

1. Preamble

- 1.1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.
- 1.2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of 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 (General Data Protection Regulation).
- 1.3. In the context of the provision of ERP software and/or Cloud hosting services and related consultancy and development services under the Agreement, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.
- 1.4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.
- 1.5. Four appendices are attached to the Clauses and form an integral part of the Clauses.
- 1.6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.
- 1.7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorized by the data controller.
- 1.8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum-security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.
- 1.9. Appendix D contains provisions for other activities which are not covered by the Clauses.
- 1.10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.
- 1.11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

2. The rights and obligations of the Data Controller

- 2.1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.
- 2.2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
- 2.3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3. The Data Processor acts according to instructions

- 3.1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data 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 Clauses.
- 3.2. The data 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. In such case, the data processor is not obligated to adhere to the instructions, which in the opinion of the data processor contravene the GDPR, and the data controller must take necessary steps to ensure that the instruction is adjusted so as to ensure compliance.

4. Confidentiality

- 4.1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.
- 4.2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

5. Security of processing

- 5.1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

- i) Pseudonymization and encryption of personal data;
 - ii) the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- 5.2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.
 - 5.3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organizational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

6. Use of Sub-Processors

- 6.1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).
- 6.2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorization of the data controller.
- 6.3. The data processor has the data controller's general authorization for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 2 weeks in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorized by the data controller can be found in Appendix B.

- 6.4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.
- 6.5. The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.
- 6.6. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller’s request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.
- 6.7. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.
- 6.8. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

7. Transfer of data to third countries or international organizations

- 7.1. Any transfer of personal data to third countries or international organization by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.
- 7.2. In case transfers to third countries or international organization, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.
- 7.3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:
 - i) transfer personal data to a data controller or a data processor in a third country or in an international organization
 - ii) transfer the processing of personal data to a sub-processor in a third country
 - iii) have the personal data processed in by the data processor in a third country
 - iv) The data controller’s instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.
 - v) The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

8. Assistance to the Data Controller

- 8.1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organizational measures, insofar as this is possible, in the fulfilment of the data controller’s obligations to respond to requests for exercising the data subject’s rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller’s compliance with:

- i) the right to be informed when collecting personal data from the data subject
- ii) the right to be informed when personal data have not been obtained from the data subject
- iii) the right of access by the data subject
- iv) the right to rectification
- v) the right to erasure ('the right to be forgotten')
- vi) the right to restriction of processing

- vii) notification obligation regarding rectification or erasure of personal data or restriction of processing
- viii) the right to data portability
- ix) the right to object
- x) the right not to be subject to a decision based solely on automated processing, including profiling

8.2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

- i) The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, the Danish Data Protection Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
- ii) the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
- iii) the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
- iv) the data controller's obligation to consult the competent supervisory authority, the Danish Data Protection Agency, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

8.3. The parties shall define in Appendix C the appropriate technical and organizational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

9. Notification of personal data breach

9.1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

9.2. The data processor's notification to the data controller shall, if possible, take place without undue delay after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

9.3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

- i) The nature of the personal data including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- ii) the likely consequences of the personal data breach;
- iii) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

10. Erasure and return of data

10.1. On termination of the provision of personal data processing services, the data processor shall be under obligation at the data controller's choice to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so, or to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

11. Audit and inspection

- 11.1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.
- 11.2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.
- 11.3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

12. The Parties' agreement on other terms

- 12.1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

13. Commencement and termination

- 13.1. The Clauses shall become effective on the date of both parties' signature.
- 13.2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.
- 13.3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.
- 13.4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

13.5. Signature

On behalf of the data controller:

Please refer to the signature page of the Agreement.

On behalf of the data processor:

Please refer to the signature page of the Agreement.

14. Data Controller and Data Processor contacts/contact points

- 14.1. The parties may contact each other using the contacts/contact points set out in the Agreement.
- 14.2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

APPENDIX A: INFORMATION ABOUT THE PROCESSING**A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:**

The data processor processes personal data on behalf of the data controller for the purpose of providing ERP software and/or Cloud hosting services and related consultancy and development services, in accordance with the Agreement.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Consultancy and development (including support services)

The data processor will advise about the use and configuration of ERP software and/or Cloud hosting services and develop customized solutions for ERP software and/or Cloud hosting services which are customized to the data controller's specific needs. The advice/support will involve processing of personal data on end users of the ERP software and/or Cloud hosting services and other software.

Additionally, the data processor will develop standard add-ons for ERP software and/or Cloud hosting services and make these available to the data controller.

A.3. The processing includes the following types of personal data about data sub-jects:

The processing will comprise name, contact details (work address, e-mail, phone number and fax number) and title/association with a specific company.

A.4. Processing includes the following categories of data subject:

The processing will comprise personal data regarding the end users of ERP software and/or Cloud hosting services and other software.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The data processor will process personal data on behalf of the data controller for the duration of the Agreement.

APPENDIX B: AUTHORIZED SUB-PROCESSORS**B.1. Approved sub-processors**

On commencement of the Clauses, the data controller authorizes the engagement of the below-mentioned sub-processors (as applicable under the Agreement).

See <https://www.boyum-solutions.com/boyum-group-and-subcontractors/> containing name, address and description of processing activities related to each authorized sub-processor.

The data controller shall on the commencement of the Clauses authorize the use of the mentioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorization – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

APPENDIX C: INSTRUCTION PERTAINING TO THE USE OF PERSONAL DATA**C.1. The subject of/instruction for the processing**

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

Consultancy services, including operational and technical customer support related to ERP software and/or Cloud hosting services and other software which may be comprised by the Agreement.

C.2. Security of processing

The data processor shall – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

- i) Application of policies concerning complexity and durations of passwords used for accessing the data processor's systems
- ii) Restricting access to office facilities via use of a personal key (authorization scheme)
- iii) Activating electronic alarms outside regular office hours
- iv) Restricting access to core systems to a limited number of employees
- v) Centralizing the installation, management and updating of antivirus software on all systems
- vi) Updating systems software (OS) on a regular basis
- vii) Use of administered firewalls on all our locations
- viii) Use of automatic screen lock on all our IT-systems
- ix) Provision of remote access via encrypted Citrix or VPN-systems
- x) Implementation of network separation using site-to-site VPN and VLAN separation
- xi) Maintenance of back-ups on separate locations
- xii) Implementation of redundancy via virtual server environments
- xiii) Storage of data in a data center which has video surveillance, access control with logging of access, water and moist sensor, fire and smoke detection, fire-fighting equipment, cooling facility, redundancy power supply including UPS, generator and redundant internet connections.
- xiv) The data processor will on a regular basis conduct attention training in relation to IT security and processing of personal data. The data processor will also implement segregation of duties in relation to access control and rights management.

The data processor will evaluate the technical security on an ongoing basis with a view to make upgrades if new technology can make the systems more secure at a cost which the data processor considers reasonable, compared to the need for security.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organizational measures:

The data processor will pass on any requests received from data subjects to the data controller and assist the data controller in replying to such requests (if the request should be accommodated).

With regard to personal data breaches, the data processor will in continuation of informing the data controller of the breach, also provide information and answers to follow-up questions in order for the data controller to comply with the applicable requirements regarding notification of personal data breaches.

C.4. Storage period/erasure procedures

The data processor will only have access to personal data as part of provision of specific support services, and the personal data will only be stored for the duration of the specific support tasks.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

The data controller accepts that the data processor may anonymize personal data as an appropriate alternative to erasing them, in all circumstances where the data processor under these Clauses is instructed or obligated to erase personal data. The data processor may anonymize the personal data for statistical purposes. The anonymization must ensure that the data processor is not able to re-create the link between the anonymized information and the person in question.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorization:

- i) The data processor's location as specified in the Agreement; and
- ii) The sub-processors' locations as specified in Appendix B.1

C.6. Instruction on the transfer of personal data to third countries

The data processor may transfer personal data to countries outside the EU/EEA.

The data processor has the data controller's authorization, on behalf of the data controller, to enter into Standard Contractual Clauses (based on the Commission decision 2010/87/EU) for the purpose of ensuring a legal basis for the transfer of personal data to recipients located outside the EU/EEA.

Warranty

Where the data controller acts in a capacity as data processor on behalf of its customer (and the data processor therefore de facto is a sub-processor), the data controller warrants and represents that the data controller has obtained from its customers a written authorization to

- i) enter into Standard Contractual Clauses as set out in this Appendix C.6 on behalf of the customers; and
- ii) assign this authorization to its sub-processor(s).

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall – at a maximum – one time each year at the data controller's request and expense obtain an auditor's report from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The auditor's report shall without undue delay be submitted to the data controller for information.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required and must be notified in writing 60 days in advance to the data processor.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor shall – at a maximum – one time each year at the data controller's request and expense obtain an auditor's from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The auditor's report shall without undue delay be submitted to the data controller for information.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

APPENDIX D: THE PARTIES' TERMS OF AGREEMENT ON OTHER SUBJECTS

The parties agree that if the data controller acts in a capacity as data processor with regard to the services under the Agreement and/or the Clauses, the Clauses will apply mutatis mutandis (i.e. the Supplier is considered sub-processor and the Clauses constitutes a sub-processor agreement).

The data processor is entitled to remuneration for consumed time and incurred costs to the extent that they can be attributed to accommodating the data controller's specific needs. This may include, without limitation:

- i) provision of assistance in accordance with Clause 9;
- ii) adjustment or implementation of security measures to accommodate the specific needs of the data controller; and
- iii) participation in audits and/or inspections as set out in Clause 12 and Appendix C.7 and C.8.