Data Processing Agreement

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 Controller"

and

BOARD OFFICE A/S
Jernbanegade 14
9000 Aalborg
DK
Company registration number: 28966237
hereinafter "The 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.

Table of contents

Appendix

1. Preamble

1.1 These Contractual Clauses (the Clauses) set out the rights and obligations of the Controller and the Processor, when processing personal data on behalf of the Controller.

1.2 The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR).

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

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

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

1.6 Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

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

1.8 Appendix C contains the Controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the Processor and how audits of the Processor and any sub-processors are to be performed.

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

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

1.11 The Clauses shall not exempt the Processor from obligations to which the Processor is subject pursuant to the General Data Protection Regulation (GDPR) or other legislation.

2. The rights and obligations of the Controller

2.1 The Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.

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

2.3 The Controller shall be responsible, among other, for ensuring that the processing of personal data, which the Processor is instructed to perform, has a legal basis.

3. The Processor acts according to instructions

3.1 The Processor shall process personal data only on documented instructions from the 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 Controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

3.2 The Processor shall immediately inform the Controller if instructions given by the Controller, in the opinion of the Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

4. Confidentiality

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

4.2 The Processor shall at the request of the Controller demonstrate that the concerned persons under the Processor's authority are subject to the abovementioned confidentiality.

5. Security of processing

5.1 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 Controller and Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The 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:

5.1.1 Pseudonymisation and encryption of personal data;

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

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

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

5.2 According to GDPR, Article 32, the Processor shall also – independently from the 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 Controller shall provide the Processor with all information necessary to identify and evaluate such risks.

5.3 Furthermore, the Processor shall assist the Controller in ensuring compliance with the Controller's obligations pursuant to GDPR, Article 32, by inter alia providing the Controller with information concerning the technical and organisational measures already implemented by the Processor pursuant to GDPR, Article 32, along with all other information necessary for the Controller to comply with the Controller's obligation under GDPR, Article 32.

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

6. Use of sub-processors

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

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

6.3 The Processor has the Controller's general authorisation for the engagement of sub-processors. The Processor shall inform in writing the Controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the 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 Controller can be found in Appendix B.

6.4 Where the Processor engages a sub-processor for carrying out specific processing activities on behalf of the 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 GDPR.

The processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the Processor is subject pursuant to the Clauses and GDPR.

6.5 A copy of such a sub-processor agreement and subsequent amendments shall – at the Controller's request – be submitted to the Controller, thereby giving the 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 Controller.

6.6 The Processor shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the Controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

6.7 If the sub-processor does not fulfil his data protection obligations, the Processor shall remain fully liable to the 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 Controller and the Processor, including the sub-processor.

7. Transfer of data to third countries or international organisations

7.1 Any transfer of personal data to third countries or international organisations by the Processor shall only occur on the basis of documented instructions from the Controller and shall always take place in compliance with Chapter V GDPR.

7.2 In case transfers to third countries or international organisations, which the Processor has not been instructed to perform by the Controller, is required under EU 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 information on important grounds of public interest.

7.3 Without documented instructions from the Controller, the Processor therefore cannot within the framework of the Clauses:

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

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

7.3.3 have the personal data processed by the Processor in a third country

7.4 The 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. Assistance to The Controller

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

This entails that the Processor shall, insofar as this is possible, assist the Data Controller in the Controller's compliance with:

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

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

8.1.3 the right of access by the data subject

8.1.4 the right to rectification

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

8.1.6 the right to restriction of processing

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

8.1.8 the right to data portability

8.1.9 the right to object

8.1.10 the right not to be subject to a decision based solely on automated processing, including profiling

8.2 In addition to the Processor's obligation to assist the Controller pursuant to Clause 5.3, the Processor shall furthermore, taking into account the nature of the processing and the information available to the Processor, assist the Controller in ensuring compliance with:

8.2.1 The 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;

8.2.2 The 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;

8.2.3 The 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);

8.2.4 The 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 Controller to mitigate the risk.

8.3 The Parties shall define in Appendix C the appropriate technical and organisational measures by which The Processor is required to assist the controller as well as the scope and the extent of the assistance required. This applies to the obligations forseen in Clause 8.1 and 8.2.

9. Notification of personal data breach

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

9.2 The Processor's notification to the Controller shall, if possible, take place within immediately and no later than 48 hours after the processor has become aware of the breach of the personal data security after the Processor has become aware of the personal data breach to enable the Controller to comply with the Controller's obligation to notify the personal data breach to the data protection agency, cf. GDPR, Article 33.

9.3 In accordance with Clause 8.2.1, the Processor shall assist The Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Processor is required to assist in obtaining the information listed below which, pursuant to GDPR, Article 33(3), shall be stated in the Controller's notification to the competent data protection authority:

9.3.1 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;

9.3.2 the likely consequences of the personal data breach;

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

9.4 The parties shall define in Appendix D all the elements to be provided by the Processor when assisting the Controller in the notification of a personal data breach to the competent data protection agency.

10. Erasure and return of data

10.1 On termination of the provision of personal data processing services, the Processor shall be under obligation to return all the personal data to the Controller and delete existing copies unless Union or Member State law requires storage of the personal data.

11. Audit and inspection

11.1 The Processor shall make available to the 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 Controller or another auditor mandated by the Controller.

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

11.3 The Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Controller's and Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Processor's physical facilities on presentation of appropriate identification.

12. The parties' agreement on other terms

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

13. Commencement and termination

13.1 The Clauses shall become effective on the date of both Parties' signature.

13.2 Both Parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

13.3 The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the Parties.

13.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Controller pursuant to Clause 10.1 and Appendix C.4, the Clauses may be terminated by written notice by either Party.

13.5 Signature:

On behalf of the Controller

On behalf of the Processor

14. The controller and the processor contacts/contact points

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

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

Contact information for The Controller:

Contact information for The Processor:
Niels Arnold Lund, nal@board-office.dk

Appendix A Information about the processing

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

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

In addition, the processing of personal data is carried out in order to fulfill the following purposes: The Data Controller wishes to use the Data Processor's board portal BOARD-OFFICE, which is an online portal containing a document repository, discussion forum, a planning tool, digital signature functionality, posting of board positions, as well as an inspiration section.
In addition, the Data Processor is responsible for the operation, testing, maintenance, development, and bug fixing of the Data Processor's applications.

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

2.1 The Data Processor processes the Personal Data in connection with the Data Processor's provision of the board portals BOARD-OFFICE and BOARD-PEOPLE.

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

3.1 password to one or several systems, address, username for one or several systems, e-mail, name, phone number, various personal data provided or recorded by the customer or the customer's customers without the organization's active processing and identification thereof

BOARD OFFICE
In connection with the use of the BOARD OFFICE platform, Personal Data is processed that is shared as part of document management, communication, and administration of board activities. This may include, among other things:

Identification information (name, email address, username, position, and affiliation with the organization)

Information contained in documents that are uploaded, processed, or shared via the platform, including, for
example, salary information, contractual information, minutes of meetings, financial materials, or other information relating to employees, management, or business partners

Correspondence and activity data (e.g., comments, votes, meeting participation)

Users may, at their own discretion—typically at the request of their organization or board—upload identification documents such as copies of a driver's license, passport, or health insurance card. In such cases, a copy thereof will only be made available to the relevant board, which shall thereafter be considered an independent Data Controller for the further processing of such information.

In addition to the specified Personal Data, further types of Personal Data may be processed depending on what the Customer chooses to share in its documents on the platform.

BOARD PEOPLE
In connection with the use of the BOARD PEOPLE platform, Personal Data is processed that the data subject chooses to provide when creating and maintaining their profile. This may include:

Identification information (name, contact details, title)

Profile information such as photo, presentation video, summary, and personal CV

Information regarding personal and professional resources, background, education, board education, networks, and references

Information regarding current and previous board positions, professional experience, board experience, and primary motivations for engaging in board work

4. Processing includes the following categories of data subject

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

5. The Processor's processing of personal data on behalf of the 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 Processor's services has been terminated, after which the personal data is either returned or erased in accordance with Clause 11. The 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 Controller authorises the engagement of the following sub-processors:

The Data Processor's sub-processors are listed in the currently applicable list of sub-processors, which can be accessed under the "Security" tab on our website (https://www.board-office.dk/sikkerhed), or under "Settings" within the individual portals.

1.2 The Processor has the Controller's general authorisation for the engagement of sub-processor(s) from the above list. The Processor shall specifically inform the Controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The Processor shall provide the Controller with the information necessary to enable the data exporter to exercise its right to object.

Appendix C Instruction pertaining to the use of personal data

1. The subject of/instruction for the processing

1.1 The Data Processor processes Personal Data on behalf of the Data Controller for the purpose of enabling the Data Controller to use the board portals BOARD-OFFICE and BOARD-PEOPLE, which are online portals containing a document repository, discussion forum, a planning tool, digital signature functionality, posting of board positions, as well as an inspiration section.

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 Processor must implement an appropriate leve of security.

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

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

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

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

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

a) All employees of the 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) Employees with access to sensitive personal data or critical IT systems have undergone a security clearance before they were employed.
d) The employees of the Processor that have access to "sensitive" personal information or critical IT systems have undergone a security clearance before they were employed.
e) The processing of personal data done by the employees of the Processor is logged and can be checked as required.
f) The Processor has an IT security policy.
g) The Processor has documentable process descriptions for breaches of the personal data security, which are reviewed at least annually.
h) The Processor has established procedures that ensure proper deletion or continuous confidentiality when the hardware is repaired, serviced, or disposed.
i) The Processor has the opportunity to respond to employees' breaches of the processor's data security or breach of instructions on the processing of personal data according to employment law.
j) The Processor's employees regularly document and report breaches of personal data security or risks thereof.

Home workplaces must be secured in a manner equivalent to workplaces within the data processing facilities. In cases where an employee makes use of home or remote workplaces, computers and other devices must never be left unattended without being locked or powered off. Two-factor authentication must be implemented to ensure that unauthorized persons cannot gain access to Personal Data. Access to the company's network resources, including access to systems, must take place via VPN.

The Data Processor shall ensure that all employees are instructed in relevant rules, in particular regarding information security and data protection. Furthermore, the Data Processor shall ensure that all employees receive ongoing awareness training on data security and thereby acquire knowledge of how to generally handle the processing of Personal Data, as well as the data protection risks associated therewith.

Technical security: Access to and protection of IT systems
The Processor shall implement the following technical security measures regarding access to and protection of IT systems:

a) The Processor has policies for password composition, including minimum requirements.
b) The Processor logs and controls unauthorized or repeated failed login attempts.
c) The Processor requires employees to use individual passwords.
d) The Processor uses antivirus programs that are updated regularly.
e) The Processor uses logical access control with username and password or other unique authorization.
f) The Processor's computers have automatic access protection during inactivity, ie. locked screen saver.
g) There are procedures for granting authorizations to IT systems when hiring new employees.
h) 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 on storage media where relevant and taking into account the nature of the processing and the Personal Data.

A firewall is implemented and continuously updated to maintain full protection.

Antivirus programs are implemented and continuously updated to ensure that both the program modules and system components maintain full protection.

The Data Processor's websites use HTTPS (Hyper Text Transfer Protocol Secure), ensuring that all communication over the open internet is encrypted peer-to-peer.

The Data Processor is obligated, on an ongoing basis and within a reasonable timeframe, to use vulnerability scanning tools and subsequently apply security updates to all devices and systems from which Personal Data is accessed.

Two-factor authentication (two-factor login) is used as a technical security measure when logging into the BOARD OFFICE and BOARD PEOPLE systems to ensure that only authorized users gain access to Personal Data and other data.

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

a) The Processor grants authorizations to individuals or groups of users to access, change and delete processed personal data.
b) The Processor has procedure(s) to restore data from backup.
c) The Processor has traceability of access, modification and erasure of data by individual users.
d) The Processor logs and controls unauthorized or repeated failed attempts to access data.
e) The Processor regularly reviews and verifies user authorizations for specific systems.
f) The Processor regularly reviews system controls.

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

a) Content on external hard drives and USB keys, etc. is encrypted when such media contain personal or sensitive personal information.
b) Passwords stored on the processor's computers, etc. are encrypted.
c) The network is encrypted.
d) The Processor encrypts personal data in systems and/or on devices.
e) The Processor encrypts sensitive personal data in systems and/or on devices.
f) The Processor's computers have encrypted hard drives.

g) The Processor's websites and web forms uses SSL certificates/HTTPS (Hyper Text Transfer Protocol Secure).

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

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

The Data Processor ensures that the applied TLS encryption always complies with the latest applicable minimum standards.

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

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

3. Assistance to the Controller

3.1 The Processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Controller in accordance with Clause 8.1 and 8.2 by implementing the following technical and organisational measures:

3.1.1 If the 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 Processor, the Processor shall assist the Controller with the necessary and relevant information and

documentation as well as appropriate technical and organizational security measures.

3.1.2 If the Controller needs the Processor's assistance in order to reply to a request from a data subject, the Controller must send a written requst for assistance to the Processor and the 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 Processor receives a request for the exercise of the rights pursuant to applicable data protection law from other persons than the Controller, and the request concerns personal data processed on behalf of the Controller, the Processor shall without undue delay forward the reuest to The Controller.

4. Storage period/erasure procedures

4.1 Upon termination of the license agreement, data will be retained for a period of 12 months following termination, after which the board and all associated data will be automatically deleted without further notice to the Customer. However, the Customer may request earlier deletion, in which case the Data Processor will carry out manual deletion within a reasonable timeframe. Deletion is performed in a manner that ensures that the data cannot be restored or reconstructed, in accordance with the Data Processor's security procedures and applicable data protection legislation.

With regard to individual user profiles, the associated Personal Data will be deleted upon written request from the Customer to the Data Processor (BOARD OFFICE A/S). Upon receipt of such a request, the Data Processor will carry out manual deletion of the relevant user profile and all associated data without undue delay and in accordance with the Data Processor's internal procedures for secure deletion. The Customer will receive written confirmation once the deletion has been completed. User profiles are automatically deactivated after 4 years of inactivity (since the last login) and are automatically deleted 1 year after deactivation.

5. Processing location

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

At the 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 Processor on the locations specified in clause C.5. Transfers to the United States occur on the basis of the data importer's

certification under the EU-U.S. Data Privacy Framework (see certified organizations here.)

6.2 If the 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 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 Controller and to the extent permitted by the applicable data protection law.

6.4 Where, in accordance with these clauses, The Processor transfers personal data to sub-data processors in third countries outside the EU / EEA, the 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 Processor's transfer to sub-processors, the Processor is by the provisions of the agreement authorized to enter into the standard contractual provisions adopted by the European Commission with the Processor's sub-processors on behalf of the Controller, provided that all the applicable rules regarding transmission and other processing of personal data are otherwise complied with. If the data controller itself is the 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 Controller must obtain authorization from the ultimate contracting party of the Processor in the standard contract terms.

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

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

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

7.3 The processor must provide the 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 controller's information gathering and must be signed by the

processor's management. The 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 Processor shall furthermore provide for and contribute to audits and inspections every 12 months, performed by auditors appointed by the Controller, the public authorities in the competent jurisdiction, to the extent necessary to verify the 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 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 shall conduct annual supervision of sub-processors by obtaining the sub-processor's own reports, management statements or similar documentation, certifications, or an audit report issued by an independent third party regarding the sub-processor's compliance with the General Data Protection Regulation, data protection provisions in other EU law or the national law of the Member States, and these Provisions.

The Parties agree that the following types of certifications and audit reports may be used in accordance with these Provisions:
ISAE 3000
ISAE 3402
ISO 27001
ISO 27701
SOC 2

The Data Processor is obligated to be able to document to the Data Controller that such supervision has been carried out.

Based on the results of the supervision, the Data Processor (and the Data Controller) shall be entitled to request the implementation of additional measures in order to ensure compliance with the General Data Protection Regulation, data protection provisions in other EU law or the national law of the Member States, and these Provisions.

If the sub-processor is unable to implement the additional measures required based on the supervision, the Data Processor shall be obligated to examine the possibility of replacing the sub-processor.

Furthermore, the Data Processor or a representative of the Data Processor shall have access to carry out inspections, including physical inspections, of the locations from which the sub-processor processes personal data, including physical premises and systems used for or in connection with the processing. Such inspections may be carried out when the Data Processor (or the Data Controller) deems it necessary.

Documentation of such inspections shall be submitted without undue delay to the Data Controller if the supervision reveals that a sub-processor is not deemed to be in

compliance with applicable requirements. In such cases, the Data Controller may challenge the scope and/or method of the inspection and request that a new inspection be carried out under different conditions and/or using a different method.

Any costs incurred by the Data Processor or the sub-processor in connection with a physical inspection of the sub-processor's premises shall not concern the Data Controller—regardless of whether the Data Controller has initiated or participated in such an inspection.

Appendix D The Parties' terms of agreement on other subjects

1. Other matters

1.1 The Data Processing Agreement does not regulate other matters.

Appendix E – Processing of Personal Data in connection with the use of BOARD Assistant™

This Appendix describes the Data Processor's processing of Personal Data in connection with customers' and users' use of BOARD Assistant™ (the "AI functionality") in the BOARD OFFICE™ and BOARD PEOPLE™ portals.

This Appendix forms an integral part of the Data Processing Agreement and specifies the purpose, data flows, processing activities, security measures, use of sub-processors, as well as the conditions for the Customer's choice of functionality, including the use of secure mode versus real-time search.

1. Purpose of the processing

1.1. The purpose of BOARD Assistant™ is to provide users with access to AI-supported functionalities that can support board work, document understanding, summaries, template assistance, agenda drafts, knowledge search, etc., all within a private, encrypted, and isolated environment where data does not leave the EU.

1.2. BOARD Assistant™ uses Microsoft Azure OpenAI in EU data centres.

1.3. BOARD Assistant™ is designed so that input data is not stored, not used for training, not logged outside the BOARD OFFICE platform, and not shared with other customers.

2. Nature of the processing and categories of data

2.1. BOARD Assistant™ only processes the data that the user actively inputs into the chat or AI functionality, as well as documents or text excerpts that the user chooses to submit for AI analysis.

2.2. Typically, the following Personal Data may be processed:

- Identification data included in board documents (name, title, etc.)
- Information contained in documents uploaded to BOARD OFFICE (e.g. contracts, minutes, financial statements, CVs, etc.)
- Information from BOARD PEOPLE profiles, if the user activates AI functionalities in BOARD PEOPLE
- Any other Personal Data that the user includes in their interaction with the AI functionality

2.3. BOARD Assistant™ does not carry out any automated decision-making or profiling that produces legal effects or similarly significant effects on individuals.

3. Technology, operation, and data storage

3.1. BOARD Assistant™ uses Azure OpenAI EU Standard Zone, where:

- All processing takes place within EU data centres
- Microsoft does not use customer data for training
- No logging or external querying of input data takes place
- Data is processed only transiently (not stored) within the AI engine

3.2. BOARD OFFICE only stores the data that the user chooses to save within the platform – AI input and AI outputs are not stored by Azure and are only stored by BOARD OFFICE if the user actively saves the content.

3.3. All communication between BOARD OFFICE and Azure OpenAI takes place via encrypted connections (TLS 1.2+) and through private endpoints.

4. Separation between operating environment and real-time search

4.1. BOARD Assistant™ is by default provided in a secure mode, where:

- No data leaves BOARD OFFICE or the Azure EU zone
- No searches are conducted in external sources or on the internet
- No real-time data is retrieved
- No processing ever takes place outside the EU/EEA

4.2. If the user activates the real-time search functionality:

- The user must actively opt in to the functionality
- The user receives an explicit warning that data may thereafter be processed outside the isolated environment
- Processing may take place outside the EU, depending on Microsoft's handling of search queries
- This functionality is considered a separate data processing choice and constitutes an instruction from the Data Controller

4.3. BOARD OFFICE logs the user's choice but never logs the content of individual queries.

5. Sub-processors

5.1. BOARD Assistant™ uses the following sub-processor:

- Microsoft Azure (EU data centres) – AI functionality

5.2. No additional sub-processors are used for the AI functionality.

5.3. When real-time search is activated, Microsoft's Bing infrastructure may be considered an additional processing chain – this use is only triggered by the Data Controller's/user's active instruction.

6. Transfers to third countries

6.1. In secure mode, all Personal Data is processed exclusively within the EU/EEA in Azure EU data centres.

6.2. When using real-time search, transfers to third countries will only occur if the user actively selects the functionality.

6.3. The Data Controller's activation of real-time search is considered a documented instruction regarding third-country transfers.

7. Security measures

7.1. BOARD Assistant™ is covered by the technical and organizational measures already described in Appendix C.

7.2. Specific AI-related security measures include:

- Use of private endpoints between BOARD OFFICE and Azure OpenAI
- Zero-data retention
- Encryption of all requests and responses in transit
- Model isolation, ensuring that data from one customer is never accessible to others
- No training, no caching, and no persistent storage in the AI environment

8. Assistance to the Data Controller

8.1. BOARD OFFICE assists the Data Controller in accordance with the Data Processing Agreement.

8.2. BOARD OFFICE can document:

- Whether a user has used secure mode or real-time search
- Whether a user has saved AI-generated content in the portal
- Relevant security logs relating to access and system operation

8.3. BOARD OFFICE cannot reconstruct AI queries, as these are not stored.

9. Deletion

9.1. As BOARD Assistant™ itself does not store Personal Data, there are no separate deletion rules.

9.2. AI-generated content that is saved in BOARD OFFICE is processed in accordance with the general deletion rules set out in the Data Processing Agreement.

10. Changes to instructions

10.1. The Data Controller may at any time choose to:

- Disable BOARD Assistant™
- Restrict usage to secure mode
- Allow or reject the use of real-time search
- Establish internal policies for its use

10.2. Changes are documented in the Customer’s settings and function as instructions.