Data Processing Agreement – Synergi Life Risk Management SAAS

Version February 22, 2021

This Data Processing Agreement (the "**Data Processing Agreement**") is an addendum to the Synergi Life Risk Management SAAS terms entered into between Customer and DNV AS ("**SAAS Agreement**"). All capitalised terms not defined in this Data Processing Agreement shall have the meanings set forth in the SAAS Agreement. Unless otherwise expressly stated in the SAAS Agreement, this version of the DPA shall be effective and remain in force for the term of your SAAS Agreement.

Hereinafter Customer is referred to as "Data Controller" and DNV AS, Veritasveien 1 1363 Høvik, Norway, hereinafter is referred to as "Data Processor".

Data Controller and Data Processor hereinafter jointly referred to as the "Parties" and each of the Parties individually also as a "Party".

Recitals

In the course of its business activities and under the SAAS Agreement, Data Processor receives from Data Controller access to personal data controlled by the Data Controller. This Data Processing Agreement is concluded in order to suffice Data Controller's data protection obligations under European data protection law.

§ 1 Definitions

1. Personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (hereinafter referred to as "Data").

2. Affiliates are defined as: any subsidiary, parent, ultimate holding company or a subsidiary of such parent or ultimate holding company. For the purpose of this definition, "subsidiary" and "holding company" shall have the meaning assigned to them under the Companies Act relevant to the applicable law.

3. Commissioned data processing shall mean any processing of Data by Data Processor on behalf of Data Controller.

§ 2 Details of the processing

1. Subject and duration of the work to be carried out

   According to the SAAS Agreement between the parties

2. Categories of personal data

   The following type of Personal Data / Personal Data categories will be subject of the processing of Data:

Corporate Customer details may include address, telephone, title, mobile numbers, e-mail, age, customer number, purchase and/or service use history and details, IT management details, all depending on Customers setup, configuration and use.

3. Purpose of the intended processing of Data

Assist Data Controller in hosting the solution and/or assisting Data Controller with technical support on the solution.

4. Categories of data subjects

Categories of Data Subjects, as determined by the Controller, may include customer representatives and (end) users, such as employees, contractors, collaborators, partners, suppliers and customers of the Customer.

It is Data Controllers obligation to notify Data Processor if No. 1 to No. 4 differ.

5. Technical and organizational measures

Technical and organizational measures to be implemented by Data Processor are stipulated in **Annex 1** to this Data Processing Agreement.

6. Rectification, erasure, and blocking of Data, portability requests and objection

Any claim of data subjects arising out of the processing of Data by Data Processor, including but not limited to rectification, erasure, and blocking of Data, portability requests and objection, has to be asserted to Data Controller. Data Controller is solely liable for any of such claims.

In scope of its activity for Data Controller, Data Processor shall transmit any claim or request of data subjects to Data Controller to ensure appropriate reaction. Data Processor shall not be entitled to decide on its own discretion on any claim or request without consultation of Data Controller.

Data Processor shall rectify, erase, and block Data as ordered by Data Controller and Data Processor has the right to charge for any work resulting from such a request.

7. Obligations of Data Processor

Data Processor shall process Data only within the scope of the work to be carried out, according to documented instructions of Data Controller, unless Data Processor is required to otherwise by Union or Member State law. In this case, Data Processor shall inform Data Controller of that legal requirement before processing, unless such information is prohibited by that law.

Data Processor shall supervise and keep records on any technical and organizational measures with respect to § 2 No. 5 of the Data Processing Agreement on a regular basis. Data Processor shall provide Data Controller with respective records on request.

Data Processor has appointed the person listed below as a contact person for data protection purposes:

Ingrid Fladmark Cornic
GDPR responsible Digital Solutions
e-mail: Ingrid.Cornic@dnv.com

Data Processor shall be liable with regard to ensuring Data confidentiality. All persons of Data Processor who may access Data shall be pledged to confidentiality or shall be under an appropriate statutory obligation of confidentiality, and shall be notified of the data protection obligations specifically arising from the work to be carried out, and any order or appropriation hereof.

The processing of Data shall only take place within the EU or the European Economic Area (EEA). Data Processor may not transfer or authorize the transfer of Data to countries outside the EU and or the EEA without approval of Data Controller except for Affiliates

8. Subcontracting

Data Controller hereby provides Data Processor with a general written authorization to employ sub-processors under this Data Processing Agreement. Data Processor informs Data Controller of any intended changes concerning the addition or replacement of sub-processors, thereby giving Data Controller the opportunity to object to such changes. Subcontractors used are listed in Annex 2.

Where Data Processor subcontracts its obligations under the Data Processing Agreement, Data Processor shall ensure that the subcontract imposes substantially the same obligations on the subcontractor as are imposed on Data Processor under this Data Processing Agreement.

Data Processor shall prior to and regularly during the term of the subcontract supervise the technical and organizational measures which are necessary to protect Data and were implemented by the subcontractor.

Data Controller agrees that Data Processor has a general consent to use the Data Processor’s Affiliates as Sub-Processors when Processing Personal Data.

9. Rights of Data Controller to monitor

Data Processor agrees that Data Controller is entitled to monitor compliance with applicable data protection laws and this Data Processing Agreement during the regular business hours. Data Processor covenants to provide Data Controller with all information that is reasonably necessary to conduct these monitoring procedures within an appropriate time period.

If Data Controller is convinced that an audit on-site at Data Processor is necessary, Data Processor warrants Data Controller access to the offices of Data Processor, and to the stored Data and data processing programs on-site. Data Controller is entitled to have the audit carried out by a third party (auditor) that is to be appointed on an individual basis. The Parties shall agree well in advance on the time and other details relating to the conduct of such Audits.

10. Notification of violations of Data Processor

Data Processor will notify Data Controller immediately about any case in which Data Processor or one of its employees breaches any provision regarding the protection of Data of Data Controller or the obligations under this Data Processing Agreement.

Data Controller shall be notified about any loss, or illegal transmission, or third party acquisition of Data irrespective of causation. Data Processor shall take appropriate measures in consultation with Data Controller regarding the security of the Data as well as the reduction of possible disadvantageous consequences for the data subjects. Insofar as notification obligations apply to Data Controller, Data Processor must assist Data Controller in fulfilling these obligations.

11. Orders by Data Controller

The processing of Data Controller's Data by Data Processor is solely carried out within the framework of the Data Processing Agreement and the specific documented and reasonable individual instructions by Data Controller.

Data Processor shall comply with (individual) instructions regarding type, extent and procedure of Data processing.

Data Processor shall promptly notify Data Controller, if Data Processor assumes that a given instruction by Data Controller may violate data protection provisions. Data Processor is entitled to suspend the processing of the respective instruction until it has been confirmed or amended by the authorized person of Data Controller.

Unless otherwise agreed, the Data Processor shall have the right to charge any work resulting from the above executed instructions.

12. Erasure of Data after the work has been carried out

After the commissioned data processing has been carried out, Data Processor shall hand over, or upon prior consent of Data Controller only, destroy in a secure and data protective manner, or safely erase according to the state of the art, all Data processed for Data Controller. Any right of retention regarding the documentation, Data, processing and utilization results and the correspondent Data carrier is excluded, unless European Union or EU Member State law requires storage of the Data.

§ 3 Further Obligations of Data Processor

1. Data Processor shall not use the transmitted Data for any other purposes than the Data processing. Copies or duplicates must not be created without knowledge of Data Controller, provided that this is not part of the work to be carried out as set forth in this Data Processing Agreement.

2. Data Processor shall support Data Controller to the appropriate extent in defending against claims arising from alleged or actual violation of data protection requirements. Data Controller will pursue complaints issued by data subjects within the framework of its data protection liability to an appropriate extent and will deal with such complaints.

3. Data Processor acknowledges that information to the data subject due to an information claim of the data subject is given exclusively by Data Controller or by an authorized representative of Data Controller. Data Processor is obliged to provide Data Controller with the relevant information and support Data Controller.

4. Data Processor shall support Data Controller in the execution of data protection impact assessments where a type of processing under this Data Processing Agreement is likely to result in a high risk to the rights and freedoms of natural persons. Data Processor shall support Data Controller in the consultation of supervisory authorities prior to processing where data protection impact assessments indicate that the processing would result in a high risk to the rights and freedoms of natural persons.

5. Unless otherwise agreed, the Data Processor shall have the right to charge any work resulting from the support described under 3 – 4 above.

§ 4 Obligations of Data Controller

1. Data Controller shall be solely liable for the legality of Data processing including but not limited to acquiring consent from data subjects, and safeguarding the rights of data subjects.

2. Data Controller shall inform Data Processor about any faults or irregularities in the Data processing by Data Processor discovered by Data Controller.

§ 5 Final provisions

1. If any of the Data of Data Controller at Data Processor may be endangered by seizure or confiscation, insolvency proceedings or composition proceedings, or any other events or measures taken by a third party, Data Processor shall inform Data Controller hereof. In addition, Data Processor shall inform any such third party that sovereignty and ownership of the Data belong solely to Data Controller.

2. If one or more stipulations of this Data Processing Agreement are deemed void, this shall not affect validity of the other stipulations of this Data Processing Agreement. In the event of invalidity of one or more stipulations of this Data Processing Agreement the Parties shall negotiate a legally effective provision commercially close to the invalid stipulation. The same shall apply in the event of a regulatory gap.

3. This Data Processing Agreement shall be governed by and construed exclusively in accordance with the laws of Norway, without regard to principles of conflict of law.

4. The parties shall use their reasonable efforts to resolve any claim or dispute arising in relation to this Data Processing Agreement by negotiations within a reasonable time. Should the parties fail to resolve any claim or dispute by negotiations, the dispute shall be exclusively subject to the jurisdiction of the courts of Oslo, Norway

3. In the event of any conflicting stipulations between this Data Processing Agreement and other agreements in place between the Parties, the stipulations within this Agreement shall prevail.

****

Annex 1

to the Data Processing Agreement

Technical and organizational measures

This text reflects the security responsibilities for DNV Digital Solution as a service provider to the DNV Business Areas and customers. Our service offerings are built using different platforms.

GENERAL INFORMATION

Digital Solutions is ISO27001 certified which covers information security and security of personal data. The Information Security management system ensures proper processes and that necessary risk assessments and controls are in place. This also includes technical measures like encryption, anonymization and secure communication.

All personal data received from controllers are documented per GDPR requirements.

For customer projects handling personal data, security of personal data is subject to the same strict regulations and procedures as per GDPR requirements.

PHYSICAL ASSET MANAGEMENT ON PREMISE

DNV Digital Solutions only allows hardware to connect to the internal network that has been subject to DNV approval, and that has been recorded in the internal IT register. The asset registration includes information such as a unique description, the specific business purpose, the physical location of the asset, and any applicable compliance requirements. The asset is tracked throughout its lifecycle to ensure that all assets are accounted for, and that no assets unable to meet the criteria of the approval are connected to the internal IT network.

APPLICATION SECURITY

All network traffic within our solutions are encrypted using standard secure transport protocols. Certificates and secrets stored securely. Multiple encryption methods, protocols, and algorithms are deployed to help provide a secure path for data to travel through the infrastructure - Protocols and technologies examples include: Transport Layer Security/Secure Sockets Layer (TLS/SSL), symmetric cryptography based on a shared secret to encrypt communications as they travel over the network.

Annex 2:

Subcontractors

All Affiliates of Data Processor.

The following external sub-contractors are used:

Microsoft Corporation