Dansk Revision Århus
Godkendt revisionspartnerselskab
Tomsagervej 2
DK-8230 Åbyhøj
aarhus@danskrevision.dk
www.danskrevision.dk
Telefon: +45 89 36 12 12
Telefax: +45 89 36 12 00
CVR: DK 26 71 76 71
Bank: 6181 0007769555

NPS.TODAY APS

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with NPS.TODAY ApS' clients.

Table of Contents

1. Management's statement

NPS.TODAY ApS processes personal data for its clients (data controller), in accordance with data processing agreements.

The accompanying description has been prepared for the data controller, who has used NPS.TODAY ApS' services, and who has 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 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. NPS.TODAY ApS confirms that:

a) The accompanying description, fairly presents NPS.TODAY ApS' services and systems, which has processed personal data for the data controllers subject to the Regulation throughout the period from 1st of September 2024 to 31st of August 2025. The criteria used in making this statement were that the accompanying description:

(i) Presents how NPS.TODAY ApS' services and systems was 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 authorised 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 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 organisational 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, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
- Controls that we, in reference to the scope of NPS.TODAY ApS' 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 the 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 in the period from 1st of September 2024 to 31st of August 2025.

(iii) Does not omit or distort information relevant to the scope of NPS.TODAY ApS' 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 NPS.TODAY ApS' services 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, in our view, suitably designed and operated effectively throughout the period from 1st of September 2024 to 31st of August 2025. 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, throughout the period from 1st of September 2024 to 31st of August 2025.

c) Appropriate technical and organisational 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.

Copenhagen, 23 October 2025

Jesper Vagtel Johansen, CEO

NPS.TODAY ApS

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with NPS.TODAY ApS' clients using the related services.

To: NPS.TODAY ApS and NPS.TODAY ApS´ clients using the related services.

Scope

We were engaged to provide assurance about NPS.TODAY ApS' description of services in relation to the processing of personal data, in accordance with the data processing agreement with NPS.TODAY ApS' clients as the data controller, throughout the period from 1st of September 2024 to 31st of August 2025. As well as provide assurance as to the design and effectiveness of controls related to the control objectives stated in the description.

We express reasonable assurance in our conclusion.

NPS.TODAY ApS' responsibilities

NPS.TODAY ApS is responsible for: preparing the description and the accompanying statement on page 3-4, including the completeness, accuracy, and the method of presentation of the description and statement, providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's independence and quality control

We have complied with the independence and other ethical requirements 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.

Dansk Revision Aarhus is 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 NPS.TODAY ApS' description and on the design and effectiveness 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, to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are appropriately designed and operating effectively.

An assurance engagement to report on the description, design, and operating effectiveness 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 about the design and operating effectiveness 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 appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. 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.

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 processor

NPS.TODAY ApS' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of NPS.TODAY ApS' services 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 operating effectiveness 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 NPS.TODAY ApS' processing of personal data, as this was designed and implemented, as of the 1st of September 2024 to 31st of August 2025, and

(b) The controls related to the control objectives stated in the description were appropriately designed as of the 1st of September 2024 to 31st of August 2025; and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from 1st of September 2024 to 31st of August 2025.

Description of tests of controls

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

Intended users and purpose

This report and the description of tests of controls, as outlined in section 4, are intended only for data controllers who have used NPS.TODAY ApS' 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 Regulation have been complied with.

Åbyhøj, 23 October 2025

Dansk Revision Aarhus
godkendt revisionspartnerselskab, CVR-nr. 26717671

Claus Guldborg Nyvold
Registered Accountant

3. Description of processing

The purpose of the Processor's processing of personal data on behalf of the data controller is divided into two services:

- Provision of NPS.TODAY's software, where loyalty information about the data controller's survey participants, e.g. customers, partners, and employees, will be collected and processed.
- Processing and storage of personal data that the data controller inserts in the system.

Nature of processing

Processing and storage of personal data that the data controller inserts in the system.

Personal data

E-mail, IP address, name and phone number, NPS score, NPS comments, customer ID, and timestamp

Categories of data subjects

- The Data controller's employees working within the NPS software.
- The individuals to whom the Data controller sends surveys, e.g. the data controller's customers, partners, etc.
- Other individuals who have or have had a direct or indirect customer and/or employment-related relationship with the Data controller.

Practical measures

The data processor has established an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons.

Organizational security

The data processor has implemented the following organizational security measures regarding the protection of personal data:

- All employees are subject to a duty of confidentiality covering all processed personal data.
- Employees' access to personal data in systems and on any physical media or facilities is restricted, so that only relevant employees have access to relevant personal data.
- Employees' processing of personal data is logged in full or in part and can be monitored as needed.
- The data processor maintains an IT security policy.
- The data processor has a documented procedure for personal data breaches, reviewed at least annually.
- The data processor has a fixed procedure to ensure that, in connection with repair, service, and disposal of hardware, data is deleted or confidentiality of the data is otherwise ensured.
- The data processor is able to take employment-related measures in response to employees' breaches of data security or instructions on personal data processing.
- The data processors employees document and regularly report personal data breaches or risks thereof.

Technical security: Access to and protection of systems

The data processor has implemented the following technical security measures regarding access to and protection of systems:

- A password policy is applied, including minimum requirements.
- Employees are required to use individual passwords.
- Logging and monitoring of unauthorised or repeated failed login attempts are performed on the data processor's systems.
- Antivirus software is used and regularly updated.
- Systems are protected by logical access controls requiring username and password or other authorisation.
- PCs are automatically access-protected when inactive (screen lock).
- Procedures are in place for granting system authorisations upon employment.
- Procedures are in place for revoking permissions when an employee leaves or changes department.

Technical security: Encryption

The data processor implements the following technical security measures regarding encryption:

- Encryption of network traffic is applied.
- The data processor's websites use HTTPS (Hyper Text Transfer Protocol Secure).
- Personal data is encrypted in relevant systems and/or on storage media.
- The data processor's computers have encrypted hard drives.

Technical security: Availability and resilience

The data processor or its sub-processors implement the following technical security measures regarding availability and resilience:

- Availability and resilience of systems and servers are ensured by third parties with whom the Processor has agreements.
- Temperature and humidity in server rooms are monitored.
- Server rooms have smoke alarms and fire extinguishers.
- Server rooms are equipped with air conditioning systems.
- Only authorised employees have access to any server rooms owned by the Processor.
- Regular backups are performed (either by the Processor or a supplier).
- Rules and guidelines exist for restoring data from backup.
- Rules and guidelines exist for performing data backups.
- Uninterruptible Power Supply (UPS) is used.
- Documented procedures for personal data breaches are reviewed at least annually.
- Active alerting is implemented in case of unauthorised access attempts to server rooms and/or processing systems and data.

Complementary controls at the data controllers

The data controller has the following obligations:

- to ensure that the personal data is up to date
- to make sure that the instruction is legal in relation to the personal data law regulation applicable at any time
- that the instruction is appropriate in relation to this data processing agreement and the main service.
- to ensure that the data controller's users are up-to-date

4. Control objectives, control activity, tests and test results

Control objective A **Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
A.1	Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures that ensure that processing of personal information only takes place in accordance with instructions. Inspected that the procedures contain requirements for a minimum annual assessment of the need for updating, including changes in the data controller's instructions or changes in data processing. Inspected that the procedures have been updated.	No exceptions noted.
A.2	The data processor only processes personal data as stated in the instructions from the data controller.	Inspected that processing of personal data only takes place in accordance with instructions.	No exceptions noted.
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	Inspected that there are formalized procedures that ensure that the processing of personal information does not go against the data protection regulation or other legislation. Inspected that there are procedures for notifying the data controller in cases where the processing	No exceptions noted. No instructions regarding the processing of personal data have been received that are contrary to applicable law.

Control objective A **Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
		of personal data is deemed to be in breach of the legislation. Inspected that the data controller is notified in cases where the processing of personal data is assessed to be in breach of the legislation.	

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.**			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
B.1	Written procedures exist which include a requirement that safeguards are established for the processing of personal data in accordance with the agreement 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.	Inspected that there are formalized procedures that ensure that the agreed security measures are established. Inspected that procedures are up to date. Inspected safeguards agreed in data processing agreements have been established.	No exceptions noted.
B.2	The data processor has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of safeguards, as required by the data controller.	Inspected that there are formalized procedures that ensure that the data processor carries out a risk assessment to achieve adequate security. Inspected that the risk assessment carried out is up to date and takes into account, the current methods of processing of personal data. Inspected that the data processor has implemented the technical measures that ensure adequate security in accordance with the risk assessment. Inspected that the data processor has implemented the security measures as agreed with the data controllers.	No exceptions noted.

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.**			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	Inspected that antivirus software has been installed for the systems and databases used to process personal information. Inspected that antivirus software is up to date.	No exceptions noted.
B.4	External access to systems and databases used for the processing of personal data takes place through a secured firewall.	Inspected that external access to systems and databases used for processing personal data only takes place through a firewall. Inspected that the firewall is appropriately configured.	No exceptions noted.
B.5	Access to internal networks is restricted to users that are granted a username and password. Guest users are deleted as soon as they have left the office location. External access to the network must be done via VPN.	Inspected that guest users have had their access to the internal network removed. Inspected that external access to the network must be done via VPN.	No exceptions noted.
B.6	Access to personal data is restricted to only users with a work-related need for such access.	Inspected that there are formalized procedures for restricting users' access to personal data. Inspected that there are formalized procedures for follow-up that users' access to personal data is in accordance with their work-related needs. Inspected that the technical measures in the application support the limitation in the users' work-related access to personal data.	No exceptions noted.

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.**			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
		Inspected, that user access to data is limited to the employees work-related needs.	
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. The monitoring includes: • Disk space • CPU load • Server uptime	Inspected that systems and databases used for processing personal data have system monitoring with alarms enabled. Inspected that follow-up on alarms is carried out.	No exceptions noted.
B.8	Effective encryption is applied where relevant, including for: • Transmission of sensitive and confidential personal data via the Internet • Storage of passwords • Personal data is encrypted in relevant systems and/or on storage media.	Inspected that formalised procedures are in place to ensure that encryption is applied where relevant. Inspected that technological solutions for encryption have been available and activated. Inspected that encryption is applied where relevant.	No exceptions noted.
B.9	Logging has been established in systems, databases, and networks of all user activities performed by employees.	Inspected that there are formalized procedures for setting up logging of user activities in systems and databases used for processing personal data. Inspected that logging of user activities in systems and databases used for processing and	No exceptions noted.

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.**			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
	Log data is protected against manipulation and technical errors.	transmission of personal data is configured and activated. Inspected that collected information about user activity is protected against manipulation and deletion.	
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's intended purpose according to agreement, and on the data controller's behalf.	Inspected that there are formalized procedures for the use of personal data for development, testing and the like, which ensure that the use only takes place in pseudonymized or anonymized form. Inspected that personal data in development and test databases is pseudonymised or anonymised, unless this prevents troubleshooting.	No exceptions noted.
B.11	The technical measures established are tested on a regular basis with vulnerability scans.	Inspected that there are formalized procedures for ongoing tests of technical measures, including the implementation of vulnerability scans. Inspected, that there are performed vulnerability scans in the audit period.	No exceptions noted.
B.12	Changes to systems or databases are made consistently with procedures that ensure maintenance using relevant updates and patches, including security patches.	Inspected that there are formalized procedures for handling changes to systems and databases, including handling 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 safeguard relevant security of processing.**			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
		Inspected that systems and databases are updated with agreed changes and relevant updates, patches, and security patches.	
B.13	A formalised procedure is in place for granting and removing a user's access to personal data. User access needs are assessed on a regular basis, including the continued justification of rights by a work-related need.	Inspected that there are formalized procedures for granting and terminating users' access to systems and databases used for processing personal data. Inspected that employees' user access rights are granted based on work-related needs. Inspected that employees with access to systems and databases have appropriate rights in accordance with their job function. Inspected that user access for terminated employees has been deactivated. Inspected that there is documentation for regular - at least once a year - assessment and approval of assigned user access.	No exceptions noted.
B.14	Access to systems and databases in which personal data is processed is granted through the use of strong passwords or two-factor authentication.	Inspected that formalised procedures are in place to ensure that employees use strong passwords or two-factor authentication."	No exceptions noted.

Control objective B **Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.**			
Nr.	Data processor's control activity	Test performed by auditor	Result of auditor's test
		Inspected that employees use strong passwords or two-factor authentication when accessing customer data.	
B.15	Physical access safeguards have been established to ensure that only authorised persons can access data centers or personal data.	Inspected that there are formalized procedures that ensure that only authorized persons can gain physical access to data centers in which personal data is stored and processed.	No exceptions noted.
B.16	Backup of data in customer systems has been established and is tested regularly.	Inspected that formalised procedures are in place to ensure that customer data is backed up. Inspected that formalised procedures are in place to ensure that restore tests of performed backups are carried out. Inspected that backup and restore tests of customer data have been performed.	No exceptions noted.

Control objective C **Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
C.1	Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the current risk assessment. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	Inspected that there is an information security policy that management has reviewed and approved within the past year. Inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No exceptions noted.
C.2	Management of the data processor has ensured that the information security policy does not conflict with data processing agreements entered into previously.	Inspected that the information security policy generally meets the requirements for security measures and processing security in concluded data processing agreements. Inspected that the requirements in the data processing agreement entered into with the clients are covered by the information security policy's requirements for security measures and processing security.	No exceptions noted.
C.3	The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant: • Certificates of criminal record	Inspected that there are formalized procedures that ensure screening of the data processor's employees during the recruitment process. Inquired that all new employees in the audit period as been screened according to the procedures.	No exceptions noted.

Control objective C **Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
C.4	Upon employment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	Inspected that all hired employees during the report period have signed a confidentiality agreement. Inspected that all new employees have been introduced to the information security policy and procedures for data processing.	No exceptions noted.
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	Inspected procedures that ensure that resigned employees' rights are deactivated or removed upon termination, and that assets such as access cards, PCs, mobile phones, etc. are seized Inspected that all resigned employees, during the report period, have had their rights removed or accounts deactivated or terminated, and that assets have been withdrawn.	No exceptions noted. No terminations during the audit period.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	Inspected that there are formalized procedures that ensure that terminated employees are made aware of the confidentiality agreement and general confidentiality requirements. Inspected that all resigned or dismissed employees during the assurance period that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality.	No exceptions noted. No terminations during the audit period.

Control objective C **Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	Inspected that the data processor offers awareness training to employees covering general IT security and processing security in relation to personal data, as well as reporting of security incidents. Inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.	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.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor'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. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures for the storage and deletion of personal information in accordance with the agreement with the data controller. Inspected that the procedures are up to date.	No exceptions noted.
D.2	The following specific requirements have been agreed upon, with respect to the data processor's storage periods and deletion routines: • After 3 years of inactivity by a survey participant, personal data will automatically be anonymised (unless otherwise agreed). The anonymised data will be retained for statistical purposes. • Upon request or upon termination of the provision of technical data processing services (e.g. technical survey data), data will be anonymised no later than 30 days after the notice of termination. Due to system services such as backup devices, data may remain in the systems for an additional 30 days. In summary, data subject to anonymisation may remain unchanged in the systems for up to 60 days before the process is completed. Any personal data processed, e.g. survey comments or responses to follow-up	Inspected that the existing procedures for storage and deletion contain the specific requirements for the data processor's storage periods and deletion routines. Inspected that deletion upon terminated agreements has been carried out in accordance with the customer agreement. Inspected that, for terminated data processing activities, documentation exists confirming that the agreed deletion or return of data has been executed.	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.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
	questions (all free text fields), will be deleted within 60 days.		
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: • Returned to the data controller; and/or • Deleted if this is not in conflict with other legislation.	Inspected that there are formalized procedures for processing the data controller's data when the processing of personal data ceases. Inspected, that there is documentation that the agreed deletion or return of data has been carried out.	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.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor'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. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures for the storage and processing of personal data only in accordance with the data processor agreements. Inspected that the procedures are up to date. Inspected that documentation exists confirming that the data processing is carried out in accordance with the data processing agreement.	No exceptions noted.
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	Inspected that the data processor has a comprehensive and up-to-date overview of processing activities with an indication of locations, countries or land areas. Inspected that documentation exists confirming that the data processing, including the storage of personal data, is carried out only at the locations specified in the data processing agreement – or otherwise 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 organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
F.1	Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures for the use of sub-data processors, including requirements for sub-data processor agreements and instructions. Inspected that the procedures are up to date.	No exceptions noted.
F.2	The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.	Inspected that the data processor has a comprehensive and up-to-date overview of used sub-data processors. Inspected that all sub-processors from the data processor's overview of sub-processors, that there is documentation that the sub-processor's data processing appears in the data processor agreements - or is otherwise approved by the data controller.	No exceptions noted.
F.3	When changing the generally approved sub-data processors used, the data controller is informed in time to enable such data controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-data processors used, this has been approved by the data controller.	Inspected that there are formalized procedures for notifying the data controller of changes in the use of sub-data processors. Inspected documentation that the data controller is notified of changes in the use of sub-data processors during the report period.	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 organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
F.4	The data processor 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.	Inspected that there are signed sub-data processor agreements with used sub-data processors, which appear from the data processor's overview. Inspected that all sub-data processor agreements contain the same requirements and obligations as stated in the data processor 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 containing the following details: • Name • CVR number • Address • Description of data processing	Inspected that the data processor has a comprehensive and up-to-date overview of used and approved sub-data processors. Inspected that the overview contains, at a minimum, the required information about the individual sub-data processors.	No exceptions noted.
F.6	Based on an updated risk assessment of each sub-data processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-data processor.	Inspected that there are formalized procedures for follow-up on processing activities by the sub-data processors and compliance with the sub-data processor agreements. Inspected documentation that a risk assessment has been carried out of the individual sub-data	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 organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
		processor and the current processing activity of this. Inspected documentation that proper follow-up has been carried out on technical and organizational measures, the processing security of the sub-processors used, third country transfer basis and the like.	

Control objective G **Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
G.1	Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures that ensure that personal data is only transferred to third party countries or international organizations in accordance with an agreement with the data controller on the basis of a valid transfer basis. Inspected that the procedures are up to date.	No exceptions noted.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	Inspected that the data processor has a complete and updated list of transfers of personal data to third countries or international organisations. Inspected that data transfers were arranged with the data controller in the data processing agreement or subsequently approved.	No exceptions noted.
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	Checked by way of inspection that formalised procedures are in place for ensuring a valid basis of transfer. Checked by way of inspection that procedures are up to date. Inspected that a valid basis for transfer exists.	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.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
H.1	Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures for the data processor's assistance by the data controller in relation to the rights of the data subjects. Inspected that the procedures are up to date.	No exceptions noted.
H.2	The data processor has established procedures in so far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects.	Inspected that the available procedures for assistance to the data controller contain procedures for: • Disclosure of information • Correction of information • Deletion of information • Restriction of processing of personal data • Information on the processing of personal data for the data subject. Inspected documentation that the systems and databases used support the implementation of the mentioned procedures.	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.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
I.1	Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that there are formalized procedures that contain requirements for notifying the data controllers in the event of a breach of personal data security. Inspected that the procedure is up to date.	No exceptions noted.
I.2	The data processor has established the following controls to identify any personal data breaches: • Employee awareness • Monitoring of the servers	Inspected that the data processor offers awareness training to employees in relation to the identification of possible breaches of personal data security. Inspected documentation confirming that servers are monitored, and that follow-up on monitoring alarms is carried out.	No exceptions noted.
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay after having become aware of such personal data breach at the data processor or a sub-data processor.	Inspected that the data processor has an overview of security incidents with an indication of whether the individual incident has resulted in a breach of personal data security. Inquired, the sub-data processors if they have detected any breach of personal data security during the report period Inspected that the data processor has included any breaches of personal data security by sub-	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.**			
Nr.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
		data processors in the data processor's overview of security incidents.	
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency: • The nature of the breach of personal data security • Probable consequences of the breach of personal data security • Measures taken or proposed to be taken to deal with the breach of personal data security.	Inspected that the existing procedures for notifying the data controllers in the event of a breach of personal data security contain detailed procedures for: • Description of the nature of the breach of personal data security • Description of probable consequences of the breach of personal data security • Description of measures taken or proposed to be taken to deal with the breach of personal data security. Inspected documentation that the existing procedures support that measures are taken to handle the breach of personal data security.	No exceptions noted.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Jesper Vagtel Johansen
Direktør
Serienummer: 496612b8-d394-4ebe-8b3e-ba39d3ae306a
IP: 2.106.xxx.xxx
2025-10-27 10:07:49 UTC

Mit ID

Claus Guldborg Nyvold
DANSK REVISION ÅRHUS, GODKENDT REVISIONSPARTNERSELSKAB CVR: 26717671
Registreret revisor
Serienummer: 6ab17a51-67d6-4a70-8939-8d28f439a780
IP: 188.120.xxx.xxx
2025-10-28 06:32:08 UTC

Mit ID