Deloitte

Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR-no. 33 96 35 56
Weidekampsgade 6
P.O. Box 1600
0900 Copenhagen C
Denmark

Phone +45 36 10 20 30
Fax +45 36 10 20 40
www.deloitte.dk

Assembly Voting ApS

Independent auditor's ISAE 3000 type 1 assurance report on information security and measures pursuant to the data processing agreement with clients using Assembly Voting as of December 17, 2019.

Table of contents

1. Independent auditor's report 3

2. Management's statement 6

3. Description of processing 8

4 Assembly Voting's control objectives, controls, test, and results 14

1. Independent auditor's report

To: Assembly Voting ApS and Assembly Voting ApS' clients who have used the services described.

Scope

We have been engaged to provide assurance about Assembly Voting ApS' (hereinafter "Assembly Voting") description in section 3 of the described services in accordance with the data processing agreements with Assembly Voting as of December 17, 2019 (hereinafter "the description"), and about the design and implementation of controls related to the control objectives stated in the description.

Assembly Voting is using the following sub-data processors:

- Bech - (Physical attribution)
- Peytz - (Email attribution)
- Compaya – (SMS service)
- Amazon – (Storage of logs and backups).

The description provided by Assembly Voting in section 3 of this report does not include control objectives and supporting controls at the sub-data processor.

Some of the control objectives presented in the description provided by Assembly Voting can only be achieved if complementary controls at the data controllers are implemented and are working effectively. This report does not include the design, implementation and operating effectiveness of such complementary controls.

Assembly Voting's responsibilities

Assembly Voting is responsible for preparing the Description and the accompanying statement in section 2, including the completeness, accuracy, and method of presentation of the description and the statement; providing the services covered by the description; stating the control objectives; and designing and implementing controls to achieve the stated control objectives.

Auditor's independence and quality control

We have complied with the requirements for independence of the Code of Ethics for Professional Accountants issued by FSR - Danish Auditors (Code of Ethics for Professional Accountants), which are based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional conduct.

We are subject to the International Standard on Quality Control (ISQC 1) and accordingly uses and maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on Assembly Voting's description and on the design and implementation of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information", and additional requirements under Danish audit regulation. That standard requires that we plan and perform

our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design, and implementation of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its services, and the design and implementation of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or implemented. Our procedures included testing the design and implementation of controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved as per the audit date.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in section 2.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at a data controller

Assembly Voting's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of control that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the controls to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Management's statement section. In our opinion, in all material respects:

(a) The description fairly presents the services provided as designed and implemented as of December 17, 2019;
(b) The controls related to the control objectives stated in the description were suitably designed and implemented as of December 17, 2019.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in section 4 of this report.

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for data controllers who have used Assembly Voting's services who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard

to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with.

Copenhagen, January 8, 2020

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR No. 33 96 35 56

Thomas Kühn
Partner, State-Authorized Public Accountant

Michael Bagger
Director, CISA

2. Management's statement

Assembly Voting processes personal data for our clients in accordance with the data processing agreements.

The accompanying description has been prepared for the customers who have used the services described in this report, and who have a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with. Assembly Voting confirms that:

a) The accompanying description in section 3 fairly presents the services delivered as part of which we have processed personal data for data controllers subject to the Regulation as of December 17, 2019. The criteria used in making this statement were that the accompanying description:

   (i) Presents how the services delivered were designed and implemented, including:

   - The types of services provided, including the type of personal data processed;
   - The procedures, within both information technology and manual systems, used to initiate, record, process, and, if necessary, correct, delete, and restrict processing of personal data;
   - The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the data controller;
   - The procedures ensuring that the persons authorized to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
   - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation;
   - The procedures supporting, in the event of a breach of personal data security, that the data controller may report this to the supervisory authority and inform the data subjects;
   - The procedures ensuring appropriate technical and organizational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
   - Controls that we, in reference to the scope of the delivered services, have assumed would be implemented by the data controllers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description;
   - Other aspects of our control environment, risk assessment process, information system (including related business processes) and communication, control activities, and monitoring controls that are relevant to the processing of personal data.

   (ii) Includes relevant information about changes in the data processor's services in the processing of personal data as of December 17, 2019.

   (iii) Does not omit or distort information relevant to the scope of the services being described for the processing of personal data while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of control that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively as of December 17, 2019. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified,

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, as of December 17, 2019.

c) Appropriate technical and organizational safeguards were established and maintained to comply with the agreements with the data controllers, sound data processing practices, and relevant requirements for data processors in accordance with the Regulation.

Vallensbæk, January 8, 2020
On behalf of Assembly Voting

Jacob Gyldenkærne
CEO

3. Description of processing

The parties have agreed on Assembly Voting's assistance in connection with one or more of the following services. The established controls cover all of the processes and services mentioned below:

1. Election using: AVX - Voting system
2. Election using: Votes - Voting system
3. Election using: Cards - NemID login module for Votes
4. Candidate line-up or nomination process using: AV Candidate System
5. Online Meeting Management Tool: Meetings / "Borgerforslag"
6. Customer-managed support module using: Phoner
7. Customer-controlled trust-representative module using: TR module
8. Support, information and dialogue related to the above three areas using internal support module, as well as sharing personal sensitive data using AV Upload.

In this connection, the Data Processor must receive, process and store information about the data controller's stakeholders.

The data processing activities consist in particular of receiving data, enrichment, upload in systems and storing personal data until deletion.

The parties have entered into a separate agreement ("the Main Agreement") on the delivery of the Services ("the Services"), which are described in Appendix 1, point 1.1 of the Data Processor Agreement.

As part of Assembly Voting ApS' provision of the Services to the Data Controller in accordance with the Main Agreement, it is necessary that Assembly Voting ApS, on behalf of the Data Controller, processes the types of personal data described in Appendix 1, point 3 of the Data Processing Agreement.

This Data Processor Agreement with Appendix (the "Data Processor Agreement") establishes the rights and obligations of the Data Controller and the Data Processor respectively in relation to the Data processor's processing of Personal Data.

The personal data processed by the Data Processor on behalf of the Data Controller in connection with the provision of the Services to the Data Controller in accordance with the Main Agreement is referred to in the Data Processing Agreement as "Personal Data".

The data processing agreement is concluded to meet the requirements for data processors and data processing agreements, as set out in the "data protection regulation".

The nature of processing

The data processor's processing of personal data on behalf of the data controller is primarily about:

- Receiving personal data
- Enrichment of personal data
- Storing personal data
- Upload in Assembly Voting's systems for the solution of the services purchased in the main agreement
- Deleting data.

Personal data

The type of personal data being processed varies from task to task. The type is defined in the data processor agreement. Data controllers are only asked to share the agreed information.

- Personal information typically contains **common personal information**, including identification information such as name and address, telephone and email or e.g. customer number or identification.

- Personal information often contains other **sensitive personal information**, including information on social security numbers.
- Personal information may contain **special categories of sensitive personal information** such as trade union membership.

Typically, categories of registered persons covered by the data processing agreement include the data controller's customers, members or citizens

System overview

IT systems are considered, after the employees, as the most critical resource for Assembly Voting ApS. Emphasis is therefore placed on reliability, quality, compliance with regulatory requirements and on the user-friendliness of the systems, without unnecessarily cumbersome security measures.

Assembly Voting systems are designed to meet both legal requirements and academic recommendations in the field.

- AVX (Assembly Voting X) - Voting system with extra high security in the election process
- Votes - Digital voting system
- Cards - NemID login module for Votes
- Candidate system - Nominating and nomination system and presentation site with candidate validation
- Meetings/"Borgerforslag"/"Nem Generalforsamling" - system based on NemID for validation of participation rights.
- Upload - Upload is Assembly Voting's secure file sharing tool.
- Phoner - Customer-oriented support module where supporters cannot see CPR numbers or election codes, but look up e.g. member number or address and send an election code to the voter via email or SMS.
- Trust Representative Module - Module for sending link to participate in elections
- Scanner module for scanning letter votes
- Campaign monitor (mail system) - typically contains nothing but name and email.

Risk assessment

Risk assessment is divided into the following sub-processes:

Process	Risk assessment	Risk described	Preventive measures
Receiving data Enrichment and storage of data	Medium	Customers can send personal data over e-mail, despite instructions to use secure upload link. Mail could go wrong, which involves a risk.	Educate customers that we have a policy of refusing to use data received in this way and request a new action via secure upload link.
Enrichment and storage of data	Low to medium	Risk of new employee not deleting local data on PC despite instructions.	We ask each other if we have cleaned up on the local machines before we go home. Local data are according to instructions saved in the download folder, which is emptied before we leave work.
Protection of personal data in active systems	Low	Hacker attacks could theoretically happen.	Servers are protected as much as possible with the latest certificates.

Process	Risk assessment	Risk described	Preventive measures
Sharing with subcontractors	Low	Potential sub-data processor who has no control over data.	We only use approved subcontractors with relevant certifications and documented security processes.
Deleting data	Medium	Data are not deleted from systems.	There is a task in each project in Teamwork to delete data from relevant systems (which systems data should be deleted from is specified in the task). The project cannot be closed and archived until data are deleted. The upload folder has an expiration date and sends notifications when the scheduled deletion date is reached.

Practical measures

Assembly Voting takes the following technical and organizational security measures when processing personal sensitive information. The security measures apply to all systems that may have an impact on the processing of personal data.

Procedures and controls are complied to ensure that:

A. Instructions regarding the processing of personal data are complied with the entered data processing agreement

B. The data processor has implemented technical measures to ensure relevant processing security.

1. Server environments
   a. Data are stored at Hetzner. Hetzner is ISO 27001 certified, which means that they live up to one of the most recognized IT security standards

2. Exchange of data with Data Manager or authorized sub-processor on secured connections.
   a. Data controllers or sub-processors receive an upload link from Assembly Voting ApS. Prior to receipt, a folder for receiving a temporary expiration date is issued by Assembly Voting ApS.
   b. Data managers upload data in a dedicated directory on the Assembly Voting ApS web server, the link can only be used once. The connection is encrypted via TLS.

3. Physical security
   a. 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 which are protected against damage caused by physical conditions such as fire, water damage, power failure, theft or vandalism.

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

b. Creating, changing and deleting accounts: All new employee accounts are requested and approved by admin. Documentation is kept for all accounts.
c. Assembly Voting 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 Processor Agreement. Particular attention is paid to third parties (for example, customers and partners) and temporary accounts.
d. Authentication principles are using "Devise" as an authentication solution for Rails. See more here: https://github.com/plataformatec/devise

5. Periodic review of accounts
   a. Periodic reviews of administrative accounts are performed to ensure that all administrative accounts on systems are approved, legitimate and that any redundant accounts are deleted. This is a regular item on the agenda of the periodic meetings of the IT Security Committee.

6. Generic accounts
   a. All user accounts for AV systems are unique and private, and instructions are given that they should not be shared due to loss of traceability.

7. Super admin accounts
   a. All highly privileged and high-risk account activities are logged on a continuous basis where possible and their use is reviewed regularly.
   b. Creation documentation is kept for a minimum of 1 year
   c. Is limited to a minimum number of authorized users.

8. General system security
   a. The systems are built around a common data security custom and "data protection/privacy by design"
   i. Examples of our measures are:
      1. Minimizing personal data processing
      2. Encryption of data in transit
      3. Securing the infrastructure against unauthorized intrusion.

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

C. The data processor has implemented the following organizational measures to ensure relevant processing security.

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

2. Employees receive instruction on data processing via ad hoc workplaces and mobile equipment, including guidelines for its use, and establish the necessary security measures in connection therewith.

D. Personal information is deleted or returned if agreed with the data controller.

1. Data are deleted after 30 days, unless the data controller has requested otherwise with a reasoned delay. A new date for deletion is added to the Upload folder, as well as the reminder set in the Teamwork Project Management tool.

E. The data processor alone stores personal information in accordance with the data controller agreement.

1. Downloading data as well as local data enrichment by Assembly Voting employee.

a. Approved employees at Assembly Voting ApS download data to a local PC. MacBooks are used with automatically updated OS, as well as hard disk encryption. The employee enriches data, typically with e.g. election code and user ID reference number.
b. All computers have keypad lock and system logoff after an appropriate period of inactivity. Access to the system, application, or workstation is re-authorized only after properly entering the user's username / password.
c. Unique user IDs are used for all system passwords and passwords, and password parameters contain at least 12 characters, and employees are encouraged to generate a password through 1password.
d. All passwords are stored in a one-way encrypted form so that they cannot be opened or read.
e. Data processed on local PC is placed in download folder. After enriching and working with data, as well as uploading the enriched file via the safe AV Upload, data are deleted locally on the employee's machine from the download folder.
f. After enriching and working with data, Upload is used to put the enriched file in the safe AV Upload.
g. Data are uploaded to the systems required for the task with minimum required person sensitive information.

F. Only approved sub-data processors are used

1. If data are to be shared e.g. with physical attribution partner or email sender, this is shared over upload by a download link, which can be used once or through other secure connection required by subcontractor. Sub-contractors such as e-Box, KMD, Strålfors and Bech have different standards.

G. The data processor only transfers personal data to third countries or international organizations in accordance with the agreement with the data controller on the basis of a valid transfer basis.

1. The Data Processor may NOT, without written consent of the Data Controller, process including export and retain Personal Data outside the European Union / EEA, this includes transfer via sub-data processors.

2. 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 a national law of an EU 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 before processing, unless the court concerned prohibits such notification for the sake of important societal interests.

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.

G. The data processor may assist the data controller with the provision, correction, deletion or limitation of information on the processing of personal data to the data subject.

1. Notification of deletion and deletion of data.
    a. About 14 days after the election, data controllers are notified by email of permission to delete the data. Data processor chase data-controller until we have approval.
    b. Data are deleted after 30 days, unless the data controller has requested otherwise with a reasoned delay. A new date for deletion is added to the Upload folder, as well as the reminder set in the Project Management tool Teamwork.

H. Any security breach may be handled in accordance with the data processing agreement.

1. The data processor shall notify the data controller of any breach of the personal data security without undue delay and no later than 48 hours, after being informed of the data security breach of the data processor or a sub-processor, inform the data controller of violations or suspected of violating the rules on the processing of Personal Data (the Personal Data Regulation, etc.), including breaches of the personal data security. The data controller must also be notified of any disruptions or other irregularities if these have an impact on the processing of the Personal Data. The notification requirements also apply in relation to any breaches, etc. at sub-processors.

2. In the event of a breach of the personal data security, the Data Processor must gather/prepare and immediately after the breach submit all relevant documentation to the Data Controller regarding the facts of the breach, including:
   a. document/describe the nature of the breach of the personal data security, including, if possible, the categories and approximate number of data subjects affected, as well as the categories and approximate number of personal data records affected;
   b. describe as far as possible the likely effects/consequences of the breach of personal data security; and
   c. document the measures taken by the Data Processor, or describe the measures proposed by the Data Processor to deal with the breach of personal data security, including, where appropriate, measures to mitigate its potential adverse effects. The latter measures must be documented when taken.

3. 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 the obligations under Article 34 of the Personal Data Regulation on notification of personal data breaches to the data subjects.

Please refer to section 4, which describes the actual control activities.

Complementary controls at the controller

The data controller has the following obligations:

1. To ensure that personal sensitive data are sent on secure connection
2. To ensure that only agreed and necessary data are sent and received
3. Ensure approval of data being deleted 30 days after completion and approved election, subject to reasoned postponement at the request of the data controller.
4. To ensure that the instructions are lawful in relation to the personal data regulation applicable at all times.
5. That the instruction is appropriate in relation to this data processing agreement and the main performance.

4 Assembly Voting's control objectives, controls, test, and results

Introduction

This report is intended to provide the data controllers with information about the controls at Assembly Voting that may affect the processing of personal data, and to provide the data controllers with information about the design and implementation of the controls that were tested.

This report, when combined with an understanding and assessment of the controls at the data controllers, is intended to assist the data controllers in assessing the risks related to the processing of personal data that may be affected by the controls at Assembly Voting.

Our testing of Assembly Voting's controls was limited to the control objectives and related controls listed in the matrices in this section of the report and did not include all controls described in the system description, nor controls that may be in place at the data controllers. It is the responsibility of the data controllers to evaluate this information in relation to the controls in place at each data controller. If certain complementary controls are not in place at the data controller, Assembly Voting's controls may not compensate for such weaknesses.

Test of controls

The test of controls performed involves one or more of the following methods:

Method	Description
Interview	Interviews with selected personnel at Assembly Voting.
Observation	Observation of the execution of controls.
Inspection	Review and evaluation of policies, procedures and documentation of the performance of the control. This includes reading and evaluating reports and other documentation to assess whether specific controls are designed and implemented. Furthermore, it is assessed whether controls are monitored and supervised adequately and at appropriate intervals.
Re-performance	Repetition of the relevant control to verify that the control functions as intended.

Control objectives, controls and test results

The following matrices state the control objectives and controls tested, and present the audit procedures performed and the results thereof. If we identified material control weaknesses, we have described them as well.

Control objective A **Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied consistently with the data processing agreement entered into.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
A.1	Assembly Voting has developed a standard data processing agreement which is concluded with all customers using the Assembly Voting service. Assembly Voting has written procedures in place, as well as a data processing agreement which includes the requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis as to whether the procedures should be updated.	Deloitte has checked by way of inspection that formalized procedures are in place to ensure that personal data are only processed according to instructions. Deloitte has checked by way of inspection that the procedures include a requirement to assess at least once a year the need for updates, including changes in the data controller's instructions or changes in the data processing. Deloitte has checked by way of inspection that procedures are up to date.	No exceptions noted.
A.2	The data processing agreement entered into by Assembly Voting and the customer states that Assembly Voting only processes personal data indicated in the instructions from the data controller.	Deloitte has checked by way of inspection that Management ensures that personal data are only processed according to instructions.	No exceptions noted.

Control objective A **Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied consistently with the data processing agreement entered into.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
A.3	Assembly Voting immediately informs the data controller if an instruction, in the data processor's opinion, infringes the contract concluded, the Regulation, or other European Union or Member State data protection provisions. In addition, Assembly Voting informs the data controller if a data subject contacts them regarding data processing. Assembly Voting ensures that the data controller has a legal basis for processing the personal data of the data subject.	Deloitte has checked by way of inspection that formalized procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation. Deloitte has checked by way of inspection that procedures are in place for informing the data controller of cases where the processing of personal data is considered to be in breach of legislation. Deloitte has checked by way of inspection that the data controller was informed in cases where the processing of personal data was considered to be in breach of legislation.	No exceptions noted.

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant security of processing.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
B.1	Assembly Voting has developed a standard data processing agreement which is concluded with all customers using Assembly Voting services. Assembly Voting has written procedures in place which include a requirement that agreed safeguards are established for the processing of personal data in accordance with the agreement with the data controller. Furthermore, the technical and organizational measures in place are described in the internal policies. Assessments are made on a regular basis as to whether the procedures should be updated.	Deloitte has checked by way of inspection that formalized procedures are in place to ensure establishment of the agreed safeguards. Deloitte has checked by way of inspection that procedures are up to date. Deloitte has checked by way of inspection that the agreed safeguards have been established for the latest sample of data processing agreements.	No exceptions noted.
B.2	Assembly Voting has performed a risk assessment and, based on it, implemented the technical measures considered relevant in terms of achieving an appropriate level of security, including establishment of the safeguards agreed with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Deloitte has checked by way of inspection that formalized procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. Deloitte has checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data. Deloitte has checked by way of inspection that the data processor has implemented technical measures ensuring an appropriate level of security consistent with the risk assessment. Deloitte has checked by way of inspection that the data processor has implemented the safeguards agreed with the data controller.	No exceptions noted.

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant security of processing.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
B.4	External access to systems and databases used by Assembly Voting in the processing of personal data takes place through a secured firewall.	Deloitte has checked by way of inspection that external access to systems and databases used in the processing of personal data takes place only through a secured firewall. Deloitte has checked by way of inspection that the firewall is configured in accordance with the relevant internal policy.	No exceptions noted.
B.6	Access to personal data in Assembly Voting and the underlying databases is restricted to users with a work-related need for such access.	Deloitte has checked by way of inspection that formalized procedures are in place for restricting users' access to personal data. Deloitte has checked by way of inspection that formalized procedures are in place for following up on users' access to personal data being consistent with their work-related needs. Deloitte has checked by way of inspection that the agreed technical measures support retention of the restriction in the users' work-related access to personal data. Deloitte has inspected the latest sample of users' access to systems and databases and checked that such access is restricted to the employees' work-related needs.	No exceptions noted.

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant security of processing.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
B.7	For the systems and databases used for the processing of personal data, system monitoring with alarms has been established. The monitoring includes: • Exception alarm is sent to exceptions@aion.dk • Server locations are monitored at Hetzner • By default, PM tool Teamwork has a task of notifying customers that we want to delete data and a last deletion date. • The file upload system (AV Upload) prompts an expiry date when creating a new folder for sensitive data.	Deloitte has checked by way of inspection that system monitoring has been established with an alarm feature for systems and databases used in the processing of personal data. In one alarm sample Deloitte has checked by way of inspection that this was followed up on, and that the data controllers were informed thereof as appropriate.	No exceptions noted.
B.8	Assembly Voting has implemented TLS encryption for the transmission of confidential and sensitive personal data. Data are only exchanged via the secure File Upload System (AV Upload).	Deloitte has checked by way of inspection that formalized procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognized algorithm. Deloitte has checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet.	No exceptions noted.
B.9	Logging of the following matters has been established in systems where personal data can be accessed: • Data access and actions performed by system administrators and users with extended access rights; • Changes to security settings; • Logon information.	Deloitte has checked by way of inspection that logging has been activated as described. Deloitte has checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.	No exceptions noted.

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant security of processing.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
B.10	Personal data used for development, testing or similar activity are always in pseudonymized or anonymised form. Assembly Voting has formalised procedures which states that development, testing or similar activity are performed with test data.	Deloitte has checked by way of inspection that formalized procedures exist for using personal data for development, testing, or similar activities to ensure that such use only takes place in a pseudonymized or anonymized form. Deloitte has inspected a sample of one technical change and ensured that the activity in regard to development is performed using test data.	No exceptions noted.
B.11	Changes to Assembly Voting's systems and databases are made consistently with the procedures in place that ensure maintenance using relevant updates and patches, including security patches.	Deloitte has checked by way of inspection that formalized procedures exist for handling changes to systems, databases, or networks, including handling of relevant updates, patches and security patches. Deloitte has inspected extracts from technical security parameters and setups to check that systems, databases, or networks have been updated using the agreed changes and relevant updates, patches and security patches.	No exceptions noted.

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to ensure relevant security of processing.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
B.12	A formalized procedure is in place for granting and removing users' access to personal data in Assembly Voting's systems and databases. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	Deloitte has checked by way of inspection that formalized procedures exist for granting and removing users' access to systems and databases used for processing personal data. Deloitte has inspected the latest sample of employees' access to systems and databases and checked that the user access granted had been authorized, and that a work-related need exists. Deloitte has inspected the latest sample of resigned or dismissed employees and checked that the access to systems and databases was deactivated or removed on a timely basis. Deloitte has checked by way of inspection that documentation exists that user access granted is evaluated and authorized on a regular basis.	No exceptions noted.
B.14	Physical security measures are in place for securing information in the Assembly Voting work place.	Deloitte has checked by way of inspection that a formalized procedure exist to ensure physical access to buildings. Deloitte inspected the building and found access controls implemented as described.	No exceptions noted.

Control objective C **Procedures and controls are complied with to ensure that the data processor has implemented organizational measures to ensure relevant security of processing.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
C.1	The management of Assembly Voting has approved a written information security policy that was communicated to all relevant stakeholders, including Assembly Voting's employees. The IT security policy is based on the risk assessment performed. Assessments are made on a regular basis as to whether the IT security policy should be updated.	Deloitte has checked by way of inspection that an information security policy exists which the management has considered and approved within the past year. Deloitte has inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No exceptions noted.
C.2	The management of Assembly Voting has checked that the information security policy is consistent with data processing agreements entered into.	Deloitte has inspected documentation of the management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered into. Deloitte has inspected the latest sample of data processing agreements and checked that the requirements in this agreements are covered by the requirements of the information security policy for safeguards and security of processing.	No exceptions noted.
C.3	The employees of Assembly Voting are screened as part of the employment process. Such screening comprises, as relevant: • Certificates of criminal record. • Collection of references from former employers.	Deloitte has checked by way of inspection that formalized procedures are in place to ensure screening of the data processor's employees as part of the employment process. Deloitte has inspected the latest employee recruitments and noted that the screening comprised of the relevant elements is available.	No exceptions noted.

Control objective C **Procedures and controls are complied with to ensure that the data processor has implemented organizational measures to ensure relevant security of processing.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
C.4	Employees sign a confidentiality agreement, which is included in the employment contract. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information about the employees' processing of personal data.	Deloitte has inspected the latest employee recruitment and checked that the relevant employee has signed a confidentiality agreement. Deloitte has inspected the latest employee recruitment and checked that the employee has been introduced to: • The information security policy; • Procedures for processing data and other relevant information. HERTIL	No exceptions noted.
C.5	For resignations or dismissals, Assembly Voting has implemented a process to ensure that users' rights are deactivated or terminated and that assets are returned.	Deloitte has inspected procedures ensuring that the rights of resigned or dismissed employees are deactivated or terminated upon resignation or dismissal, and that assets such as access cards, computers, mobile phones, etc., are returned. Deloitte has inspected the latest employee dismissal and checked that rights have been deactivated or terminated, and that assets have been returned. No resignations were noted.	No exceptions noted.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by Assembly Voting for the data controllers. In addition, the agreement states that it applies both during the employee's employment period and after.	Deloitte has checked by way of inspection that formalized procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. No resignations noted.	No exceptions noted.

Control objective C **Procedures and controls are complied with to ensure that the data processor has implemented organizational measures to ensure relevant security of processing.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
C.7	Awareness training is provided to Assembly Voting's employees on a regular basis with respect to general IT security and security of processing related to personal data.	Deloitte has checked by way of inspection that Assembly Voting provides awareness training to the employees covering general IT security and security of processing related to personal data.	No exceptions noted.

Control objective D **Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.	Deloitte has checked by way of inspection that formalized procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. Deloitte has checked by way of inspection that the procedures are up to date.	No exceptions noted.
D.2	According to the data processing agreement, it is agreed between the data controller and Assembly Voting what the storage periods and deletion routines should be. Data are deleted no later than 30 days after an election has ended.	Deloitte has checked by way of inspection that the existing procedures for storage and deletion exist. Deloitte has inspected a sample of data processing sessions from the data processor's list of processing activities and checked that documentation exists and that personal data are stored in accordance with the agreed storage periods. Deloitte has inspected a sample of data processing sessions from the data processor's list of processing activities and checked that documentation exists and that personal data are deleted in accordance with the agreed deletion routines.	No exceptions noted.
D.3	Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: • Deleted no later than 30 days after the termination of the agreement if this is not in conflict with other laws.	Deloitte has checked by way of inspection that formalized procedures are in place for processing the data controller's data upon termination of the processing of personal data. Deloitte has inspected the latest terminated data processing sessions and noted that the agreed deletion of data has taken place.	No exceptions noted.

Control objective E **Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
E.1	Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller.	Deloitte has checked by way of inspection that formalized procedures exist for only storing and processing personal data in accordance with the data processing agreements. Deloitte has checked by way of inspection that the procedures are up to date. Deloitte has inspected a sample of one data processing session from the data processor's list of processing activities and checked that documentation exists that data processing takes place in accordance with the data processing agreement.	No exceptions noted.
E.2	Data processing and storage by Assembly Voting must only take place in localities, countries or regions approved by the data controller.	Deloitte has checked by way of inspection that the data processor has a complete and up-to-date list of processing activities stating localities, countries, or regions. Deloitte has inspected a sample of one data processing session from the data processor's list of processing activities and checked that documentation exists that the processing of data, including the storage of personal data, only takes place in the localities stated in the data processing agreement – or otherwise as approved by the data controller.	No exceptions noted.

Control objective F **Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organizational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
F.1	Written procedures exist which include requirements for Assembly Voting when using sub-data processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular as to whether the procedures should be updated.	Deloitte has checked by way of inspection that formalized procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions. Deloitte has checked by way of inspection that procedures are up to date.	No exceptions noted.
F.2	Assembly Voting only uses sub-data processors to process personal data specifically or generally approved by the data controller.	Deloitte has checked by way of inspection that the data processor has a complete and up-to-date list of sub-data processors used. Deloitte has inspected a sample of one sub-data processor from the data processor's list of sub-data processors and checked that documentation exists that the processing of data by the sub-data processor is stated in the data processing agreements or otherwise as approved by the data controller.	No exceptions noted.
F.3	When changing sub-data processors, this can only happen after a written consent from the data controller has been received.	Deloitte has checked by way of inspection that requirements for written consent from the data controller, in case of changing sub-data processors, are part of the data processing agreement. Deloitte has inspected documentation that written consent from a data controller was requested and received prior to adding a sub-data processor.	No exceptions noted.

Control objective F **Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organizational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
F.4	Assembly Voting has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	Deloitte has checked by way of inspection the existence of signed sub-data processing agreements against the sub-data processors used and stated on the data processor's list. Deloitte has inspected a sample of one sub-data processing agreement and checked that it includes the same requirements and obligations as those stipulated by the data processing agreements between the data controllers and the data processor.	No exceptions noted.
F.5	The data processor has a list of approved sub-data processors disclosing: • Name • Business Registration No. • Address • Description of the processing activities.	Deloitte has checked by way of inspection that the data processor has a complete and up-to-date list of sub-data processors used and approved. Deloitte has checked by way of inspection that the list at least includes the required details about each sub-data processor.	No exceptions noted.

Control objective F **Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organizational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
F.6	Based on an up-to-date risk assessment of each sub-data processor and the activity taking place at such processor, Assembly Voting regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activities. The data controller is informed of the follow-up activities performed at the sub-data processor.	Deloitte has checked by way of inspection that formalized procedures are in place for following up on processing activities at sub-data processors, and checked their compliance with the sub-data processing agreements. Deloitte has inspected documentation that each sub-data processor and the current processing activity at such processor are subjected to risk assessment. Deloitte has inspected documentation that technical and organizational measures, security of processing at the sub-data processors used, third countries' bases of transfer and similar matters are appropriately followed up on. Deloitte has inspected documentation that information on the follow-up activities at sub-data processors is communicated to the data controller so that such controller may plan an inspection.	No exceptions noted.

Control objective H **Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting, or restricting information on the processing of personal data to the data subject.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
H.1	Written procedures exist which include a requirement that Assembly Voting must assist the data controller in relation to the rights of data subjects.	Deloitte has checked by way of inspection that formalized procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. Deloitte has checked by way of inspection that the procedures are up to date.	No exceptions noted.
H.2	Assembly Voting has established procedures in so far as this was agreed that enable timely assistance to the data controller in handing out and deleting information about the processing of personal data to data subjects.	Deloitte has checked by way of inspection that the procedures are in place for assisting the data controller. Deloitte has inspected documentation that the systems used support the performance of the relevant detailed procedures. Deloitte has checked by way of inspection that requests by the data controller for assistance have been documented in a correct and timely manner.	No exceptions noted.

Control objective I **Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
I.1	Written procedures exist which include a requirement that Assembly Voting must inform the data controllers in the event of any personal data breaches.	Deloitte has checked by way of inspection that formalized procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. Deloitte has checked by way of inspection that procedures are up to date.	No exceptions noted.
I.2	Assembly Voting has established controls to identify any personal data breaches, including an IT security instruction for the employees, awareness training, ongoing briefings on security related matters and logging of data access.	Deloitte has checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches. Deloitte has inspected the IT security policy and instruction. Deloitte has inspected documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on in a timely manner.	No exceptions noted.
I.3	If any personal data breach occurs, Assembly Voting will inform the data controller without undue delay and no later than 48 hours after having become aware of such personal data breach at Assembly Voting or a sub-data processor.	Deloitte has checked by way of inspection that guidelines for informing the data controllers in case of a breach exist. We were informed that no data breaches have occurred in 2019.	No exceptions noted.

Control objective I **Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.**			
No.	**Assembly Voting's control activity**	**Test performed by Deloitte**	**Results of Deloitte's test**
I.4	Assembly Voting has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency.	Deloitte has checked by way of inspection that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for: • Describing the nature of the personal data breach; • Describing the probable consequences of the personal data breach; • Describing the measures taken or proposed to be taken to respond to the personal data breach.	No exceptions noted.