agreement. However, the Controller may change the instructions at any time provided that the instructions do not conflict with requirements imposed by the GDPR. Such instructions shall be given in writing.

4. The processor's obligation to act according to instructions

The Processor may only process personal data in accordance with the Data Processing Agreement, the Engagement Agreement, and documented instructions from the Controller, unless the Processor is subject to statutory requirements to process the personal data. If the Processor is subject to such requirements, the Processor shall notify the Controller thereof before processing is initiated, unless such notification is prohibited by law.

The Processor is obliged to notify the Controller if the Controller's instructions conflict with requirements imposed by the GDPR or other legislation.

5. Confidentiality

The Processor shall ensure that the personal data pursuant to the Data Processing Agreement is only accessible to authorized persons. The Processor shall only authorize persons who need access to the personal data to perform the services as described in the Engagement Agreement. The Processor shall revoke such access if the need for access is no longer present.

The Processor shall ensure that authorized persons with access to the personal data are subject to a duty of confidentiality. The Controller may require the Processor to document that authorized persons are subject to such a duty. The obligation to ensure the confidentiality of personal data also applies after the termination of the Data Processing Agreement.

6. Security of processing

The Processor shall carry out all technical, organizational and security measures necessary pursuant to GDPR Article 32 and the Data Processing Agreement.

The Processor shall, as a minimum:

- Implement necessary technical and organizational measures regarding the confidentiality, integrity, and availability of the processing of personal data on behalf of the Controller to ensure a satisfactory level of information security. The Processor shall carry out risk assessments to determine what constitutes a satisfactory level of information security.
- Have internal control.

- Have procedures for authorization and management of access that ensure that only persons with a need for access to personal data have such access and ensure that these are complied with.
- Have routines for handling incidents and ensure that these are complied with.
- Ensure that personal data covered by the GDPR art. 9 and other personal data worthy of special protection, such as social security numbers and payroll information, are subject to such protection and are not sent by unencrypted e-mail.

7. Personal data breaches

In the event of a personal data breach pursuant to Article 4 (12) of the GDPR, the Processor shall notify the Controller without undue delay after becoming aware of the breach.

If the breach requires the Controller to notify the supervisory authority or data subjects, the Processor shall, taking into account the nature of the processing and the information available to the Processor, assist the Controller in fulfilling the obligations under Article 33(3) and Article 34(3) of the GDPR. To the extent that it is not possible to provide all necessary information at the same time as the notification, it may be given in stages without further undue delay.

8. Sub-processors

A sub-processor means a person (physical or legal) who processes personal data on behalf of BDO AS.

The Controller gives the Processor a general written permission to use sub-processors. When entering into the Data Processing Agreement, the Processor has stated that the sub-processors listed in annex 1 will be used to provide the agreed services. A complete and up-to-date list of BDO's sub-processors can be found on BDO's website.

If the Processor makes changes in their use of sub-processors that the Controller is not aware of, the Processor shall notify the Controller thereof within a reasonable time before the sub-processor is engaged. Such notification shall be made by BDO updating the list of sub-processors on BDO's website. The Controller has the right to object to the Processor's use of sub-processors as long as this is justified. If the Controller objects to the change, the Processor shall be notified as soon as possible.

Where the Processor engages a sub-processor for carrying out specific processing activities, it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the Processor in accordance with this Data Protection agreement.

The Processor shall remain fully responsible to the Controller for the performance of the sub-processor’s obligations in accordance with its contract with the processor.

9. Transfer of personal data

The Data Processor may not, without a written agreement with the Controller, transfer personal data processed under the Data Processing Agreement to countries outside the EU/EEA area ("Third Countries") or to international organizations, unless the European Commission has decided that the country or the international organization has an adequate level of protection, or the Processor is subject to legal obligations requiring such transfer. In the event of a transfer, the Processor shall implement appropriate safeguards in accordance with the Data Protection Regulation.

10. Assistance to the controller

If the Processor receives any requests from data subjects in connection with the processing of personal data for the Controller, the Processor shall forward the request to the Controller without undue delay.

The Processor is obliged, to the extent possible and taking into account the nature of the processing, to assist the Controller in responding to requests from data subjects regarding the exercise of their rights.

The Processor shall also assist the Controller in ensuring compliance with the obligations of Articles 35 and 36 of the GDPR, taking into account the nature of the processing and the information available to the Processor.

11. Audits

The Processor shall make available to the Controller all information necessary to demonstrate that the Processor complies with its obligations under the Data Processing Agreement.

The Processor shall conduct security audits of information systems used to process personal data on behalf of the Controller. The Processor may use an independent third party to conduct such security audits. The Processor shall, upon request, make available to the Controller the summary of the audit. Upon request, a detailed report can also be shared with the Controller in a meeting.

The Processor shall enable the Controller, supervisory authorities or a third party designated by the Controller to conduct its own audits in accordance with the Data Protection Regulation, including inspections. However, if an independent third party has conducted a security audit with the Processor within the last 12 months, and the Processor confirms that there are no changes thereafter, the Controller shall accept these reports rather than request a new audit.

If the third-party audit does not cover the Controller's needs, a separate audit can be arranged with the Processor. The Controller shall have the right to carry out such audit a maximum of once a year and is responsible for covering the costs of the audit, including the Processor's costs and time spent. If such audit is to include an inspection, the Processor shall be notified in writing and no later than 30 days before the inspection is to be carried out. Inspections shall take place within the Processor's normal office hours and shall have the least possible impact on the Processor's daily activities. If the Controller appoints a third party to conduct the audit, the third party shall be bound by a duty of confidentiality in accordance with BDO's requirements.

The Controller's right to information in connection with audits shall be limited to that related to the services provided by the Processor on behalf of the Controller. The Controller shall not have the right to access information concerning the Processor's other clients or other information that is subject to a duty of confidentiality.

12. Term and termination

The Data Processing Agreement enters into force when both Parties have signed the Data Processing Agreement and it is valid for as long as the Engagement Agreement applies.

In the event of a breach of the Data Processing Agreement or the Data Protection Regulation, the Controller may order the Processor to stop the processing of personal data with immediate effect.

Upon termination of the Data Processing Agreement, the Processor shall, upon request, return and/or delete all personal data that has been processed under the Data Processing Agreement,

unless it is necessary to keep the personal data longer in order to document the Processor's performance of the services or the Processor is subject to legal obligations to store the personal data. This also applies to any backups, but where it is sufficient to overwrite according to the Processor's established backup routines. Upon request, the Processor shall provide the Controller with a written confirmation that the personal data has been deleted.

13. Notices

Notifications pursuant to the Data Processing Agreement shall be sent in writing to:

Controller	Processor
Name: [Insert] **Email:** [Insert] **Telephone:** **[Insert]**	**Name:** **[Insert]** **Email:** **[Insert]** **Telephone:** **[Insert]**

14. Governing law and venue

The Data Processing Agreement is governed by Norwegian law and the Parties adopt Oslo District Court as the legal venue. This also applies after termination of the Data Processing Agreement.

Annex 1: Sub-processors

Name	Description of services	Hosting location
Intility AS	IT infrastructure provider, including operation of applications, storage and backup of data.	Norway
Brussel Worldwide Services BV/ BDO Global	Operation and development of BDO's Customer Portal and audit tools.	Netherlands / Ireland
Microsoft Ireland Operations Ltd.	Microsoft 365 and Azure provider	Netherlands / Ireland
Tessian	Provider of software to ensure information security when using e-mail.	Ireland
Inmeta Consulting AS	Personnel that assist with the development and improvement of IT systems.	N/A
[If relevant, insert any other sub-processors used]	[Describe the service provided]	[Insert where the personal data is stored]