Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

GENERISK DATAANSVARLIG
GENERISK DANNET ADRESSE
Aalborg 9000
DK
Company registration number:
hereinafter "The Data Controller"

and

BOARD OFFICE A/S
Vesterbro 21 B, 1.
9000 Aalborg
DK
Company registration number: 28966237
hereinafter "The Data Processor"

each a "Party"; together the "Parties"

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

This is version 2, last updated 20.09.2022 15:18.

1. **Content**

2. Preamble

2.1 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.

2.2 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).

2.3 In the context of the provision of BOARD-OFFICE & BOARD-PEOPLE, the Data Processor will process personal data on behalf of the Data Controller in accordance with the Clauses.

2.4 The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

2.5 Four appendices are attached to the Clauses and form an integral part of the Clauses.

2.6 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.

2.7 Appendix B contains the Data Controller's conditions for the Data Processor's use of sub-processors and a list of sub-processors authorised by the Data Controller.

2.8 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.

2.9 Appendix D contains provisions for other activities which are not covered by the Clauses.

2.10 If standard contractual clauses as referred to in GDPR, article 46(2), litra c and d form basis of transfer of personal data between the Data Controller and the Data Processor covered by chapter V of the GDPR, these will be attached as Appendices E and E1.

2.11 The Clauses along with appendices shall be retained in writing, including electronically, by both parties

2.12 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.

3. The rights and obligations of The Data Controller

3.1 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.

3.2 The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3 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.

4. The Data Processor acts according to instructions

4.1 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.

4.2 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.

5. Confidentiality

5.1 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.

5.2 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.

6. Security of processing

6.1 GDPR, article 32, 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 organisational 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:

6.1.1 Pseudonymisation and encryption of personal data;

6.1.2 the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

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

6.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2 According to GDPR, article 32, 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.

6.3 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 organisational measures already implemented by the Data Processor pursuant to GDPR, article 32, along with all other information necessary for the Data Controller to comply with the Data Controller's obligation under GDPR, article 32.

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 GDPR, article 32, the Data Controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

7.1 The Data Processor shall meet the requirements specified in GDPR, article 28(2) and (4) in order to engage another processor (a sub-processor).

7.2 The Data Processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the Data Controller.

7.3 The Data Processor has the Data Controller's general authorisation 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 30 days 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 authorised by the Data Controller can be found in Appendix B.

7.4 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 organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

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.

7.5 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.

7.6 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.

7.7 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 GDPR, articles 79 and 82 – against the Data Controller and the Data Processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

8.1 Any transfer of personal data to third countries or international organisations 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.

8.2 In case transfers to third countries or international organisations, 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.

8.3 Without documented instructions from the Data Controller, the Data Processor

therefore cannot within the framework of the Clauses:

8.3.1 transfer personal data to a data controller or a data processor in a third country or in an international organization

8.3.2 transfer the processing of personal data to a sub-processor in a third country

8.3.3 have the personal data processed by the data processor in a third country

8.4 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.

8.5 The Clauses shall not be confused with standard data protection clauses within the meaning of GDPR, article 46(2)(c) and (d), and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR unless such standard contractual clauses are attached in Appendix E.

9. Assistance to the Data Controller

9.1 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:

9.1.1 the right to be informed when collecting personal data from the data subject

9.1.2 the right to be informed when personal data have not been obtained from the data subject

9.1.3 the right of access by the data subject

9.1.4 the right to rectification

9.1.5 the right to erasure ('the right to be forgotten')

9.1.6 the right to restriction of processing

9.1.7 notification obligation regarding rectification or erasure of personal data or restriction of processing

9.1.8 the right to data portability

9.1.9 the right to object

9.1.10 the right not to be subject to a decision based solely on automated processing,

including profiling

9.2 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:

9.2.1 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 data protection agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

9.2.2 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;

9.2.3 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);

9.2.4 the Data Controller's obligation to consult the competent 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.

9.3 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.

10. Notification of personal data breach

10.1 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.

10.2 The Data Processor's notification to the Data Controller shall, if possible, take place within immediately and no later than 12 hours after the data processor has become aware of the breach of the personal data security 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 data protection agency, cf. GDPR, article 33.

10.3 In accordance with Clause 9.2.1, 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 GDPR, article 33(3), shall be stated in the Data Controller's notification to the competent data protection agency:

10.3.1 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;

10.3.2 the likely consequences of the personal data breach;

10.3.3 the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.4 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 data protection agency.

11. Erasure and return of data

11.1 On termination of the provision of personal data processing services, the Data Processor shall be under obligation 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.

12. Audit and inspection

12.1 The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in GDPR, 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.

12.2 Procedures applicable to the Data Controller's audits, including inspections, of the Data Processor and sub-processors are specified in C.7 and C.8.

12.3 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.

13. The parties' agreement on other terms

13.1 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.

14. Commencement and termination

14.1 The Clauses are binding upon the Parties.

14.2 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.

14.3 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.

14.4 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.

14.5 The Data Processor is bound by the Data Processor Agreement without the Parties' signatures. The Data Processor Agreement is thus concluded without physical / digital signatures, as the Data Processor Agreement is binding in accordance with the requirement of GDPR, article 28(3), first sentence.

15. Data controller and data processor contacts/contact points

15.1 The Parties may contact each other using the following contacts/contact points

15.2 The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Contact information for the Data Controller:

Contact information for the Data Processor:
Niels Arnold Lund, NAL@board-office.dk

Appendix A Information about the processing

1. **The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:**

1.1 The following purposes form the basis of the Data Processor's processing of personal data on behalf of the Data Controller:

The data controller wishes to make use of the data processors product, BOARD-OFFICE & BOARD-PEOPLE, which is an online portal which contains document-storage, debate-forum, planning tool, enables digital signature, job ads for board positions and a creativity area.

The data processor is responsible for the day-to-day operation, maintenance, development and debugging of the provided products.

2. **The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):**

2.1 The data processor processes personal data related to the provided products.

3. **The processing includes the following types of personal data about data subjects:**

3.1 name, address, phone number, e-mail, username for one or several systems, password to one or several systems, various personal data provided or recorded by the customer or the customer's customers without the organization's active processing and identification thereof, billing and accounting documents, various personal data which are recorded in connection with the delivery of the service and cannot be precisely defined

3.2 The Data Processor may process personal data about the Data Controller's employees in connection with the Data Processor's sales, marketing and product development. This processing of personal data is not covered by the Clauses, because the Data Processor acts as a data controller in regard of this processing. Instead, reference is made to the Data Processor's privacy policy which can be found on the Data Processor's website or upon request.

4. **Processing includes the following categories of data subject**

4.1 affiliates that are individuals or sole proprietorships, customers that are consumers or sole proprietors

Leaders and board members.

5. **The Data Processor’s processing of personal data on behalf of the Data Controller may be performed when the Clauses commence. The processing has the following duration:**

5.1 The processing of personal data shall be performed until the Data Processor's services has been terminated, after which the personal data is either returned or erased in accordance with Clause 11. The Data Processor's processing of personal data is performed as long as the underlying commercial agreement(s) consists.

Appendix B Authorised Sub-processors

1. Approved sub-processors

1.1 On commencement of the Clauses, the Data Controller authorizes the engagement of the following sub-processors

1.2 The Data Processors sub-processors are listed in the List of Sub-processors, that is available on our website under the ‘Security’ tab, and in ‘Settings’ on the individual boards.

1.3 The Data Controller shall on the commencement of the Clauses authorize the use of the abovementioned 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

1. The subject of/instruction for the processing

1.1 Storage of documents, debate-forum, planning tool, digital signature, job ads for board members and a creativity area.

2. Security of processing

2.1 The level of security shall take into account:

Taking into account the nature, scope, context and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons, the Data Processor must implement an appropriate level of security.

The Data Processor shall hereafter be entitled and under obligation to make decisions about the technical and organizational security measures that are to be applied to create the necessary (and agreed) level of data security.

The Data Processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the Data Controller:

Physical security
The Data Processor shall implement the following physical security measures:

a) The data processor's office space can be locked.
b) The data processor uses alarm systems to detect and prevent burglary.
c) The data processor uses fire alarms and smoke detectors to detect and prevent fires.
d) The data processor's devices (including PCs, servers, etc.) are secured behind locked doors.
e) The data processor's premises and facilities or access routes are subject to video or image monitoring.
f) The data processor uses a verification process or verification system to control the identity of visitors.
g) The data processor uses key management, i.e. provide keys to the relevant and necessary employees, etc.
h) A protocol is kept of the Data Processor's visitors.

Organizational security
The Data Processor shall implement the following organizational security measures:

a) All employees of the data processor are subject to confidentiality obligations that apply to all processing of personal data.
b) The employee access to personal data is limited, so that only the relevant employees have access to the necessary personal data.
c) The processing of personal data done by the employees of the data processor is

logged and can be checked as required.

d) Employees with access to personal data or critical IT systems have undergone a security clearance before they were employed.
e) The data processor has documentable process descriptions for breaches of the personal data security, which are reviewed at least annually.
f) The data processor has an IT security policy.
g) The data processor has established procedures that ensures proper deletion or continuous confidentiality when hardware is repaired, serviced or disposed.

Technical security: Access to and protection of 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 authorization.
b) The data processor uses antivirus programs that are updated regularly.
c) The data processor requires employees to use individual passwords.
d) The data processor's computers have automatic access protection during inactivity, ie. locked screen saver.
e) The data processor has policies for password composition, including minimum requirements.
f) There are procedures for revoking permissions when an employee stops or switches department.

Automatic daily backup of the database, through the storage and backup solution, IBM Tivoli Storage Manager.

Personal data is encrypted in systems and/or storage solutions, where relevant and in consideration to character of the processing and personal data.

Firewall, which is updated regularly with the purpose of always providing full protection.

Antivirus programs, which are updated regularly, to make sure that the programs modules and its system components are able to provide full protection.

The data processors websites use HTTPS (Hyper Text Transfer Protocol Secure), to make sure that all communication on the open internet is encrypted peer-to-peer.

Technical security: Access to personal data
The Data Processor shall implement the following technical security measures regarding access to personal data:

a) The data processor grants authorizations to individuals or groups of users to access, change and delete processed personal data.
b) The data processor regularly reviews and verifies user authorizations for specific systems.

c) The data processor has traceability of access, modification and erasure of data by individual users.
d) The data processor regularly reviews system controls.

Technical security: Encryption
The Data Processor shall implement the following technical security measures regarding encryption:

a) Passwords stored on the processor's computers, etc. are encrypted.
b) Content on external hard drives and USB keys, etc. is encrypted when such media contain personal or sensitive personal information.
c) The data processor's computers have encrypted hard drives.
d) The data processor encrypts personal data in systems and/or on devices.
e) The data processor's websites and web forms uses SSL certificates/HTTPS (Hyper Text Transfer Protocol Secure).

Technical security: Protection of personal data during transmission
The Data Processor shall implement the following technical security measures regarding protection of personal data during transmission:

a) The data processor uses and has guidelines for secure email.
b) Outgoing emails with sensitive personal data or information about purely private matters are encrypted.
c) The data processor has guidelines for the use of work emails, including use for private use, appropriate use, encryption, secure use, etc.

Technical security: Availability and robustness
The Data Processor shall implement the following technical security measures regarding availability and robustness:

a) Accessibility and robustness of the data processor's systems and servers are secured by a third party with whom the data processor has an agreement.
b) Only authorized employees have access to the data processor's own servers.
c) Server rooms have smoke alarms and fire extinguishers.
d) Server room has air conditioning system.
e) There are rules and guidelines for data backup.
f) There are rules and guidelines for restoring data from backup.
g) Active alerting by unauthorized attempts to access server rooms and / or processing systems and data.
h) Backups are made regularly (either in-house or at supplier).
i) Uninterruptible power supply (UPS) is used.
j) Monitoring of temperature and humidity in server rooms.
k) The data processor has procedure descriptions for breaches of the personal data security that are reviewed at least annually.

3. Assistance to the data controller

3.1 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 organisational measures:

3.1.1 If the Data Controller receives a request for the exercise of one of the rights of the data subjects in accordance with applicable data protection law, and a proper reply to the request requires assistance from the Data Processor, the Data Processor shall assist the Data Controller with the necessary and relevant information and documentation as well as appropriate technical and organizational security measures.

3.1.2 If the Data Controller needs the Data Processor's assistance in order to reply to a request from a data subject, the Data Controller must send a written request for assistance to the Data Processor and the Data Processor shall in response provide the necessary help or documentation as soon as possible and no later than 7 calendar days after receiving the request.

3.1.3 If the Data Processor receives a request for the exercise of the rights pursuant to applicable data protection law from other persons than the Data Controller, and the request concerns personal data processed on behalf of the Data Controller, the Data Processor shall without undue delay forward the request to the Data Controller.

4. Storage period/erasure procedures

4.1 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.

5. Processing location

5.1 Processing of the personal data under the Clauses cannot be performed at other locations than the following without the Data Controller’s prior written authorisation:

At the Data Processor's own headquarter or at the headquarters of approved sub-processors as specified in Appendix B.

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

6.1 Personal data is only being processed by the Data Processor on the locations specified in Clause C.5. The Data Processor does not transfer personal data to third countries or international organizations.

6.2 If the Data Controller does not provide a documented instruction in these Clauses or subsequently with regards to the transfer of personal data to a third country, the Data Processor is not entitled to carry out such transfers within the scope of these Clauses.

6.3 Transfer of personal data can in all cases only be done in accordance with these Clauses, on the instructions of the Data Controller and to the extent permitted by the applicable data protection law.

6.4 Where, in accordance with these clauses, the Data Processor transfers personal data to sub-data processors in third countries outside the EU / EEA, the Data Processor must independently secure a legal basis for the transfer in accordance with Chapter 5 of GDPR.

6.5 If the transfer of personal data to third countries outside the EU / EEA is carried out in connection with the Data Processor's transfer to sub-processors, the Data Processor is by the provisions of the agreement authorized to enter into the standard contractual provisions adopted by the European Commission with the Data Processor's sub-processors on behalf of the Data Controller, provided that all rules of the Danish Data Protection Law for transmission and processing are otherwise complied with. If the data controller itself is data processor, and the data processor is a sub-data processor of the data in relation to the data controller's ultimate contractual partner(s), the Data Controller must obtain authorization from the ultimate contracting party of the Data Processor in the standard contract terms.

7. Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

7.1 The Data Processor shall, upon the Data Controller's written request, document to the Data Controller that the Data Processor

7.1.1 is complying with his obligations under these Clauses and the Instruction, and

7.1.2 with the relevant articles in the GDPR in regards to the personal data being processed on behalf of the Data Controller.

7.2 According to Clause C.7.1 the Data Processor's documentation shall be sent to the Data Controller within a reasonable time after receiving the request.

7.3 The data processor must provide the data controller with documentation of continuous compliance with the provisions. These self-audit reports must be prepared at least once a year and shall follow the principles and control objectives of the ISAE 3000 auditing standard, as laid down by Common Strategic Framework (CSF) - Danish Auditors and the Danish Data Protection Agency (and/or alternatively internationally recognized standards such as ISO/IEC 27701:2019). Self-audit reports may be conducted as part of the data controller's information gathering and must be signed by the data processor's management. The Data Processor is not obligated to initiate and undertake external audits of its compliance with the Clauses on its own initiative.

7.4 Regardless of Clause C.7.3, the Data Processor shall furthermore provide for and contribute to audits and inspections every 12 months, performed by auditors appointed by the Data Controller, the public authorities in Denmark or other competent jurisdiction, to the extent necessary to verify the Data Processor's compliance with these Clauses and the applicable data protection law. The auditor in question must be subject to confidentiality under law or agreement. The Data Controller must notify the audits in writing with 10 calendar days.

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

8.1 The data processor is responsible for running regular self-assessment in accordance with ISAE 3000 principles.
The data controller is to be made aware of changes to the agreement that are considered to be of importance and of relevance for the processing of their data.

Appendix D The Parties' terms of agreement on other subjects