DATA PROCESSING AGREEMENT

Standard contractual clauses

pursuant to Article 28(3) of Regulation 2016/679 (General Data Protection Regulation) for the purpose of the processor's processing of personal data

Between

Data Controller:

hereinafter "the controller"

and

The data manager:
BORG IT ApS
Borggade 22
6300 Gråsten, Denmark
CVR: DK28698623
Contact: Lauge Borg
borgit@borgit.com

hereinafter the "data processor"

each of which is a "party" and together constitute the "parties"

HAVE AGREED the following standard contractual clauses (the Clauses) in order to comply with the GDPR and ensure the protection of the privacy and fundamental rights and freedoms of natural persons

1. Content

2. Preamble

1. These Clauses set out the rights and obligations of the processor when processing personal data on behalf of the controller.

2. These provisions are designed to ensure the parties' compliance with Article 28(3) of Regulation (EU) 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).

3. In connection with the delivery from BORG IT, the data processor processes personal data on behalf of the data controller in accordance with these Terms and Conditions.

4. The provisions take precedence over any corresponding provisions in other agreements between the parties.

5. There are four annexes to these Regulations and the annexes form an integral part of the Regulations.

6. Annex A contains details of the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of data subjects and the duration of the processing.

7. Appendix B contains the controller's conditions for the processor's use of sub-processors and a list of sub-processors authorised by the controller.

8. Appendix C contains the data controller's instructions regarding the data processor's processing of personal data, a description of the minimum security measures that the data processor must implement and how the data processor and any sub-processors are supervised.

9. Annex D contains provisions regarding other activities not covered by the Clauses.

10. The provisions and their appendices shall be kept in writing, including electronically, by both parties.

11. These Clauses do not release the data processor from obligations imposed on the data processor under the General Data Protection Regulation or any other legislation.

3. Rights and obligations of the controller

1. The controller is responsible for ensuring that the processing of personal data is carried out in accordance with the General Data Protection Regulation (see Article 24 of the Regulation), data protection provisions of other EU law or Member[1] national law and these Regulations.

2. The controller has the right and obligation to decide for which purpose(s) and with which means personal data may be processed.

1 References to "Member State" in these provisions shall be construed as references to "EEA Member States".

3. The controller is responsible for, among other things, ensuring that there is a legal basis for the processing of personal data that the data processor is instructed to perform.

4. The data processor acts on instructions

1. The data processor may only process personal data following documented instructions from the data controller, unless required by EU or Member State law to which the data processor is subject. These instructions shall be specified in Annexes A and C. Subsequent instructions may also be given by the controller while personal data is being processed, but the instructions must always be documented and stored in writing, including electronically, together with these Clauses.

2. The processor shall inform the controller without delay if, in its opinion, an instruction infringes this Regulation or data protection provisions of other Union or Member State law.

5. Confidentiality

1. The data processor may only grant access to personal data processed on behalf of the data controller to persons who are subject to the data processor's instructions, who have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality, and only to the extent necessary. The list of persons who have been granted access shall be reviewed on an ongoing basis. Based on this review, if access to personal data is no longer necessary, access to the personal data may be closed and the personal data shall no longer be accessible to these individuals.

2. At the request of the controller, the data processor must be able to demonstrate that the persons in question, who are subject to the data processor's powers of instruction, are subject to the aforementioned duty of confidentiality.

6. Treatment safety

1. Article 32 GDPR states that the controller and processor shall implement appropriate technical and organisational measures to ensure a level of protection appropriate to the risks, 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 risks of varying likelihood and severity for the rights and freedoms of natural persons.

   The controller must assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to address those risks. Depending on their relevance, this may include:

   a. Pseudonymisation and encryption of personal data

   b. Ability to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services

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

d. a procedure for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures to ensure the security of processing.

2. According to Article 32 of the Regulation, the processor must - independently of the controller - also assess the risks to the rights of natural persons posed by the processing and implement measures to mitigate those risks. For the purposes of this assessment, the controller must provide the processor with the necessary information to enable it to identify and assess such risks.

3. In addition, the processor shall assist the controller in its compliance with the controller's obligation under Article 32 of the Regulation by, inter alia, providing the controller with the necessary information regarding the technical and organisational security measures already implemented by the processor pursuant to Article 32 of the Regulation and any other information necessary for the controller to comply with its obligation under Article 32 of the Regulation.

   If addressing the identified risks - in the controller's judgement - requires the implementation of additional measures beyond the measures already implemented by the processor, the controller shall specify the additional measures to be implemented in Annex C.

7. Use of sub-processors

1. The data processor must fulfil the conditions referred to in Article 28(2) and (4) of the GDPR to use another data processor (a sub-processor).

2. The Data Processor may thus not use a sub-processor to fulfil these Clauses without prior general written approval from the Data Controller.

3. The Data Processor has the Data Controller's general authorisation for the use of sub-processors. The Data Processor shall notify the Data Controller in writing of any planned changes regarding the addition or replacement of sub-processors with at least one month's notice, thereby giving the Data Controller the opportunity to object to such changes prior to the use of the sub-processor(s) in question. Longer notice periods for notification for specific processing operations may be specified in Annex B. The list of sub-processors already authorised by the controller is set out in Annex B.

4. Where the processor uses a sub-processor to carry out specific processing activities on behalf of the controller, the processor shall, by contract or other legal act under Union or Member State law, impose on the sub-processor the same data protection obligations as those set out in these Clauses, in particular providing appropriate guarantees that the sub-processor will implement the technical and organisational measures in such a manner that the processing will comply with the requirements of these Clauses and the GDPR.

   The Data Processor is therefore responsible for requiring the Sub-Processor to, as a minimum, comply with the Data Processor's obligations under these Clauses and the General Data Protection Regulation.

5. The sub-processor agreement(s) and any subsequent amendments thereto shall - at the request of the data controller - be sent a copy to the data controller, which thereby

has the opportunity to ensure that similar data protection obligations arising from these Clauses are imposed on the sub-processor. Provisions on commercial terms that do not affect the data protection law content of the sub-processor agreement shall not be sent to the data controller.

6. In its agreement with the sub-processor, the processor must include the controller as a third party beneficiary in the event of the processor's bankruptcy so that the controller can subrogate itself to the rights of the processor and enforce them against sub-processors, for example, enabling the controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil its data protection obligations, the processor remains fully liable to the controller for the fulfilment of the sub-processor's obligations. This shall be without prejudice to the rights of data subjects resulting from the GDPR, in particular Articles 79 and 82 thereof, vis-à-vis the controller and the processor, including the sub-processor.

8. Transfer to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations may only be made by the data processor on the basis of documented instructions from the data controller and must always be in accordance with Chapter V of the GDPR.

2. Where the transfer of personal data to third countries or international organisations which the processor has not been instructed to carry out by the controller is required by Union or Member State law to which the processor is subject, the processor shall inform the controller of that legal requirement prior to processing, unless that law prohibits such notification for reasons of important public interest.

3. Without documented instructions from the controller, the data processor may not, within the framework of these Clauses:

    a. transfer personal data to a controller or processor in a third country or an international organisation
    b. entrust the processing of personal data to a sub-processor in a third country
    c. process the personal data in a third country

4. The controller's instructions regarding the transfer of personal data to a third country, including any transfer basis in Chapter V of the GDPR on which the transfer is based, shall be specified in Annex C.6.

5. These Clauses shall not be confused with standard contractual clauses within the meaning of Article 46(2)(c) and (d) of the GDPR and these Clauses cannot constitute a basis for the transfer of personal data within the meaning of Chapter V of the GDPR.

9. Assistance to the controller

1. The processor shall, taking into account the nature of the processing, assist the controller as far as possible by appropriate technical and organisational measures to fulfil the controller's obligation to respond to requests for the exercise of data subjects' rights as laid down in Chapter III of the GDPR.

This means that the data processor must, as far as possible, assist the data controller in connection with the data controller ensuring compliance with:

a. the information obligation when collecting personal data from the data subject
b. the information obligation if personal data has not been collected from the data subject
c. the right of access
d. the right to rectification
e. the right to erasure ("right to be forgotten")
f. the right to restriction of processing
g. the duty to inform in connection with rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3, the data processor shall, taking into account the nature of the processing and the information available to the data processor, further assist the data controller with

   a. the obligation of the controller to report a personal data breach to the competent supervisory authority, the Danish Data Protection Agency, without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

   b. the controller's obligation to notify the data subject without undue delay of a personal data breach where the breach is likely to result in a high risk to the rights and freedoms of natural persons

   c. the obligation for the controller to analyse the impact of the intended processing operations on the protection of personal data prior to processing (a data protection impact assessment)

   d. the controller's obligation to consult the competent supervisory authority, the Danish Data Protection Agency, prior to processing if a data protection impact assessment shows that the processing would result in high risk in the absence of measures taken by the controller to mitigate the risk.

3. The parties shall specify in Annex C the necessary technical and organisational measures with which the data processor shall assist the data controller and to what extent and scope. This applies to the obligations arising from Clauses 9.1 and 9.2.

10. Personal data breach notification

1. The Processor shall notify the Controller without undue delay after becoming aware that a personal data breach has occurred.

2. The data processor's notification to the data controller must, if possible, take place within 24 hours of becoming aware of the breach so that the data controller can fulfil

its obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 of the General Data Protection Regulation.

3. In accordance with Clause 9.2.a, the processor shall assist the controller in making the breach notification to the competent supervisory authority. This means that the processor shall assist in providing the following information, which, according to Article 33(3), shall be included in the controller's notification of the breach to the competent supervisory authority:

    a. the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected and the categories and approximate number of personal data records affected

    b. the likely consequences of the personal data breach

    c. the measures that the controller has taken or proposes to take to address the personal data breach, including, where applicable, measures to mitigate its possible adverse effects.

4. The parties shall specify in Annex C the information to be provided by the processor in the context of its assistance to the controller in its obligation to notify personal data breaches to the competent supervisory authority.

11. Deletion and return of information

1. Upon termination of the personal data processing services, the processor shall be obliged to erase all personal data processed on behalf of the controller and confirm to the controller that the data have been erased, unless Union or Member State law provides for the retention of the personal data.

   The data processor undertakes to process the personal data only for the purpose(s), for the period and under the conditions prescribed by these rules.

12. Audit, including inspection

1. The Processor shall provide the Controller with all information necessary to demonstrate compliance with Article 28 of the GDPR and these Clauses and shall enable and contribute to audits, including inspections by the Controller or another auditor authorised by the Controller.

2. The procedures for the controller's audits, including inspections, with the data processor and sub-processors are detailed in Appendices C.7 and C.8.

3. The data processor is obliged to grant supervisory authorities that have access to the data controller's or data processor's facilities under applicable legislation, or representatives acting on behalf of the supervisory authority, access to the data processor's physical facilities against proper identification.

13. The parties' agreement on other matters

1. The parties may agree other provisions relating to the service concerning the processing of personal data, such as liability for damages, as long as these other provisions do not directly or indirectly conflict with the Clauses or impair the data subject's fundamental rights and freedoms under the GDPR.

14. Entry into force and termination

1. The provisions shall enter into force on the date of signature by both parties hereto.

2. Either party may demand renegotiation of the Clauses if changes in legislation or inappropriateness in the Clauses give rise to this.

3. The Terms are valid for the duration of the personal data processing service. During this period, the Clauses cannot be terminated unless other provisions governing the provision of the personal data processing service are agreed between the parties.

4. If the provision of the Personal Data Processing Services ceases and the personal data has been deleted or returned to the Controller in accordance with Clause 11.1 and Appendix C.4, the Clauses may be terminated with written notice by either party.

5. Your signature
   On behalf of the data controller

   Name
   Position
   Phone number
   E-mail
   Your signature

   On behalf of the data processor

Name	Lauge Borg
Position	CTO
Phone number	3033 3966
E-mail	lauge.borg@borgit.com
Your signature	

15. Contact persons at the data controller and data processor

1. The parties can contact each other via the contact persons below.

2. The parties are obliged to keep each other informed of changes regarding contact persons.

   Name
   Position
   Phone number
   E-mail
   Your signature

Name	Lauge Borg

Position	CTO
Phone number	3033 3966
E-mail	lauge.borg@borgit.com

Annex A Information about the processing

A.1 Purpose of the processor's processing of personal data on behalf of the controller

The processor processes personal data to enable the controller to use the software as described in the contract. In addition, the processing may be carried out to
other purposes in accordance with any written instructions from the controller.

A.2 Processing of personal data by the Processor on behalf of the Controller primarily concerns (the nature of the processing)

The processing of personal data primarily concerns the management of IT systems for handling the controller's SAP services and SAP products.

The data processor's processing of personal data on behalf of the data controller concerns SAP consulting and products, including but not limited to:

- Provide support and consultancy services from BORG IT's consultants when the Customer needs help
- Provide help with the start-up and creation of the Customer and Employees
- Operation, testing, maintenance, development and troubleshooting of systems and applications within BORG IT and SAP software

A.3. The processing includes the following types of personal data of the data subjects

Types of personal data subject to processing under the agreement:

- Contact details, such as name, address, email, phone
- Personal data to be used to calculate social and governance ESG metrics, including, but not limited to:
    - Sick leave,
    - employee satisfaction,
    - Working hours,
    - gender,
    - Salary,
    - seniority,
    - job title.

A.4. Processing includes the following categories of data subjects

Categories of data subjects included in the processing:

- End users of the controller (Customer)
- The controller's (Customer's) employees
- Contact persons of the data controller (Customer)
- The controller's (Customer's) customers

A.5 The data processor's processing of personal data on behalf of the data controller may commence after the entry into force of these Clauses. The duration of the processing is as follows

The processing of personal data shall be carried out until the services of the data processor are
has ceased, after which the personal data is either returned or deleted in accordance with section 11. The Data Processor's processing of personal data is carried out for the duration of the underlying commercial agreement(s).

Appendix B Sub-processors

B.1 Authorised sub-processors

Upon entry into force of the Regulations, the controller has authorised the use of the following sub-processors

NAME	ADDRESS	COUNTRY	DESCRIPTION OF TREATMENT
Zoho Project Management	Zoho Corporation B.V. Beneluxlaan 4B 3527 HT UTRECHT	Netherlands (Data Centres in the Netherlands & Ireland)	Project Management and time registration
Microsoft Danmark ApS	Kanalvej 7, 2800 Kongens Lyngby, DK	Datacenter Sweden and datacenter Denmark	Microsoft Azure

Upon the entry into force of the Clauses, the Data Controller has authorised the use of the above-mentioned sub-processors for the processing activity described. The Data Processor may not - without the Data Controller's written authorisation - use a Sub-Processor for a processing activity other than the described and agreed processing activity or use a different Sub-Processor for this processing activity.

B.2 Notification for authorisation of sub-processors

The Processor shall notify the Controller in writing of any planned changes regarding the addition or replacement of sub-processors, thereby giving the Controller the opportunity to object to such changes. Such notification shall be made with at least 30 days' notice.

If the controller objects to the changes, the controller shall notify the data processor accordingly. The controller may only object if the controller has reasonable, specific reasons for doing so.

Objections to the addition or replacement of sub-processors shall not have a suspensive effect on the implementation thereof. If the Data Controller has objections, both the Data Controller and the Data Processor are entitled to terminate the Agreement in writing with effect from the time of implementation of new sub-processors, so that the change will not take effect vis-à-vis the Data Controller.

Appendix C Instructions for the processing of personal data

C.1. Subject matter/instruction of the treatment

The data processor's processing of personal data on behalf of the data controller takes place by the data processor performing the processing activities described in Appendix A.

C.2 Processing security

The Data Processor shall implement all measures required under Article 32 of the General Data Protection Regulation, which states, inter alia, that a high level of security shall be implemented, taking into account the current level, implementation costs and the nature, scope, context and purposes of the processing concerned and the risks of varying likelihood and severity for the rights and freedoms of natural persons.

The data processor is then entitled and obliged to make decisions about which technical and organisational security measures must be implemented to establish the necessary (and agreed) security level.

However, the processor shall - in any case and as a minimum - implement the following measures agreed with the controller:

Organisational security

The Data Processor shall implement the following organisational security measures:
a) All employees of the data processor are subject to confidentiality obligations that apply for all processing of personal data.
b) Employee access to personal data is restricted so that only the relevant employees have access to the necessary personal data.
c) The processing of personal data carried out by the data processor's employees is logged and can be controlled as necessary.
d) The Processor has an IT security policy.
e) The data processor has the possibility to respond to employees' breaches of the data processor's data security of the data processor or breach of instructions on the processing of personal data in personal data under employment law.
f) The Data Processor's employees regularly document and report personal data security breaches or risks thereof.
g) The Processor has established procedures to ensure proper erasure or Continuous confidentiality when the hardware is repaired, serviced or disposed of.

Technical security: Accessing and protecting IT systems

The Data Processor shall implement the following technical security measures regarding Access to and protection of IT systems:
a) The Data Processor uses logical access control with username and password or other unique authorisation.
b) The Data Processor uses antivirus programmes that are regularly updated.
c) The Data Processor logs and checks unauthorised or repeated failed login attempts.
d) The processor requires employees to use individual passwords.
e) The Data Processor's computers have automatic access protection during inactivity, e.g. Locked screensaver.
f) The Data Processor has policies for password composition, including minimum requirements.
g) There are procedures for revoking authorisations when an employee leaves or changes departments.
h) There are procedures for granting rights to IT systems when hiring new employees.

Technical security: Access to personal data
The Data Processor shall implement the following technical security measures regarding access to personal data:
a) The Processor shall undergo regular system checks.
b) The processor grants authorisations to individuals or groups of users to access, modify and delete processed personal data.
c) The Data Processor has procedure(s) to restore data from backup.
d) The Processor regularly reviews and verifies user authorisations for specific systems.
e) The Processor logs and controls unauthorised or repeated unsuccessful attempts to access data.
f) The Data Processor has traceability of access to, modification and deletion of data by individual users.

Technical security: Encryption
The Data Processor shall implement the following technical security measures regarding Encryption:
a) Passwords stored on the data processor's computers etc. are encrypted.
b) The Data Processor's websites and web forms use SSL certificates/HTTPS (Hyper Text Transfer Protocol Secure).

C.3 Assistance to the controller
The data processor shall, as far as possible - within the scope and extent set out below - assist the data controller in accordance with Clauses 9.1 and 9.2 by implementing the following technical and organisational measures:

- Description of the sequence of events
- Identification of the data subjects affected by the incident
- Types of personal data covered by the incident

C.4 Storage period/deletion routine
Upon termination of this agreement, the controller and its representatives will no longer have access to the software specified in the contract. The underlying database will be stored in the backup system for up to three (3) months, after which all copies of the personal data provided by the controller will be deleted.

Any access to and restoration of backed up data requires a written instruction from the Data Controller. A backup copy of data will be provided to the Data Controller upon written request. The costs associated with this will be paid at the Data Processor's hourly rates applicable at the time in question.

C.5 Location of treatment
Processing of personal data in accordance with the Clauses cannot be carried out on other locations other than the following without the prior written authorisation of the controller:
At the Data Processor's own head office or at the head office of authorised sub-processors as specified in Appendix B.

C.6 Instructions for the transfer of personal data to third countries
Personal data is only processed by the data processor at the locations specified in Section C.5. the data processor does not transfer personal data to third countries or international organisations.

If the controller does not provide documented instructions in these Clauses or subsequently regarding the transfer of personal data to a third country, the data processor is not authorised to make such transfers within the framework of these Clauses.

C.7 Procedures for the controller's audits, including inspections, of the processing of personal data entrusted to the processor

Once a year, the controller or a representative of the controller may carry out a physical inspection of the premises from which the processor processes personal data, including physical premises and systems used for or in connection with the processing, in order to determine the processor's compliance with the GDPR, data protection provisions of other Union or Member State law and these Clauses.

Any costs incurred by the controller in connection with a physical inspection shall be borne by the controller itself. However, the data processor is obliged to allocate the resources (mainly time) necessary for the controller to carry out its inspection.

C.8 Procedures for audits, including inspections, of processing of personal data entrusted to sub-processors

The Data Processor shall at least every 12 months, at its own expense, conduct an audit of the Data Processor's sub-processors and submit documentation of this audit to the Data Controller.

The parties agree that the independent auditor's ISAE 3000 statement may be used for this purpose.