DATA PROCESSING AGREEMENT

Between Keyforce AS (“Processor”) and Customer (“Controller”)

This agreement is valid from November 1st, 2023.

1. Purpose and definitions

The purpose of this Data Processing Agreement is to regulate the Processor’s processing of personal data on behalf of the Controller whilst providing the Keyforce AS Software (“the Service”) as further described in the Keyforce Master Subscription Agreement (“MSA”).

This Data Processing Agreement governs the Processor’s rights and obligations, in order to ensure that all Processing of Personal Data is conducted in compliance with applicable data protection legislation. Processing of Personal Data (as defined below) is subject to requirements and obligations pursuant to applicable law. When the Controller is a legal entity established in the European Economic Area (the "EEA") relevant data protection legislation will include local data protection legislation and the present EU- Regulation 2016/679 dated April 27th 2016. The parties agree to amend this Data Processing Agreement to the extent necessary due to any mandatory new requirements following from the EU Regulation 2016/679 and the revised Electronic Communications Regulation (“ePrivacy”) pursuant to its local implementation.

“Personal Data” shall mean any information relating to an identified or identifiable natural person, as further defined in applicable law and EU- Regulation 2016/679.

“Processing” of Personal Data shall mean any use, operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, transfer, storage, alteration, disclosure as further defined in applicable law and EU- Regulation 2016/679.

“Third Countries” shall mean countries outside of the EU/EEA area which are not recognized as countries providing adequate protection of Personal Data.

2. Controller’s responsibilities

In order to access the Service, the Controller must provide certain data to the Processor, including correct name, contact data and email address of the users. In addition, the users of the Service must allow the Processor to store and retrieve session information through the use of “cookies” which are necessary to enable the login/logout procedures used in the Service and to ensure that unauthorized persons do not gain access to the Services.

The Controller acknowledges and accepts that any Personal Data that the Controller uploads onto the Service, such as uploaded Personal Data pertaining to the Controller’s own customers, may be transferred to a third party (sub processor) based in the European Economic Area (EEA) which will provide for hosting of the Service, including the provisioning of all hardware, infrastructure, data storage and communication lines. The obligations of the third party in regard to Personal Data are set forth in a separate data processing agreement between Processor and the third party within the framework of this Data Processing Agreement. All data in the Service are stored on servers located in Europe.

The Controller confirms that the Controller:

- Has sufficient legal basis for Processing of Personal Data
- Has the right to use the Processor for Processing of the Personal Data Has the responsibility for the correctness, integrity, content, reliability and legality of the Personal Data
- Complies with applicable law on notification to and authorizations from relevant authorities
- Has informed the Data Subject in accordance with applicable law

The Controller shall

- Reply to requests from the Data Subjects regarding the Processing of Personal Data pursuant to this Data Processing Agreement
- Assess the necessity for specific measures as set forth in this Data Processing Agreement Art. 3.3.2 and 3.3.4, and order such measures from the Processor.

The Controller shall implement sufficient technical and organizational measures to ensure and demonstrate compliance with the EU Regulation 2016/679 from the time it enters into force.

The Controller has a duty to notify any personal data breaches to the relevant authorities and, if necessary, the Data Subjects without undue delay in accordance with applicable law.

3. Processor’s responsibilities

3.1 Compliance

The Processor shall comply with all provisions for the protection of Personal Data set out in this Data Processing Agreement and in applicable data protection legislation with relevance for Processing of Personal Data. The Processor shall provide the Controller with assistance to ensure and document that the Controller complies with its requirements under the applicable data protection legislation.

The Processor shall comply with the instructions and routines issued by the Controller in relation to the Processing of Personal Data.

3.2 Restrictions on use

The Processor shall only Process Personal Data on, and in accordance with, the instructions from the Controller. The Processor shall not Process Personal Data without prior written agreement with the Controller or without written instructions from the Controller beyond what is necessary to fulfil its obligations towards the Controller under the Agreement.

3.3 Information Security

3.3.1 Duty to ensure information security

The Processor shall by means of planned, systematic, organizational and technical measures ensure appropriate information security with regard to confidentiality, integrity and accessibility in connection with the Processing of Personal Data in accordance with the information security provisions in applicable data protection legislation.

The measures and documentation regarding internal control shall be made available to the Controller upon request.

3.3.2 Assessment of measures

In deciding which technical and organizational measures should be implemented, the Processor shall, in consultation with the Controller, take into account:

- The state of the art
- The costs of implementation
- The nature and scope of the processing
- The context and purpose of the processing,
- The severity of risks the Processing of Personal Data has for the rights and freedoms of the data subject

The Processor shall, in consultation with the Controller, consider:

- Implementing pseudonymising and encryption of Personal Data
- the ability to ensure the confidentiality, integrity, availability and resilience of processing systems and services on an ongoing basis

- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- a process for, on an ongoing basis, testing, assessing and evaluating regularly the effectiveness of technical and organizational measures for ensuring the security of the Processing

3.3.3 Requests from the data subjects

Considering the nature of the Processing, the Processors shall implement appropriate technical and organizational measures to support the Controller's obligation to respond to requests regarding exercising the rights of the data subject.

3.3.4 Assistance to the Controller

The Processor shall assist the Controller in ensuring compliance with applicable law, including assisting the Controller with:

- Implementing technical and organizational measures as stated above;

- Complying with duty of notification to supervisory authorities and data subjects in case of a personal data breach

- Conduct data privacy impact assessments

- Conduct prior consultations with supervisory authorities when a privacy impact assessment makes it it necessary

- Notice to the Controller if the Processor is of the opinion that an instruction from the Controller is non-compliant with applicable data protection regulations.

Assistance as set out above, shall be carried out to the extent necessary, taking into account the Controller’s need, the nature of the processing and the information available to the Processor.

3.3.5 Compensation

Assistance from the Processor as set down in this Data Processing Agreement, as well as assistance in relation to specific routines and instructions imposed by the Controller, shall be compensated by the Controller in accordance with the Processor’s regular terms and prices.

3.4 Discrepancies and data breach notifications

Any use of the information systems and the Personal Data not compliant with established routines, instructions from the Controller or applicable data protection legislation, as well as any security breaches, shall be treated as a discrepancy.

The Processor shall have in place routines and systematic processes to follow up discrepancies, which shall include re-establishing of the normal state of affairs, eliminating the cause of the discrepancy and preventing its recurrence.

The Processor shall immediately notify the Controller of any breach of this Data Processing Agreement or of accidental, unlawful or unauthorized access to, use or disclosure of Personal Data, or that the Personal Data may have been compromised or a breach of the integrity of the Personal Data. The Processor shall provide the Controller with all information necessary to enable the Controller to comply with applicable data protection legislation and enabling the Controller to answer any inquiries from the applicable data protection authorities. It is the Controller`s responsibility to notify the applicable Data Protection Authority of discrepancies in accordance with applicable law.

3.5 Confidentiality

The Processor shall keep confidential all Personal Data and other confidential information. The Processor shall ensure that each member of the staff of the Processor, whether employed or hired employee, having access to or being involved with the Processing of Personal Data under the MSA (i) undertakes a duty of confidentiality and (ii) is informed of and complies with the obligations of this Data Processing Agreement. The duty of confidentiality shall also apply after termination of the MSA or this Data Processing Agreement.

3.6 Security audits

The Processor shall on a regular basis carry out security audits for systems and similar relevant for the Processing of Personal Data covered by this Data Processing Agreement. Reports documenting the security audits shall be available to the Controller.

The Controller has the right to demand security audits performed by an independent third party at the Processors choice. The third party will provide a report to be delivered to the Controller upon request. The Controller accepts that the Processor may claim compensation for the performance of the audit.

3.7 Use of sub-contractors (sub-processors)

The Processor is entitled to use sub-contractors and the Controller accepts the use of sub-contractors. A list of pre-approved sub-processors is available in the Keyforce Trust Center. The Processor shall, by written agreement with any sub-contractor ensure that any Processing of Personal Data carried out by sub-contractors shall be subject to the same obligations and limitations as those imposed on the Processor according to this Data Processing Agreement.

If the Processor plans to change sub-contractors or plans to use a new sub-contractor, Processor shall notify the Controller in writing 4 months prior to any Processing by the new sub-contractor, and the Controller may within 1 month of the notice object to the change of sub-contractors. Should the Controller object to the change, Controller may terminate the MSA upon 3 months' notice. To the extent Controller does not terminate the MSA, the change of sub-contractor shall be regarded as accepted.

3.8 Transfer of Personal Data to Third Countries

If the Processor uses sub-contractors outside the EU/EEA area for Processing of Personal Data, such Processing must be in accordance with the EU Privacy Shield Framework, EU Standard Contractual Clauses for transfer to third countries, or another specifically stated lawful basis for the transfer of personal data to a third country. For the avoidance of doubt, the same applies if the data is stored in the EU/EEA but may be accessed from locations outside the EU/EEA.

Should the Controller approve such transfer of Personal Data, the Processor is obligated to cooperate with the Controller in order to ensure compliant transfers.

4. Liability, breach

In the event of breach of this Data Protection Agreement, or a breach of obligations according to applicable law on Processing of Personal Data, the relevant provisions regarding breach in the MSA shall apply.

Claims from one party due to the other party’s non-compliance with the Data Processing Agreement shall be subject to the same limitations as in the MSA. In assessing whether the limitation in the MSA is reached, claims under this Data Processing Agreement and the MSA shall be viewed in conjunction, and the limitation in the MSA shall be viewed as a total limitation.

The Processor shall notify the Controller without undue delay if it will or has reason to believe it will be unable to comply with any of its obligations under this Data Protection Agreement.

5. Term and termination of the Data Processing Agreement, changes

This Data Processing Agreement shall be effective from the date it is signed by both parties and until the Processor's obligations in relation to the performance of services in accordance with the MSA is terminated, except for those provisions in the MSA and Data Processing Agreement that continues to apply after such termination.

Upon termination of this Data Processing Agreement the Personal Data/data shall be returned in a standardized format and medium along with necessary instructions to facilitate the Controller’s further use of the Personal Data/data. The Processor shall first return and subsequently delete all Personal Data and other data. The Processor (and its sub-contractors) shall immediately stop the Processing of Personal Data from the date stipulated by the Controller

As an alternative to returning the Personal Data (or other data), the Controller may, at its sole discretion, instruct the Processor in writing, that all or parts of the Personal Data (or other data) shall be deleted by the Processor, unless the Processor is prevented by mandatory law from deleting the Personal Data.

The Processor has no right to keep a copy of any data provided by the Controller in relation to the MSA or this Data Protection Agreement in any format, and all physical and logical access to such Personal Data or other data shall be deleted.

The Processor shall provide the Controller with a written declaration whereby the Processor warrants that all Personal Data or other data mentioned above has been returned or deleted according to the Controller's instructions and that the Processor has not kept any copy, print out or kept the data on any medium.

The obligations pursuant to sections 3.5 and 4 shall continue to apply after termination. Further, the provisions of the Data Processing Agreement shall apply in full to any Personal Data retained by the Processor in violation of this section 5.

The parties shall amend this Data Protection Agreement upon relevant changes in applicable law.

6. Dispute and jurisdiction

This Data Processing Agreement shall be governed by the laws according to the Keyforce entity the Customer is contracting with:

Norway

Keyforce Norge AS

Karenslyst Allè, 0277 Oslo

Finland and Sweden

Keyforce Sverige AB

Lindhagensgatan 94, 112 18 Stockholm

Denmark

Keyforce Danmark Aps

Hovedvejen 31, 2600 Glostrup