DATA PROCESSING AGREEMENT

1. Scope and Applicability

The use of the Supplier's SaaS solutions and services may imply access to personal data, thus subject to the EU General Data Protection Regulation (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 and repealing Directive 95/46/EC, hereafter GDPR). Therefore, this Data Processing Agreement (hereafter DPA) applies to Suppliers' Processing of Personal Information on behalf of the Client as a Processor for the provision of the Services specified in the SaaS Terms document. Unless otherwise expressly stated in the Agreement, the Data Processing Agreement shall be effective and remain in force for the term of the SaaS Agreement.

This DPA is a part of the SaaS Agreement for the provision of the Supplier's services, together with the Annex 1 to this DPA. Annex 1 (available upon request) is an integral part of the DPA and includes the subject matter of processing, duration of processing, nature and purpose of processing, types of personal data, sub-processors, security measures, and technical and organizational measures in place. In the event of any conflict, discrepancy, error or omission, the Data Processing Agreement shall take precedence over the Agreement and its other sections for matters relating to privacy under the GDPR.

This DPA shall not exempt the data processor from obligations to which the data processor is subject pursuant to the GDPR or other applicable privacy legislation.

2. Responsibility for Processing of Personal Information

2.1 The client is and will at all times remain the Controller of the Personal Data Processed by SaaS solutions and services under the Agreement. Client is responsible for compliance with the obligations as a Controller under Applicable Data Protection Law, in particular for justification of any transmission of Personal Data to the Supplier (including providing any required notices and obtaining any required consents and/or authorizations, or otherwise securing an appropriate legal basis under Applicable Data Protection Law), and for all decisions and actions concerning the Processing of such Personal Data.

2.2 The Supplier and any persons acting under the authority of the Supplier, including any Third Party sub-processors as set forth in Section 4, will Process Personal Data solely for the purpose of providing the Services in accordance with the Terms of the Agreement and this Data Processing Agreement and always according with instructions of the Client.

2.3 Unless otherwise specified in the Terms of the Agreement, the Client may not provide the SaaS Solution with any sensitive or special Personal Information that imposes specific data security or data protection obligations on the Supplier.

2.4 The Supplier is responsible to comply with The General Data Protection Regulation (GDPR) in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area as well as any other regulations governing personal data.

2.5 Instructions. The Supplier, as processor, shall process personal data only on documented instructions from the Controller, unless required to do so by Union or

Member State law to which the processor is subject. Such instructions shall be specified in the Agreement.

The Controller's instructions are stated in the Agreement and this DPA with Annex 1. The processor must notify the Controller immediately if the processor believes the instructions conflict with the applicable privacy policy, cf. Article 28 (3) (h) of GDPR.

Subsequent instructions can also be given by the Controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the DPA. The processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions. If the processor is in breach of this DPA, then the Controller shall have the right to terminate the DPA.

3. Rights of Data Subjects

The Supplier grant the Client electronic access to SaaS Service and Solution under the Agreement which will be responsible to respond to requests from Data Subjects to exercise their rights under Applicable Data Protection Law, including requests to access, delete or erase, restrict, rectify, receive and transmit, block access to or object to Processing of specific Personal Data or sets of Personal Data.

4. Third Party sub-processors

The processor may use sub-processors as defined in Annex 1 of this document. The processor may change sub-processor for the provision of the services, and such changes shall be notified to the Controller. The Controller may not object to the change of such sub-processor, except terminate the Agreement according to the termination clauses set in the SaaS Terms document.

To the extent the Supplier engages Third Party sub-processors to assure support services, such entities shall be subject to the same level of data protection and security as the Supplier under the terms of the Agreement and this DPA. The Supplier is responsible for the performance of the Third Party sub-processors' obligations in compliance with the terms of this DPA and Applicable Data Protection Law.

5. Security and Confidentiality

5.1 The Supplier has implemented and will maintain appropriate technical and organizational security measures for the access of Personal Information to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures.

5.2 The Supplier take reasonable steps to ensure the reliability of any employee, agent or contractor of any sub-processor who may have access to the Client Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Client Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that

individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6. Personal Data Transfers

The SaaS Service and solution under this contract is held in a Cloud Services environment and because of that the Supplier may access on a global basis as necessary to perform the Cloud Services, including for IT security purposes, maintenance and performance of the Cloud Services and related infrastructure, Cloud Services technical support and Cloud Service change management.

6.1 The Supplier assure that in case of transfer of the Saas Service and solutions, this transfer will only be made to countries originating from the European Economic Area (EEA), or if not originating from EEA such transfer may take place on the following grounds,

(i) a decision of the European Commission concerning an adequate level of protection in accordance with Article 45 of GDPR; or

(ii) 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

(iii) binding corporate rules in accordance with Article 47 of GDPR.

7. Incident Management and Breach Notification

7.1 The Supplier has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorized disclosure or access to Personal Information transmitted, stored or otherwise Processed. The Supplier will promptly define paths to investigate such incidents in order to confirm if a Personal Information Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of the Personal Information Breach, mitigate any possible adverse effects and prevent a recurrence.

7.2 The Supplier shall notify the Client without undue delay when becoming aware of a Personal Data Breach affecting Client Personal Data, providing Client with sufficient information to allow the Client to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws. The notification must according to GDPR:

i. 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
ii. state the name and contact details of the data protection officer or other contact point from where more information can be obtained
iii. describe the likely consequences of the personal data breach; and
iv. describe the measures taken or proposed by the 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.

7.3 The Supplier shall cooperate with the Client and take reasonable commercial steps as are directed by Client to assist in the investigation, mitigation and remediation of each

such Personal Data Breach and agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected Data Subjects and/or notices to the relevant Supervisory Authorities.

7.4 The Controller is responsible for notifying the Data Protection Authority and the data subjects affected by the personal data breach. The 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 Controller.

8. Return and Deletion of Personal Information

8.1 Upon termination of the Agreement, the Supplier shall promptly return, including by providing available data retrieval functionality, or delete any remaining copies of Personal Information on Supplier systems or Services environments, except as otherwise stated in the Agreement.

8.2 For Personal Information held on Client systems or environments, or for Services for which no data retrieval functionality is provided by the Supplier as part of the Services, the Client must take appropriate action to back up or otherwise store separately any Personal Information while the production Services environment is still active prior to termination.

9. Legal Requirements

9.1 The Supplier may be required by law to provide access to Personal Information, such as to comply with a subpoena or other legal process, or to respond to government requests, including public and government authorities for national security and/or law enforcement purposes.

9.2 The Supplier will promptly inform the Client of requests to provide access to Personal Information, unless otherwise required by law.

10. Assistance to the Controller

10.1 When requested as required under GDPR, the processor shall assist the 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 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 Agreement.

10.2 Without delay, the processor shall forward all enquiries that the processor may receive from the data subject concerning the rights of said data subject under the applicable privacy policy to the Controller. Such enquiries may only be answered by the processor when this has been approved in writing by the Controller.

10.3 The processor must assist the 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 Agreement.

10.4 If the processor, at the request of the Controller, provides assistance as described in sections above, and the assistance goes beyond what are the processor's own

obligations under the GDPR, the processor may claim all costs related to the assistance be reimbursed according to the hourly rates and other price provisions of the Agreement.

11. Security of processing

11.1 The 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 processor must, as a minimum, apply the measures specified in Annex 1 of the DPA.

11.2 The processor shall carry out risk assessments to ensure that an appropriate security level is maintained at all times. The 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.

11.3 The processor must document the risk assessment and security measures and make them available to the Controller on request, and also allow for the audits agreed between the Parties, cf. section 12 of the Data Processing Agreement.

12. Audit

12.1 Upon request, the processor shall make available to the Controller all relevant information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and this DPA. Such information is defined in Annex 1 (available upon request).

12.2 Subject to legal requirements of the GDPR, the processor shall allow and contribute to inspections and audits for the compliance of the service, and if so performed by a third-party appointed by the processor. The processor shall also allow and contribute to inspections conducted by relevant supervisory authorities. The Controller's review of any sub-processor shall be conducted by the processor, unless otherwise specifically agreed. Specific procedures for conducting audits are stated in Annex 1.

12.3 If an audit reveals a breach in the obligations in the applicable privacy policy or the DPA, the processor must rectify the breach as soon as possible. The Controller may require the processor to temporarily stop all or part of the processing of the Controller's data activities until the breach has been rectified.

12.4 The Controller shall pay for all costs related to the processor's audit.

13. Breach and suspension of order

13.1 In the event of breach of the DPA and/or the applicable privacy policy, the Controller and relevant supervisory authorities may order the processor to cease all or part of the processing of the data effective immediately.

13.2 If the processor fails to comply with its obligations pursuant to this DPA, this shall be deemed a breach of the Agreement, and the limitations of liability in the Agreement shall apply.

14. Duration and expiry

14.1 The DPA comes into effect from the date of the signing of the Agreement. The DPA shall apply for as long as the processor processes personal data on behalf of the Controller. It shall also apply to any personal data held by the processor or any of its sub-processors after the expiry of the Agreement.

14.2 The rules concerning termination specified in the Agreement shall also apply to the DPA, to the extent this is applicable. The DPA may not be terminated if the Agreement is in effect unless it is replaced by a new Data Processing Agreement.

15. Governing law and jurisdiction

This DPA is governed by Norwegian law. Disputes will be resolved in accordance with the provisions of the Agreement, including any provisions concerning legal venue.