STANDARD CONTRACTUAL CLAUSES

Version 1.7 á January 15. 2021

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

between

Customer:

_____

(**the Data controller or Customer**)

&

Assembly Voting ApS
Ringager 4C
2605 Broendby
Denmark
CVR nummer: 25600665 (**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.

Assembly Voting
Dedicated to democracy

1. TABLE OF CONTENTS

2. Preamble

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. 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).

3. In the context of the provision of the service described in the Main agreement, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

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

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.

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.

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.

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

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

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

3. The rights and obligations of the data controller

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[1] data protection provisions and the Clauses.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

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

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

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.

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.

3. If data controllers have issued an unlawful instruction to a data processor who, unknowingly, has performed the task under instruction - the data controller will indemnify against any financial implications thereof, such as fines from the Data Protection Authority.

5. Confidentiality

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.

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

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and 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:

a. Pseudonymisation and encryption of personal data;

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

c. the ability to restore the availability 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. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

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 Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

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

7. Use of sub-processors

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

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior specific written authorisation of the data controller.

3. The data processor shall engage sub-processors solely with the specific prior authorisation of the data controller. The data processor shall submit the request for specific authorisation at least 30 days prior to the engagement of the concerned sub-processor. The list of sub-processors already authorised by the data controller can be found in Appendix B.

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.

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.

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. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

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.

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.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization
    b. transfer the processing of personal data to a sub-processor in a third country
    c. have the personal data processed in by the data processor in a third country

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.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational 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:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.4., 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:

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

   b. 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;

   c. 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);

   d. the data controller's obligation to consult the competent supervisory authority, the Danish Datatilsyn, 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.

3. The parties shall define in Appendix C the appropriate technical and organisational 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. Remuneration and costs

1. The Data Processor is entitled to payment for time used and the Data Processor's other costs thereof, for the services performed according to the Data Processor Agreement at the request of the Data Controller. Services may include, but are not limited to: changes to the instruction, disclosure and deletion of information, assistance in auditing, assistance in termination, cooperation with supervisory authorities and assistance in complying with requests from data subjects.

2. he Data Processor is entitled to payment for time used, as well as the Data Processor's other costs, for the services performed under the Data Processor Agreement as a result of changes in the Data Controller's relationship. The benefits may include, but are not limited to, assistance with changes resulting from new risk assessments and impact assessments, as well as changes necessitated by changes in legislation. The remuneration is calculated according to the agreed hourly rates in agreement on delivery of the Main Services, and where no hourly rates have been agreed therein, as per the Supplier's applicable hourly rates.

11. Notification of personal data breach

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.

2. The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

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

    a. 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;

    b. the likely consequences of the personal data breach;

    c. 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.

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

12. Erasure and return of data

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

   The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

13. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

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.

14. The parties' agreement on other terms

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.

15. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

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.

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.

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.

5. Signature

If this DPA is signed in combination with a SaaS, there is no need to return a signed copy. Data Controller/Customer can just keep a copy.

On behalf of the data controller	On behalf of the data processor
Date:	Date: 15. January 2021
Place:	Place: Broendby
Customer:	Assembly Voting:
	Camilla Banja
Name:	Name: Camilla Banja
Position:	Position: CBO and DPO
Phone:	Phone: +45 27591201
E-mail:	E-mail: camilla@aion.dk

16. Data controller and data processor contacts/contact points

1. The parties may contact each other using the below contact point:

Company:	Assembly Voting ApS
Name:	Camilla Banja
Position:	COO and DPO for Assembly Voting
Phone:	+45 27591201
E-mail:	camilla@aion.dk

In case of need to contact customer, the customers admins for the organisation will be contacted through backend message system of Assembly Conference Voting.

Appendix A Information about the processing

1. PURPOSE

1.1. The parties have entered into a SaaS agreement on use of the Application Assembly Conference Voting. In this connection, the Data Processor processes the Data controller's data.

1.2. The data processing activities consist of storing personal data in the application for the use of the applications authentication and communication to Conference participants.

2. TREATMENT

2.1 The data processor only receives data and only processes within the scope of the purpose, cf. clause 1.1 and 1.2 above. It is the responsibility of the Data controller not to upload data not necessary for the purpose.

Appendix B Authorised sub-processors

B.1. Approved sub-processors
On commencement of the Clauses, the data controller authorizes the engagement of the following sub-processors:

Amazon Web Services EMEA SARL
38 Avenue John F., Kennedy, L-1855, Luxembourg
We Use Amazon for our Hosting of Assembly Voting Conference Cloud solution
We use Amazon hosting service in Europe for an encrypted backup from our servers as well as log files.
Backup and log is stored in Amazon hosting center in Stokholm.
Amazon AWS has ISO 27001, ISO 27017 and ISO 27018 certifications.

Peytz
CVR-nr.: 12692 3549
Address: Rentemestervej 56C, 2400 København NV
Country: Danmark
We send emails through Peytz mails
Peytz operates our physical servers and delivers hosting facilities to Assembly Voting.

Compaya A/S,
CVR-nr: 31375428
Address: Palægade 4, 2. tv,, 1261 København K.
Country: Denmark
Service used for sending SMS.

B.2. Prior notice for the authorisation of sub-processors
The Data Processor shall notify the Data Controller in writing of the addition or replacement of a Sub-Processor prior to commencement of use. Similarly, The Data Processor must notify the Data Controller of discontinuance of use of a Sub-Processor.

The Data Controller cannot refuse to approve the addition or replacement of a Sub-Data Processor unless there is a concrete justification for this and must give such objection within 30 days.

Appendix C Instruction pertaining to the use of personal data

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the in this appendix listed.

C.2. Security of processing
The processing involves a larger amount of personal data covered by Article 9 of the Data Protection Regulation and therefore a high level of security must be established.

1. Technical measures

1.1. **Password security and complexity**
Unique user IDs are used and passwords and password parameters meet minimum requirements (e.g. minimum length of 12 characters, recommended complexity and lockout).

1.2. Password protection

All systems / applications enforce access to the user password file to prevent user account compromise. All passwords are stored in an encrypted form so that they cannot be opened or read. When changing or verifying network passwords, the system must ensure that only hashed versions of the password are compared. The hashed version is used and not plain text passwords.

1.3. Physical security

The premises are protected by physical access controls, which limit the risk of unauthorized access. Operating systems used for data processing are run from premises that are protected from damage caused by physical conditions such as fire, water damage, power failure, theft or vandalism.

1.4. Encryption

Forced TLS 1.2 encryption is used when data is transmitted electronically.

1.5. Firewall

Firewall has been implemented on all systems used to process or store personal data.

1.6. Backups

The data processor ensures that personal data is backed up regularly. The backups are stored safely and so that backups are not lost in the event.

1.7. Equipment disposal

It is ensured that effective deletion of personal data occurs before the disposal of electronic equipment.

1.8. Log

All SSH logins for our servers are logged and an audit report can be made from the system.

1.9. General system security

The systems are built around "data protection and privacy by design". Examples of our measures are:

-Minimization of personal data processing
-Encryption of data in transit and rest,
-Security of the infrastructure against unauthorized intrusion.

1.10. SMS

No sensitive personal data or information surrounded by special legislation should be sent via SMS, as this is seen as an unsafe media.

2. Organizational measures

2.1. Information Security Committee

A Committee on Information Security has been established, which meets quarterly and, in addition, as needed to discuss and form the basis for IT policies, which are submitted for approval at management meetings. The policies are communicated to relevant employees as an instruction for data processing and systems and processes are adapted based on the approved policies.

2.2. Training of employees

Employees who participate in the processing of personal data receive periodic training / training, so that they are aware of the personal data regulation and their role. Employees need to know the purpose and workflow of data processing and to ensure that employees are kept informed of their duty of confidentiality.

2.3. User Accounts

All accounts used for access, applications, and networks are uniquely identifiable to a named person to ensure traceability.

2.3.1. Creating, modifying and deleting accounts

All new employee accounts must be formally requested and approved. Documentation is kept for all accounts. The data processor ensures that an appropriate background check is made for all personnel who, during their employment, will have access to personal data covered by the data processing agreement.

Particular attention is paid to third parties and temporary accounts that may have been created for the installation of new applications. In such circumstances, it is ensured that:

- All redundant and unnecessary third party accounts have been deleted and
- Any third-party accounts required for ongoing support have been disabled and enabled for specific support sessions only, and
- Documentation for creation and approval must be available for at least one year.

2.3.2. Periodic review of accounts

Periodic reviews of administrative accounts are performed to ensure that all administrative accounts on systems are approved, eligible and that any redundant accounts are deleted.

2.3.3. Administrative accounts

Administrative accounts are highly privileged and must be subject to the following additional controls:

- All highly privileged and high-risk account activities must be logged wherever possible and their use reviewed regularly.
- Creation documentation is kept for a minimum of 1 year
- Limited to a minimum number of authorized users.

C.3. Assistance to the data controller

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 conducting necessary impact assessments and consultations in accordance with Article 35 of the Personal Data Regulation.

C.4. Storage period/erasure procedures

1. Deletion of data

1.1. Data is deleted 30 days after ended service. The request for deletion is notified 14 days before deletion. Postponement can only be made on valid Customer's grounds and may imply a further cost.

1.2. Logs files are stored for 24 months.

1.3. Encrypted backup files from servers are stored for 6 months.

C.5. Processing location

1. Locations

1.1. The processing and / or retention of Personal Data under the Data Processing Agreement can/will take place from the following locations:

Assembly Voting ApS
Ringager 4C, 1 th.
2605 Brøndby
DK Denmark

Amazon Web Services EMEA SAR
38 Avenue John F., Kennedy, L-1855, Luxembourg
Stockholm datacenter
Sweeden

Peytz A/S
Rentemestervej 56C,
2400 København NV
Danmark

Compaya A/S,
Palægade 4, 2. tv,,
1261 København K.
Denmark

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

1.1 The Data Processor may NOT, without the written consent of the Data Controller, process, including export to and retention of, Personal Data outside the European Union / EEA, including via sub-data processors.

1.2 The requirement in clause 3.1 for instructions includes, that the Data Processor may only transfer Personal Data to a third country or an international organization (as defined in the Personal Data

Regulation), upon instruction, unless transfer is required under EU law or EU law, national law of the Member State to which the Data Processor may be subject; in this case, the Data Processor must notify the Data Controller of this legal requirement prior to processing unless the right in question prohibits such notification for the sake of important societal interests.

1.3 If the Data Controller has approved the transfer to a third country, the Data Processor must ensure the necessary and valid legal basis for the transfer. An example could be the use of valid EU Commission standard contracts.

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

1.1 The data processor shall make available to the data controller all information necessary to demonstrate the data processor's compliance with Article 28 of the Data Protection Regulation and this agreement and shall provide and contribute to audits, including inspections carried out by the data controller or another auditor, is authorized by the data controller.

1.2 The data controller or a representative of the data controller has the right to supervise, including physical supervision of the data processor, when, in the opinion of the data controller, a need arises. Requests for supervision must be made at least 30 days' notice

1.3 The data controller's supervision of any sub-data processors is normally done through the data processor. The data controller can choose to initiate and participate in a physical inspection at the sub-processor. The possible involvement of the data controller in a sub-processor supervision does not change the fact that the data processor also has full responsibility for compliance with the data protection law and this data processing agreement by the sub-processor. "

1.4 The data processor is obliged to grant access to the data processor's physical facilities for proper identification by authorities who, under applicable law at any time, have access to the data controller's and data processor's facilities, or representatives acting on behalf of the authority.

1.5 Note that a ISAE3000 Type 1 is available from 17/12-2019 and a yearly ISAE3000 Type 2 will be available from February 2021.