Kabal

Data Processing Agreement

Kabal

1. BACKGROUND AND SCOPE

This Data Processing Agreement is entered into between Kabal AS (the “Processor”) and the customer (the “Controller”) that has entered into an agreement with the Processor for the provision of Kabal`s software solutions (the “Main Agreement”). The Processor and the Controller are each a “Party” and together the “Parties”.

The purpose of this Data Processing Agreement is to ensure that the Processor's Processing of Personal Data on behalf of the Controller in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (the "**GDPR**") and the applicable Norwegian law implementing the GDPR (hereinafter jointly referred to as "**Applicable Data Protection Law**").

This Data Processing Agreement fulfils the requirements for a data processing agreement in accordance with Applicable Data Protection Law. This Data Processing Agreement shall govern the Processor's rights and obligations with regard to all Processing of Personal Data on behalf of the Controller under the Main Agreement in order to ensure that all Processing of Personal Data is conducted in compliance with Applicable Data Protection Law.

This Data Processing Agreement does not include processing of genetic data or biometric data but *may* include health data such as weight for offshore booking purposes (if so, this will be addressed in the relevant Annex or Annexes, ref. Clause 3 below).

2. DEFINITIONS

For the purposes of this Data Processing Agreement, "**Controller**", "**Data Subject**", "**Processor**", "**Process/Processing/Processed**", "**Personal Data**", "**Personal Data Breach**" and "**Supervisory Authority**" shall have the meanings provided in Applicable Data Protection Law. Where the term “**Data”** is used in relation to portability, return, and deletion upon termination, it shall be understood to include both Personal Data as defined by GDPR and non-personal data as specified in the Data Portability Policy.
“EEA” means the European Economic Area.
“Third Country” means a country outside the EEA that is not subject to a valid adequacy decision of the European Commission under Applicable Data Protection Law.
“Standard Contractual Clauses” means the standard contractual clauses for the transfer of personal data to third countries approved by the European Commission in Implementing Decision (EU) 2021/914 of 4 June 2021, comprising the Processor-to-Controller Clauses and the Processor-to-Processor Clauses, as applicable.
“Processor-to-Controller Clauses” means Module Four (processor to controller) of the Standard Contractual Clauses. Subject to Clause 4.7, the Processor and the Controller agree that Module Four shall apply, to a transfer of Personal Data to, or access to Personal Data from a Third Country by or on behalf of the Controller, to the extent required under Applicable Data Protection Law.
“Processor-to-Processor Clauses” means Module Three (processor to processor) of the Standard Contractual Clauses, which the Processor and any Sub-processor shall enter into where required under this Data Processing Agreement.

3. DESCRIPTION OF THE PROCESSING

This Data Processing Agreement shall apply to all Processing of Personal Data carried out by the Processor on behalf of the Controller under the Main Agreement. In the event of conflict between the Main Agreement and this Data Processing Agreement concerning the subject matter explicitly regulated herein, this Data Processing Agreement shall prevail. Nothing in this Data Processing Agreement varies or modifies the Processor-to-Controller Clauses or the Processor-to-Processor Clauses, and in the event of any conflict between this Data Processing Agreement and either set of clauses, the relevant Standard Contractual Clauses shall prevail.

The Processor shall only Process the categories of Personal Data and the categories of Data Subjects for the purposes set out in the applicable Annex or Annexes, unless otherwise instructed by the Controller.

4. THE PROCESSOR’S GENERAL OBLIGATIONS

4.1 Compliance

The Processor's Processing of Personal Data as Processor for the Controller in order to fulfil the Main Agreement shall be carried out in accordance with all relevant provisions set out in the Main Agreement and Applicable Data Protection Law. The Processor shall not by actions or omission of actions put the Controller in a situation where the Controller is in breach of any provision of Applicable Data Protection Law.

The Processor shall provide the Controller with reasonable cooperation and assistance to ensure that the Controller complies with its requirements under Applicable Data Protection Law.

Taking into account the nature of the Processing, and insofar as this is possible, the Processor shall, on the Controller`s documented instructions, promptly assist the Controller with the handling of any requests from data subjects, including any rights of access, rectification, restriction, erasure, data portability and objection, to the extent such rights apply under the Applicable Data Protection Law.. Such assistance shall be provided without undue delay and in sufficient time to enable the Controller to meet the response deadline applicable to it under Applicable Data Protection Law. The Controller remains responsible for assessing and verifying each request and for responding to the Data Subject. The Processor may charge a reasonable fee for or decline to provide assistance in respect of requests that are manifestly unfounded, excessive or repetitive, or that require effort materially beyond routine handling.
The Controller has the right to access any information the Processor holds on behalf of the Controller and shall be admitted access to the systems used by the Processor for this purpose, unless otherwise is agreed or follows from mandatory law.

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

4.2 Restrictions on use

The Processor shall only Process Personal Data on the instructions from the Controller and strictly in accordance with such instructions. The Processor shall not under any circumstances Process Personal Data beyond what is necessary to fulfil its obligations towards the Controller under the Main Agreement unless by prior written agreement with the Controller or subject to written instructions from the Controller. The Controller's written request for access to Personal Data through the Processor's Application Programming Interface ("API"), as approved by the Processor in accordance with the Processor's API Terms of Service, constitutes the Controller's documented instructions to make such Personal Data available through API.

4.3 Information Security

The Processor shall by means of planned, systematic organisational and technical measures ensure information security appropriate to the risk with regard to confidentiality, integrity and accessibility in connection with the Processing of Personal Data in accordance with Applicable Data Protection Law, including as appropriate:

i. Security organization with clear responsibilities;

ii. Information security policy and privacy policy;

iii. Access control to systems and data. Both authorized use and attempts on unauthorized use of systems shall be registered. Documentation shall be kept for at least three months;

iv. Access control to buildings and equipment used for Processing of Personal Data;

v. Virus protection, spam-filters and firewalls as appropriate;

vi. Logging of all critical system operations;

vii. Security breach processes and monitoring. Security breaches shall be documented, and documentation shall be kept for at least three months;

viii. Backup/restore process for all critical systems and restore-tests;

ix. Training and education in information and personal data security;

x. Encryption of communication if appropriate. Sensitive data shall always be encrypted;

xi. Policies for deletion or anonymization of Personal data when there is no longer a need for keeping them with a view to the processing purposes set out in this Data Processing Agreement and/or the Main Agreement;

xii. Supplier management with requirements regarding information security.

The Processor shall implement measures ensuring, by default, that Personal Data are not made accessible to an indefinite number of natural persons without the individual's consent/intervention.

The Processor shall upon request provide the Controller with sufficient documentation to enable the Controller to demonstrate that the appropriate technical and organizational security measures have been implemented and that the Processor is acting in compliance with this Data Processing Agreement and Applicable Data Protection Law.

Records of authorised use of the information system and of attempts at unauthorised use shall, for the purpose of ensuring a sufficient level of information security and in order to enable investigation of a possible personal data breach, be stored for at least 3 months. The same applies to records of all other events of significance for data security.

4.4 Notifications – Data breach

The Processor must without undue delay after becoming aware of the facts in writing notify the Controller about:

(i) any Personal Data Breach, providing the information required under Applicable Data Protection Law to the extent available
(ii) any suspicion that the instructions from the Controller are in violation of Applicable Data Protection Law;
(iii) any request for disclosure of Personal Data Processed under the Data Processing Agreement by authorities, unless expressly prohibited under mandatory law;
(iv) any request for access to the Personal Data received from third parties;
(v) whether it is or is likely to become unable to comply with any of its obligations under this Data Processing Agreement.

The Processor shall provide the Controller with all information necessary to answer any inquiries from the data protection authorities and to comply with the applicable personal data breach notification requirements to the data protection authority and Data Subjects.

4.5 Confidentiality

The Processor shall keep confidential all Personal Data and other confidential information. The Processor shall further ensure that each member of the staff of the Processor, whether employed or for hire, having access to or being involved in the Processing of Personal Data under the Main Agreement (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 this Data Processing Agreement.

4.6 Security audits

Subject to reasonable prior written notice, audits and inspections of the Processor`s organisation, data processing facilities, relevant security measures, use of subcontractors and other aspects relevant to the current processing under this Data Processing Agreement, but not more than once annually, may be subject to audits and inspections by the Controller or a third party on behalf of the Controller, to verify Processor`s compliance with the Main Agreement, this Data Processing Agreement and Applicable Data Protection Law. Any audit shall be limited to documentation review and shall not include access to the Processor`s production systems, source code, other customers`information or security-sensitive technical information.

4.7 Transfer of Personal Data

The Processor shall not transfer Personal Data outside the EEA or give anyone outside the EEA access to Personal Data, (including by remote or API access) without the Controller's prior written consent. For the avoidance of doubt, the transfers of Personal Data set out in the Annex or Annexes to this Data Processing Agreement, are regarded as pre-approved by the Controller.

Where the Controller has given its written consent under this Clause to a transfer of Personal Data to, or access to Personal Data from, a Third Country, the Processor-to-Controller Clauses shall automatically apply where required under Applicable Data Protection Law and are incorporated by reference into this Data Processing Agreement. The information required in the relevant annexes to the Processor-to-Controller Clauses is set out in this Data Processing Agreement, the Main Agreement, the applicable Annex or Annexes, and the Controller's contractual details.

4.8 Use of subcontractors

To the extent the Processor wishes to use subcontractors to fulfil the obligations under the Main Agreement, the Processor shall ensure that the subcontractor undertakes responsibilities corresponding to the obligations set out in this Data Processing Agreement.

Such subcontractors shall be subject to approval by the Controller prior to Processing any Personal Data under this Data Processing Agreement. The Processor shall maintain a list of all subcontractors which shall be available for the Controller upon request.

The Processor shall bear the responsibilities for the subcontractor's acts and omissions as if they were the Processor's own.

In a situation where the Processor has received the Controller's approval to use a subcontractor established outside the EEA, the Processor shall take measures to ensure an adequate level of protection for the Personal Data in accordance with Applicable Data Protection Law. Such measures shall include the Processor, and/or any subcontractor, entering into the Processor-to-Processor Clauses, which are hereby incorporated by reference into this Data Processing Agreement and are deemed to complete the corresponding Appendix.

4.9 Liability

The Processor's accumulated liability based on or related to this Data Processing Agreement, whether in contract, tort or otherwise, shall be subject to the limitation of liability as set out in the Main Agreement.

5. OBLIGATIONS OF THE CONTROLLER

The Controller is responsible for ensuring there is a legal basis for the Processing of Personal Data carried out by the Processor on behalf of the Controller under the Main Agreement and according to this Data Processing Agreement. Specifically, the Controller is responsible for ensuring such legal basis for Personal Data uploaded to the Processor's SaaS system by Controller's contractors / suppliers and processed by the Processor under the Main Agreement.

6. TERM AND TERMINATION OF THE DATA PROCESSING AGREEMENT

This Data Processing Agreement shall be effective from the date it becomes binding on the Controller as part of the Main Agreement and shall remain in force until the Main Agreement expires or the Processor's obligations in relation to the performance of the services under the Main Agreement are otherwise terminated, except for those provisions in the Main Agreement and this Data Processing Agreement that continue to apply after such termination.

Upon termination of this Data Processing Agreement, the Processor shall cease the Processing of Personal Data on behalf of the Controller. and, at the Controller`s choice, return or delete all Personal Data Processed on behalf of the Controller, unless Applicable Data Protection Law requires continued storage. The Processor may charge its reasonable cost for any return of Personal Data.

Upon request, the Processor shall no later than three months after termination of this Data Processing Agreement, issue a written confirmation to the Controller, stating that Personal Data has been returned or deleted in accordance with this Clause 6.

Where the Controller terminates the Main Agreement for the purpose of switching to another provider, the return and deletion of Personal Data shall take place in accordance with switching and data portability provisions of the Main Agreement, which shall prevail over this clause 6 to that extent.

7. AMENDMENTS

The Processor may amend this Data Processing Agreement from time to time by giving the Controller at least thirty (30) days prior written notice. An amendment required to comply with Applicable Data Protection Law may take effect on shorter notice where reasonably necessary. No amendment shall materially reduce the overall security of the Processing or cause the Processing of Personal Data to be inconsistent with Applicable Data Protection Law.

8. DISPUTE AND GOVERNING LAW

This Data Processing Agreement is governed by the law, and disputes shall be resolved in accordance with the manner and venue agreed in the Main Agreement.