Data Processing Agreement.

Prepared in accordance with the standard contractual clauses adopted by the European Data Protection Board

Standard Contractual Clauses

pursuant to Article 28(3) of Regulation 2016/679 (GDPR)
for the Data Processor's processing of personal data

between

GENERIC COMPANY NAME
GENERIC ADDRESS
CVR-nr.: GENERIC CVR
hereinafter the "Data Controller"

Contact person:
GENERIC NAME
GENERIC EMAIL/PHONE NUMBER

and

BOARD OFFICE A/S
Jernbanegade 14, 1.
9000 Aalborg
DK
CVR-nr.: 28966237

hereinafter the "Data Processor"

individually referred to as a "Party" and collectively as the "Parties"

HAVE AGREED on the following standard contractual clauses ("Clauses") to ensure compliance with the GDPR and the protection of privacy and fundamental rights and freedoms of natural persons.

1. **Table of Contents**

2. Preamble

1. These Clauses set out the rights and obligations of the Data Processor when processing personal data on behalf of the Data Controller.

2. These Clauses 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 ("GDPR").

3. In connection with the provision of BOARD-OFFICE & BOARD-PEOPLE, the Data Processor processes personal data on behalf of the Data Controller in accordance with these Clauses.

4. The Clauses shall take precedence over any similar provisions contained in other agreements between the Parties.

5. Annexes are attached to these Clauses and form an integral part hereof.

6. Annex A contains detailed information on 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. Annex B sets out the Data Controller's conditions for the Data Processor's use of sub-processors and includes a list of sub-processors approved by the Data Controller.

8. Annex C sets out the Data Controller's instructions regarding the processing of personal data by the Data Processor, a description of the minimum security measures to be implemented by the Data Processor, and information on how supervision of the Data Processor and any sub-processors is conducted.

9. Annex D includes provisions regarding other activities not covered by these Clauses.

10. Where standard contractual clauses as referred to in Article 46(2)(c) and (d) of the GDPR constitute the legal basis for transfers of personal data between the Data Controller and the Data Processor to third countries as set out in Chapter V of the GDPR, reference is made in Annex E to the English version of the SCCs, which is the official and binding version adopted by the European Commission. The Clauses, including the Annexes, must be kept in writing, including electronically, by both Parties.

11. These Clauses do not relieve the Data Processor of any obligations imposed under the GDPR or any other applicable legislation.

3. The Data Controller's Rights and Obligations

1. The Data Controller is responsible for ensuring that the processing of personal data is carried out in compliance with the GDPR (see Article 24), data protection provisions under other applicable EU legislation or the national laws of EU/EEA Member States, and these Clauses.
2. The Data Controller has the right and obligation to determine the purposes and means of the processing of personal data.

3. The Data Controller is responsible for ensuring, among other things, that there is a valid legal basis for the processing of personal data which the Data Processor is instructed to carry out.

4. The Data Processor Acts on Instructions

1. The Data Processor may only process personal data based on documented instructions from the Data Controller, unless required to do so under Union law or the national law of an EU/EEA Member State to which the Data Processor is subject. Such instructions shall be specified in Annexes A and C. Additional instructions may be issued by the Data Controller during the course of the processing of personal data, but such instructions must always be documented and retained in writing, including electronically, together with these Clauses.

2. The Data Processor shall immediately notify the Data Controller if, in the Data Processor's opinion, an instruction infringes the GDPR or the data protection provisions of other applicable Union or Member State law.

5. Confidentiality

1. The Data Processor shall only grant access to personal data processed on behalf of the Data Controller to individuals who are subject to the Data Processor's authority and who are bound by a duty of confidentiality or a suitable statutory obligation of secrecy, and only to the extent necessary. The list of individuals who have been granted access must be reviewed on a regular basis. Based on this review, access shall be revoked if it is no longer necessary, and such individuals shall no longer have access to the personal data.
2. Upon request from the Data Controller, the Data Processor shall be able to demonstrate that the individuals under its authority who have access to personal data are subject to the aforementioned obligation of confidentiality.

6. Security of Processing

1. Article 32 of the GDPR requires that both the Data Controller and the Data Processor implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing, as well as the varying likelihood and severity of risks to the rights

and freedoms of natural persons.
The Data Controller must assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to mitigate those risks. Depending on their relevance, such measures may include:

a. Pseudonymisation and encryption of personal data
b. The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services
c. The ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident
d. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

2. Pursuant to Article 32 of the GDPR, the Data Processor must also, independently of the Data Controller, assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to mitigate those risks. For this purpose, the Data Controller shall provide the Data Processor with the necessary information to enable such assessment.
3. Furthermore, the Data Processor shall assist the Data Controller in complying with the Data Controller's obligations under Article 32 of the GDPR by, among other things, providing the necessary information about the technical and organisational security measures the Data Processor has already implemented under Article 32, and any other information required for the Data Controller to meet its obligations.

   If the Data Controller, based on its own risk assessment, determines that additional measures are required beyond those already implemented by the Data Processor, the Data Controller shall specify such additional measures to be implemented in Annex C.

4. By entering into this Data Processing Agreement, the Data Controller issues a documented instruction allowing the Data Processor to transfer personal data to third countries where necessary for the purpose of processing and the use of sub-processors, provided that a valid legal basis for the transfer exists (e.g. SCC 2021/914).

7. Use of Sub-Processors

1. The Data Processor shall comply with the conditions set out in Article 28(2) and (4) of the GDPR in order to engage another processor (a sub-processor).

2. The Data Processor may not engage a sub-processor for the purposes of these Clauses without the prior general written authorisation of the Data Controller.

3. The Data Controller has granted general authorisation for the Data Processor to use sub-processors. The Data Processor shall notify the Data Controller in writing of any intended changes concerning the addition or replacement of sub-processors at least 30 calendar days in advance, thereby allowing the Data Controller to object to such changes before the new sub-processor(s) is/are

engaged. A longer notice period for specific processing activities may be specified in Annex B. The list of sub-processors already approved by the Data Controller appears in Annex B.

4. When engaging a sub-processor to carry out specific processing activities on behalf of the Data Controller, the Data Processor shall impose on the sub-processor, by contract or other legal act under Union or Member State law, the same data protection obligations as those set out in these Clauses. In particular, sufficient guarantees shall be provided to ensure that the sub-processor implements appropriate technical and organisational measures in such a manner that the processing will meet the requirements of these Clauses and the GDPR.

   The Data Processor is therefore responsible for ensuring that the sub-processor, at a minimum, complies with the Data Processor's obligations under these Clauses and the GDPR.

5. Sub-processor agreements and any subsequent amendments shall be provided to the Data Controller upon request, thereby allowing the Data Controller to verify that the same data protection obligations as those contained in these Clauses have been imposed on the sub-processor. Provisions of a purely commercial nature that do not affect the data protection content of the agreement do not need to be shared with the Data Controller.

6. In its agreement with the sub-processor, the Data Processor shall include the Data Controller as a third-party beneficiary in the event of the Data Processor's bankruptcy, thereby allowing the Data Controller to exercise its rights directly against the sub-processor, for example to instruct the sub-processor to delete or return personal data.

7. If the sub-processor fails to fulfil its data protection obligations, the Data Processor shall remain fully liable to the Data Controller for the performance of the sub-processor's obligations. This does not affect the rights of data subjects under the GDPR, in particular Articles 79 and 82, against both the Data Controller and the Data 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 by the Data Processor may only take place on the basis of documented instructions from the Data Controller and shall always comply with Chapter V of the GDPR.

2. If the Data Processor is required to transfer personal data to a third country or an international organisation by Union or Member State law to which the Data Processor is subject, the Data Processor shall inform the Data Controller of that legal requirement before processing takes place, unless the law prohibits such notification on important grounds of public interest.

3. Without documented instructions from the Data Controller, the Data Processor may not, within the scope of these Clauses:

a. transfer personal data to a controller or processor in a third country or to an international organisation;

b. engage a sub-processor in a third country;

c. process personal data in a third country.

4. The Data Controller's instructions regarding the transfer of personal data to third countries, including the applicable legal basis under Chapter V of the GDPR, shall be specified in Annex C.

5. These Clauses must not be confused with the standard contractual clauses referred to in Article 46(2)(c) and (d) of the GDPR, and these Clauses do not constitute, on their own, a legal basis for the transfer of personal data as described in Chapter V of the GDPR unless such standard contractual clauses are set out in Annex E.

6. By entering into this Data Processing Agreement, the Data Controller issues a documented instruction allowing the Data Processor to transfer personal data to third countries if such transfers are necessary to fulfil the purpose of the processing and involve the use of sub-processors, provided that a valid transfer mechanism exists (e.g. SCC 2021/914).

9. Assistance to the Data Controller

1. Taking into account the nature of the processing, the Data Processor shall, as far as possible, assist the Data Controller by appropriate technical and organisational measures in fulfilling the Data Controller's obligation to respond to requests for the exercise of data subjects' rights under Chapter III of the GDPR.

   This means that the Data Processor shall assist the Data Controller, to the extent possible, in ensuring compliance with:
   1. the obligation to provide information when personal data is collected from the data subject;
   2. the obligation to provide information when personal data is not collected from the data subject;
   3. the right of access;
   4. the right to rectification;
   5. the right to erasure ("right to be forgotten");
   6. the right to restriction of processing;
   7. the obligation to notify recipients regarding rectification or erasure of personal data or restriction of processing;
   8. the right to data portability;
   9. the right to object;
   10. the right not to be subject to a decision based solely on automated processing, including profiling.

2. In addition to the obligation set out in Clause 7.1, the Data Processor shall, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller in ensuring compliance with:

    1. the obligation to notify the supervisory authority of a personal data breach without undue delay and, where feasible, no later than 72 hours after becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons;
    2. the obligation to notify the data subject of a personal data breach without undue delay when the breach is likely to result in a high risk to the rights and freedoms of natural persons;
    3. the obligation to carry out a data protection impact assessment (DPIA) prior to processing where required under the GDPR;
    4. the obligation to consult the supervisory authority prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk.

3. The Parties shall set out in Annex C the technical and organisational measures by which the Data Processor shall assist the Data Controller, as well as the scope and extent of such assistance as required under Clauses 9.1 and 9.2.

10. Notification of Personal Data Breach

1. The Data Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach.

2. Where feasible, the notification to the Data Controller shall be made immediately and no later than 12 hours after the Data Processor becomes aware of the personal data breach, in order to enable the Data Controller to meet its obligation to notify the competent supervisory authority in accordance with Article 33 of the GDPR.

3. In accordance with Clause 9.2, the Data Processor shall assist the Data Controller in fulfilling its obligation to notify the supervisory authority. This includes, but is not limited to, providing the following information, which must be included in the Data Controller's notification under Article 33(3):

    1. 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 concerned;

    2. the likely consequences of the personal data breach;

    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.

4. The Parties shall specify in Annex C the type of information the Data Processor shall provide to assist the Data Controller in fulfilling its notification obligations to the supervisory authority.

11. Deletion and Return of Data

1. Upon termination of the services relating to the processing of personal data, the Data Processor shall, at the choice of the Data Controller, either delete or return all 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

1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with Article 28 of the GDPR and these Clauses, and shall allow for and contribute to audits, including inspections, carried out by the Data Controller or an auditor mandated by the Data Controller.

2. The procedures for audits and inspections of the Data Processor and any sub-processors are specified in Annexes C.7 and C.8.

3. The Data Processor shall grant access to its physical facilities to competent supervisory authorities, or their representatives acting on behalf of such authorities, who are entitled to access the facilities of the Data Controller or the Data Processor under applicable law, upon presentation of proper identification.

13. Agreement on Other Provisions

1. The Parties may agree on additional provisions concerning the service related to the processing of personal data, such as provisions on liability, provided that such provisions do not directly or indirectly contradict these Clauses or prejudice the fundamental rights and freedoms of data subjects under the GDPR.

14. Commencement and Termination

1. These Clauses are binding on the Parties.

2. Either Party may request that the Clauses be renegotiated if legislative changes or practical circumstances justify such renegotiation.

3. The Clauses shall apply for as long as the services relating to the processing of personal data are provided. During this period, the Clauses may not be terminated, unless the Parties agree to other provisions governing the service.

4. If the provision of services is terminated and the personal data has been deleted or returned to the Data Controller in accordance with Clause 9.1 and Annex C.4, the Clauses may be terminated by either Party with written notice.

5. The Data Processor is bound by these Clauses without the need for signature by the Parties. The Clauses are therefore concluded without physical or digital signatures and are binding pursuant to Article 28(3), first paragraph, of the GDPR.

15. Contact Persons

1. The Parties may communicate with each other through the contact persons listed in the agreement.

2. The Parties are obligated to inform each other promptly of any changes to their respective contact persons.

Contact info for the

Contact info for the Data Processor:

Niels Arnold Lund, mail: nal@board-office.dk

Annex A – Details of the Processing

1. Purpose of the Data Processor's processing of personal data on behalf of the Data Controller

1.1 The Data Processor processes personal data on behalf of the Data Controller for the following purposes:

The Data Controller wishes to use the Data Processor's board portal, BOARD-OFFICE, which is an online platform containing, among other features, a document repository, discussion forum, planning tool, digital signature module, board position postings, and an inspiration area.

In addition, the Data Processor is responsible for operating, testing, maintaining, developing, and correcting errors in the Data Processor's applications.

2. Nature of the processing of personal data on behalf of the Data Controller

2.1 The Data Processor processes personal data in connection with the provision of the BOARD-OFFICE & BOARD-PEOPLE board portals.

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

3.1 Name, address, phone number, email, username(s) for one or more systems, password(s) for one or more systems, and various personal data submitted or registered by the customer or the customer's clients without the organisation actively processing or identifying the information.

3.2 The Data Processor may also process personal data about the Data Controller's employees in connection with the Data Processor's sales, marketing, and product development. These personal data are not covered by the Clauses, as the Data Processor is the data controller for such information. Reference is instead made to the Data Processor's privacy policy, which is available on the Data Processor's website or upon request.

4. The processing includes the following categories of data subjects

4.1 Management, board members, administrative staff, and other external stakeholders to whom the individual company grants access to the portal.

5. Commencement and duration of the processing

5.1 The processing of personal data may begin after the Clauses take effect. The personal data will be processed until termination of the services related to personal data processing, after which the personal data will be deleted or returned in accordance with Clause 11. Processing will therefore continue for as long as the underlying commercial agreement(s) remain in force.

Annex B – Sub-Processors

Approved sub-processors

1. **A**t the time of entry into force of these Clauses, the Data Controller has approved the use of the following sub-processors:
   The Data Processor's sub-processors are listed in the most up-to-date list of sub-processors, which can be accessed under the "Security" section on the Data Processor's website:
   https://www.board-office.dk/media/ew0nz3rl/underdatabehandlere-09-12-24.pdf,
   or under "Settings" within the individual board portals.

2. Scope of approval
   By accepting these Clauses, the Data Controller approves the use of the above-mentioned sub-processors for the described processing activity.
   The Data Processor may not – without the prior written consent of the Data Controller – use a sub-processor for any processing activity other than the one described and agreed, or use a different sub-processor for that activity.

Annex C – Instructions on the Processing of Personal Data

1. Subject of the Processing / Instruction

1.1 The Data Processor processes personal data on behalf of the Data Controller to enable the Data Controller to use the BOARD-OFFICE & BOARD-PEOPLE board portals. These are online platforms that include, among other features, a document repository, discussion forum, planning tool, digital signature, board position postings, and an inspiration area.

2. Security of Processing

2.1 The level of security must reflect:

The Data Processor shall establish an appropriate level of security taking into account the nature, scope, context, and purpose of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons.

The Data Processor is both entitled and obligated to determine the specific technical and organisational security measures necessary to achieve the required and agreed level of protection.

However, the Data Processor shall, as a minimum and as agreed with the Data Controller, implement the following measures:

a) Physical security

- Office premises can be locked.
- An alarm system is in place to detect and prevent unauthorized access.
- Smoke detectors and fire alarms are installed.
- Equipment (PCs, servers, etc.) is stored behind locked doors.
- Buildings, rooms, and access routes are monitored by video or image surveillance.
- Visitor identity is controlled using a process or system.
- Key management ensures only necessary staff receive access keys.
- A visitor log is maintained.

b) Organisational security

- All employees are bound by confidentiality regarding all processed personal data.
- Access to personal data is restricted to relevant employees only.
- Employees with access to sensitive data or IT systems are subject to security vetting before employment.
- Processing activities are logged and subject to review.
- A documented procedure for handling personal data breaches is reviewed at least annually.
- An IT security policy is in place.
- A process ensures data is securely deleted or kept confidential when hardware is repaired, serviced, or decommissioned.

c) Technical security – Access to and protection of systems

- Logical access control (e.g., usernames and passwords) is implemented.
- Individual login credentials are required.
- Workstations auto-lock after inactivity.
- Antivirus software is installed and regularly updated.
- Password composition policies with minimum requirements are enforced.
- Access rights are revoked when employees leave or change roles.
- Failed login attempts are logged and monitored.

A daily automatic backup of the database is performed using IBM Tivoli Storage Manager.

Personal data is encrypted in systems and/or on storage devices, as appropriate based on the nature of processing and data sensitivity.
A continuously updated firewall and antivirus software ensure full system protection.
All web traffic uses HTTPS (Hyper Text Transfer Protocol Secure) for peer-to-peer encryption over the internet.

d) Technical security – Access to personal data

- Regular review and validation of user access rights.
- Traceability of data access, changes, and deletions by individual users.
- User and group-based permissions to access, modify, and delete personal data.
- Data restoration procedures from backups are established.

e) Technical security – Encryption

- External hard drives and USB devices containing personal or sensitive data are encrypted.
- All websites use HTTPS.
- Computers have encrypted hard drives.
- Personal data is encrypted in systems and/or storage media.
- Stored passwords are encrypted.
- Sensitive personal data is encrypted in relevant systems.

f) Technical security – Transmission control

- Guidelines for secure email usage are in place.
- Outgoing emails containing sensitive or private personal data are encrypted.
- Work email usage policies include rules for private use, appropriate use, encryption, and security.

g) Technical security – Availability and resilience

- System and server availability is secured through third-party agreements.
- Only authorized personnel may access in-house servers.
- Server rooms are equipped with smoke detectors and fire extinguishers.
- Air conditioning systems are in place.
- Data backup and recovery policies are defined.
- Backups are performed regularly (in-house or by vendor).
- Unauthorized access attempts trigger alarms.
- Uninterruptible power supply (UPS) is used.
- Temperature and humidity in server rooms are monitored.
- Breach response procedures are documented and reviewed annually.

3. Assistance to the Data Controller

3.1 The Data Processor shall, to the extent possible and within the scope described below, assist the Data Controller in accordance with Clauses 9.1 and 9.2 by implementing the following technical and organisational measures:

3.1.1 If the Data Controller receives a data subject request under applicable data protection law and the response requires assistance from the Data Processor, the Data Processor shall assist by providing necessary and relevant information and documentation, along with appropriate technical and organisational measures.

3.1.2 If the Data Controller requests help responding to a data subject, a written request must be submitted to the Data Processor. The Data Processor must provide the requested assistance 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 data subject request directly that relates to data processed on behalf of the Data Controller, it must be forwarded to the Data Controller without undue delay.

4. Retention Period / Deletion Procedure

4.1 Upon termination of the data processing service, the Data Processor shall delete or return all personal data in accordance with Clause 11.1, unless the Data Controller has changed its original decision after entering into these Clauses. Any such change must be documented and retained in writing, including electronically, with the Clauses.

5. Location of Processing

5.1 Processing of personal data covered by these Clauses may not take place at any other locations than the following, unless prior written approval has been obtained from the Data Controller:

5.2 At the Data Processor's own main offices and at the main offices of approved sub-processors, as listed in Annex B.

6. Instruction on the Transfer of Personal Data to Third Countries

6.1 Personal data shall only be processed by the Data Processor at the locations specified in Clause C.5. The Data Processor does not transfer personal data to third countries or international organisations.

6.2 To the extent personal data is transferred to third countries that have not been the subject of an adequacy decision under Article 45 of the GDPR, where both parties act as data controllers and the transfer is not subject to one or more of the derogations in Article 49, the legal basis must be the Standard Contractual Clauses (SCCs) set out in Annex E.

6.3 If the Data Controller has not provided a documented instruction in these Clauses or subsequently concerning the transfer of personal data to a third country, the Data Processor is not entitled to make such transfers within the scope of these Clauses.

6.4 Transfers of personal data may only take place as set out in these Clauses, on the instruction of the Data Controller, and only to the extent permitted by applicable data protection legislation.

6.5 If the transfer of personal data to third countries outside the EU/EEA is made by the Data Processor through its use of sub-processors, the Data Controller hereby authorises

the Data Processor to enter into the Standard Contractual Clauses adopted by the European Commission with such sub-processors on behalf of the Data Controller, provided that all applicable data protection requirements concerning transfers and processing are complied with.
If the Data Controller itself acts as a data processor and the Data Processor operates as a sub-processor in relation to the Data Controller's ultimate contractual party(ies), the Data Controller must obtain authorisation from the ultimate contractual party for the Data Processor to enter into the Standard Contractual Clauses.

6.6 Where the Data Processor, in accordance with these Clauses, transfers personal data subject to the agreement to sub-processors or independent data controllers located in third countries, the Data Processor shall ensure that the transfer complies with Chapter V of Regulation (EU) 2016/679.

6.7 By entering into this Data Processing Agreement, the Data Controller issues a documented instruction allowing the Data Processor to transfer personal data to third countries if this is necessary to fulfil the purpose of the processing and to allow the use of sub-processors, provided that a valid legal basis exists for such transfers (e.g. SCC 2021/914).

7. Procedures for the Data Controller's Audits, Including Inspections, of the Processing of Personal Data Entrusted to the Data Processor

7.1 Upon written request, the Data Processor shall document to the Data Controller that the Data Processor:

7.1.1 complies with its obligations under this Data Processing Agreement and the Instructions; and

7.1.2 complies with the provisions of the GDPR in respect of the personal data processed on behalf of the Data Controller.

7.2 The documentation referred to in Clause C.7.1 shall be provided to the Data Controller within a reasonable time after receipt of the request.

7.3 As evidence of ongoing compliance with the Clauses, the Data Processor shall make available internal control reports to the Data Controller. These reports must be prepared at least once a year and shall follow the principles and control objectives in the ISAE 3000 audit standard developed by FSR – Danish Auditors and the Danish Data Protection Authority (or alternatively other internationally recognised standards such as ISO/IEC 27701:2019).
The internal control reports may, at the Data Controller's discretion, be provided by way of information gathering and must be signed by the management of the Data Processor.
The Data Processor is not obligated to commission independent external audits but relies on the documented IT and data security provided by its hosting provider, Scannet A/S, which is subject to both ISAE 3402 Type II and ISO/IEC 27001:2017 certifications.
Upon request, the Data Processor shall provide relevant parts of such audit documentation to the Data Controller to demonstrate compliance with the Clauses.

7.4 Notwithstanding Clause C.7.3, the Data Processor shall, in addition, permit and contribute to audits and inspections once every 12 months, conducted by auditors appointed by the Data Controller, the public authorities of Denmark, or any other competent jurisdiction, insofar as necessary to verify that the Data Processor complies with the Clauses and applicable data protection law. The appointed auditor must be subject to confidentiality by law or agreement. The Data Controller must give at least 10 calendar days' written notice of any such audit.

8. Procedures for Audits, Including Inspections, of Sub-Processors

8.1 The Data Processor is responsible for supervising the sub-processors it uses by obtaining internal control reports based on the ISAE 3000 standard.
The Data Controller will be notified of any changes deemed relevant or significant for the processing of its data.

Annex D – Other Provisions Agreed Between the Parties

1. Limitation of Liability: The Parties agree that liability for indirect losses, including data loss and loss of profits, is excluded, unless such loss results from gross negligence or wilful misconduct.

2. Notification of Changes: The Data Processor is obligated to notify the Data Controller of material organisational or technical changes that may affect the data processing activities.

3. Specific Security Requirements: The Data Controller requires that access to certain data is subject to two-factor authentication.

4. Contact Information for Security Officer:
   Niels Arnold Lund
   Email: nal@board-office.dk

Annex E – Standard Contractual Clauses

This Annex contains the Standard Contractual Clauses (SCCs) which constitute the legal basis for the transfer and processing of personal data to third countries in accordance with Article 46(2)(c) and (d) of the GDPR.

If personal data is transferred to processors or sub-processors outside the EU/EEA, such transfer is made on the basis of the Standard Contractual Clauses adopted by the European Commission pursuant to Commission Decision 2021/914.
The following modules from SCC 2021/914 apply:

- **Module 2**: Transfer from controller to processor
- **Module 3**: Transfer from processor to processor

The Parties agree that the SCCs constitute the legal basis for data transfers to third countries under this Data Processing Agreement where such transfers are necessary, and they are accepted by the Parties upon acceptance of the Agreement.

The full text of the SCCs is available upon request from the Data Processor and can be accessed here:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0914