
Cadpeople A/S

Independent auditor's ISAE 3000 assurance report on information security and measures as at April 16 2023 pursuant to the data processing agreement with clients to Cadpeople with signed DPA

April 2023



Contents

- 1. Management’s statement 3
- 2. Independent auditor’s report..... 5
- 3. Description of processing7
- 4. Control objectives, control activities, tests and related findings10

1. Management's statement

Cadpeople A/S processes personal data on behalf of client(Data Controller) in accordance with the data processing agreements.

The accompanying description has been prepared for data controller who has used the services of Cadpeople A/S 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" and "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (subsequently "the data protection rules") have been complied with.

Cadpeople A/S uses Curanet A/S and Microsoft as subprocessors for hosting. This report uses the carve-out method and does not comprise controls that Curanet A/S and Microsoft performs for Cadpeople A/S.

Some of the control objectives stated in our description in section 3 can only be achieved if the complementary controls at data controller are suitably designed together with our controls. This report does not comprise the suitability of the design of these complementary controls.

Cadpeople A/S confirms that:

- a) The accompanying description in section 3 fairly presents the services of Cadpeople A/S that has processed personal data for data controllers subject to the data protection rules as at April 16 2023. The criteria used in making this statement were that the accompanying description:
 - (i) Presents how information security and measures services of Cadpeople A/S 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 security measures 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 the services of Cadpeople A/S, 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) Does not omit or distort information relevant to the scope of the services of Cadpeople A/S 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 the services of Cadpeople A/S 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 as at April 16 2023. 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; and
 - (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.
- c) Appropriate technical and organisational measures were established to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the data protection rules.

Aarhus, 26 April 2023
Cadpeople A/S

Thomas Juel
Partner / CSO

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures as at April 16 2023 pursuant to the data processing agreement with clients to Cadpeople with signed DPA

To: Cadpeople A/S and data controller

Scope

We have been engaged to provide assurance about Cadpeople A/S' description in section 3 of the services of Cadpeople A/S in accordance with the data processing agreement with data controller as at April 16 2023 (the description) and about the design related to the control objectives stated in the description.

Our report covers whether Cadpeople A/S has designed appropriate controls related to the control objectives stated in section 4. The report does not include an assessment of Cadpeople A/S' general compliance with 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" and "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (subsequently "the data protection rules").

Cadpeople A/S uses Curanet A/S and Microsoft as subprocessors for hosting. This report uses the carve-out method and does not comprise controls that Curanet A/S and Microsoft performs for Cadpeople A/S.

Some of the control objectives stated in Cadpeople A/S' description in section 3 can only be achieved if the complementary controls at data controller are suitably designed together with Cadpeople A/S' controls. This report does not comprise the suitability of the design of these complementary controls.

We have not performed procedures regarding the operating effectiveness of the controls included in section 4, and therefore we do not express any opinion thereon.

We express reasonable assurance in our conclusion.

Cadpeople A/S' responsibilities

Cadpeople A/S is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing controls to achieve the stated control objectives.

Auditor's independence and quality control

We have complied with the independence and other ethical requirements in the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct, as well as ethical requirements applicable in Denmark.

PricewaterhouseCoopers 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 Cadpeople A/S' description and on the design of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3000 (revised), “Assurance engagements other than audits or reviews of historical financial information”, and additional requirements applicable in Denmark to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed.

An assurance engagement to report on the description and the design of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor’s description of the services of Cadpeople A/S and about the design of controls. The procedures selected depend on the auditor’s judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified by the data processor and described in the Management’s statement section.

As mentioned above, we have not performed procedures regarding the operating effectiveness of the controls included in section 4, and therefore we do not express any opinion thereon. 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

Cadpeople A/S’ description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the services of Cadpeople A/S 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 all personal data breaches.

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 information security and measures in relation to the services of Cadpeople A/S as designed and implemented as at April 16 2023; and
- b) The controls related to the control objectives stated in the description were suitably designed as at April 16 2023.

Description of test 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 in section 4 are intended only for data controllers who have used the services of Cadpeople A/S and 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 data protection rules have been complied with.

Aarhus, 26 April 2023

PricewaterhouseCoopers

Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Rico Lundager
Senior Manager

3. Description of processing

The purpose of the data processor's processing of personal data on behalf of the data controller is based on the instructions set out in the signed DPA. The DPA will follow as an appendix to the master contract and must be accompanied by a hosting and service agreement.

The services provided by Cadpeople that can include processing of personal data on behalf of our customers can be divided into three main groups:

1. Hosted web applications for digital learning or marketing
2. Hosted Learning management platform
3. XR multiuser platform

Nature of processing

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

- Logging of non-sensitive personal data for analytics and marketing purposes. Data are not further processed but stored and made available to the data controller for analytics and lead generation purposes.
- Storing of non-sensitive personal data in database used for login to applications.
- Storing of non-sensitive personal data in database used for creation of certificates for completed learning.

Personal data

Personal data processed in the application must be specified by data controller in the DPA.

The solutions developed by Cadpeople typically contains the following data:

- General personal data, including identification data such as name, address, date of employment and position, field of work, business phone, profile picture and email address.

Categories of data subjects falling within the data processing agreement:

- Employees of data controller
- Customers to data controller
- External contractors of data controller

Practical measures

Cadpeople has defined a Quality Management System (QMS) to meet the clients' requirements while ensuring a lean and agile project flow. The QMS describes Cadpeople's overall IT security processes. The QMS gives an executive summary of selected areas within organisational, physical and IT security measures, with reference to the in-depth processes in Cadpeople Quality Management System (not available to external partners). The QMS is located on a designated Wiki.js-page – an online documentation tool. Access to this site is limited to employees within Cadpeople only.

Cadpeople delivers bespoke client solutions solely based on the clients' specifications with a wide range of technical solutions and complexity. Hence some quality measures are defined as add-on services that can be added to the hosting and operation of client solutions when relevant.

Cadpeople does not deliver SaaS client solutions, as the project scope essentially covers the actual development of the codebase for the client solutions. Cadpeople offers to host the client solutions through a hosting partner. If needed, we can perform various services connected to the operation of client solutions which will be specified in a hosting agreement.

Overall quality controls are inspired by standards, such as ISO 27001, ISAE 3402, and similar.

Cadpeople has also implemented a designated GDPR-section on the Wiki.js. The purpose of this Wiki-section is to provide an overview of the different GDPR related processes and procedures. This GDPR Wiki-section is closely coupled to our Quality Management System, because a lot of the processes from the QMS also covers the GDPR section related to e.g. our development processes, security, organisation, physical environment etc.

Furthermore, the GDPR-wiki-section covers the aspect of data processing agreements (DPA).

All the procedures/processes described in the Wiki related to GDPR and QMS are to be reviewed at least once a year. However, in case of any changes in the data controllers' instructions or changes in data processing, then the relevant procedures and/or the specific DPA should be updated as well. Mostly, the Wiki is used to describe processes/procedures, whereas a Cadpeople file server is used to storage relevant files like DPA's, static documents etc. The file server is protected with a VPN-connection among others so only Cadpeople employees have access.

The work of the QMS/GDPR is planned in an annual schedule comprising relevant activities to ensure that Cadpeople always is compliant according to applicable law. An online tool, Plandisc, is used for this annual schedule.

Risk assessment

Cadpeople has formalised processes for assessing the risk of the services in which personal data are processed. Since Cadpeople does not deliver SaaS client solutions, as mentioned above, but creates bespoke client solutions, and therefore the data processing activities can vary from project to project. This effects risk assessments, since the data processing activities can change from project to project, and therefore each ISAE3000 GDPR related project must also undergo a risk assessment.

To ensure that the risk assessments are up to date, they must be reviewed at least once a year along with the respective DPA or if there are any changes in the current data processing activities.

The focal point of the risk assessments is the risk/likelihood of a personal data breach and the consequences to the data subject of such a breach.

The risk assessments help ensure that the necessary technical, organisational and security measures are always set up to protect the data being processed either in the solutions or in the organisation. The risk assessment is used in the continued effort to establish organisational and technical security measures to counter the risks (risk management) stated in the risk assessment.

Risk assessments are made by the data controller and the Cadpeople project team with input from relevant employees of the organisation.

Considering the data we process – together with the controls and the organisational, technical and security measures we have implemented to mitigate risks and minimise the likelihood of personal data breaches – the current risk profile of the general GDPR projects is assessed as being low.

Control measures

Cadpeople has established a compliance set-up composed of controls that are carried out internally in the organisation at the agreed frequency in accordance with the purpose of the procedure. These controls have been established to ensure compliance with our QMS and GDPR matters.

Cadpeople also has established formal procedures that ensure DPA's are created in collaboration with the respective data controller. DPA's are only to be created on specific projects i.e. projects that are within scope (see criteria above).

The respective project teams are responsible for filling out the DPA's in collaboration.

The respective project teams are responsible for conducting the risk assessment.

The respective project teams are responsible for updating the risk assessment if necessary, however at least once a year.

Cadpeople has established a "GDPR checklist" which are to be followed by developers on GDPR projects. The "GDPR checklist" consist of handling data subjects rights, storage of data, terms and conditions, consent etc.

Subprocessors are only selected, if they are GDPR compliant. Where applicable, subprocessing agreements are entered with subprocessor. Where not applicable, Cadpeople will conduct a risk assessment to evaluate whether or not the subprocessor is compliant with at least the same obligations as Cadpeople does towards the customer. A part of the risk assessment of subprocessors is to look at the subprocessor's general legal compliance and security level and if any certifications have been achieved.

Please refer to section 4 for a description of the specific control activities.

Complementary controls at the data controllers

As part of the delivery of services, the data controller must implement certain controls that are important to achieve the control objectives specified in the description. This includes:

- Consider the consequences related to the protection of personal data when change requests are raised
- Ensure that personal data are not included in support cases
- Inform Cadpeople about changes in employees who have access to sites shared between the customer and Cadpeople
- Warrant that the purpose of the processing of personal data is lawful and fair and that Cadpeople is only provided with the personal data necessary to fulfil the purpose
- Be responsible for ensuring that a legal basis for processing exists at the time of the transfer of the personal data to Cadpeople – including that any consent is freely given, specific, informed, unambiguous as well as explicit, if required
- Warrant that the individuals to whom the personal data relate (the data subjects) have been sufficiently informed about the processing of their personal data
- Have the primary responsibility for giving Cadpeople instructions about data processing and handle requests from data subjects regarding their rights.
- Report any personal data breaches to the Danish Data Protection Agency.

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.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
A.1	<p>Written procedures are in place which include a requirement that personal data must only be processed when instructions to this effect are available.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Checked by way of inspection that formalised procedures are in place to ensure that personal data are only processed according to instructions.</p> <p>Checked by way of inspection that the procedures include a requirement to assess at least once a year the need for updates, including in case of changes in the data controller's instructions or changes in the data processing.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
A.2	<p>The data processor only processes personal data stated in the instructions from the data controller.</p>	<p>Checked by way of inspection that Management ensures that personal data are only processed according to instructions.</p> <p>Checked by way of inspection of a sample of one personal data processing operation that the processing is conducted consistently with instructions.</p>	No exceptions noted.
A.3	<p>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.</p>	<p>Checked by way of inspection that formalised procedures are in place ensuring verification that personal data are not processed against the Data Protection Regulation or other legislation.</p> <p>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 against legislation.</p>	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.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
B.1	<p>Written procedures are in place which include a requirement that security measures agreed are established for the processing of personal data in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Checked by way of inspection that formalised procedures are in place to ensure establishment of the security measures agreed.</p> <p>Checked by way of inspection that procedures are up to date.</p> <p>Checked by way of inspection of a sample of one data processing agreement that the security measures agreed have been established.</p>	No exceptions noted.
B.2	<p>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 the security measures agreed with the data controller.</p>	<p>Checked by way of inspection that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security.</p> <p>Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data.</p> <p>Checked by way of inspection that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment.</p> <p>Checked by way of inspection that the data processor has implemented the security measures agreed with the data controller.</p>	No exceptions noted.
B.3	<p>For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.</p>	<p>Checked by way of inspection that antivirus software has been installed for the systems and databases used in the processing of personal data.</p> <p>Checked by way of inspection that antivirus software is up to date.</p>	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.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	<p>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.</p> <p>Checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy.</p>	No exceptions noted.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	<p>Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.</p> <p>Inspected network diagrams and other network documentation to ensure appropriate segmentation.</p>	No exceptions noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	<p>Checked by way of inspection that formalised procedures are in place for restricting users' access to personal data.</p> <p>Checked by way of inspection that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need.</p> <p>Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data.</p> <p>Checked by way of inspection of a sample of one user's access to systems and databases that such access is restricted to the employees' work-related need.</p>	No exceptions noted.
B.7	System monitoring with an alarm feature has been established for the systems and databases used in the processing of personal data.	<p>Checked by way of inspection that system monitoring with an alarm feature has been established for systems and databases used in the processing of personal data.</p>	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.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
B.8	<p>Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.</p>	<p>Checked by way of inspection that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm.</p> <p>Checked by way of inspection that technological encryption solutions are available and active.</p> <p>Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.</p>	No exceptions noted.
B.9	<p>Logging of the following matters has been established in systems, databases and networks:</p> <ul style="list-style-type: none"> • Activities performed by system administrators and others holding special rights • Security incidents comprising: <ul style="list-style-type: none"> ○ Changes in log set-ups, including disabling of logging ○ Changes in users' system rights ○ Failed attempts to log on to systems, databases or networks <p>Logon data are protected against manipulation and technical errors and are reviewed regularly.</p>	<p>Checked by way of inspection that formalised procedures are in place for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs.</p> <p>Checked by way of inspection that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated.</p> <p>Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.</p> <p>Checked by way of inspection of a sample of one day of logging that the content of log files is as expected compared to the set-up and that documentation confirms the follow-up performed and the response to any security incidents.</p> <p>Checked by way of inspection of a sample of one day of logging that documentation confirms the follow-up performed on activities carried by system administrators and others holding special rights.</p>	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.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
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 purpose according to agreement and on the data controller's behalf.	<p>Checked by way of inspection that formalised procedures are in place for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form.</p> <p>Checked by way of inspection of a sample of one development or test database that personal data included therein are pseudonymised or anonymised.</p> <p>Checked by way of inspection of a sample of one development or test database in which personal data are not pseudonymised or anonymised that this has taken place according to agreement with, and on behalf of, the data controller.</p>	No exceptions noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	<p>Checked by way of inspection that formalised procedures are in place for regularly testing technical measures, including for performing vulnerability scans and penetration tests.</p> <p>Checked by way of inspection of one sample that documentation confirms regular testing of the technical measures established.</p>	No exceptions noted.
B.12	Changes to systems, databases or networks are made consistently with established procedures that ensure maintenance using relevant updates and patches, including security patches.	<p>Checked by way of inspection that formalised procedures are in place for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches.</p> <p>Checked by way of inspection of extracts from technical security parameters and set-ups that systems, databases or networks have been updated using agreed changes and relevant updates, patches and security patches.</p>	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.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	<p>Checked by way of inspection that formalised procedures exist for granting and removing users' access to systems and databases used for processing personal data.</p> <p>Checked by way of inspection of a sample of one employee's access to systems and databases that the user accesses granted have been authorised and that a work-related need exists.</p> <p>Checked by way of inspection of a sample of one resigned or dismissed employee that the employee's access to systems and databases was deactivated or removed in a timely manner.</p> <p>Checked by way of inspection that documentation states that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.</p>	No exceptions noted.
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	<p>Checked by way of inspection that formalised procedures are in place to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects.</p> <p>Checked by way of inspection that users' access to processing personal data that involve a high risk for the data subjects may only take place by using two-factor authentication.</p>	No exceptions noted.
B.15	Physical access security measures have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	<p>Checked by way of inspection that formalised procedures are in place to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed.</p> <p>Checked by way of inspection of documentation that only authorised persons have physical access to premises and data centres at which personal data are stored and processed.</p>	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.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
C.1	<p>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 information security policy is based on the risk assessment performed.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the information security policy should be updated.</p>	<p>Checked by way of inspection that an information security policy exists that Management has considered and approved within the past year.</p> <p>Checked by way of inspection of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.</p>	No exceptions noted.
C.2	<p>Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.</p>	<p>Inspected documentation of Management's assessment that the information security policy generally meets the requirements for security measures and the security of processing in the data processing agreements entered into.</p> <p>Checked by way of inspection of a sample of one data processing agreement that the requirements therein are covered by the requirements of the information security policy for security measures and security of processing.</p>	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.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
C.3	<p>The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant:</p> <ul style="list-style-type: none"> • References from former employers • Certificates of criminal record • Diplomas 	<p>Checked by way of inspection that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process.</p> <p>Checked by way of inspection of a sample of one data processing agreement that the requirements therein for screening employees are covered by the data processor's screening procedures.</p> <p>Checked by way of inspection of one employee appointed during the assurance period that documentation exists of the screening having comprised:</p> <ul style="list-style-type: none"> • References from former employers • Certificates of criminal record • Diplomas 	No exceptions noted.
C.4	<p>Upon appointment, 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.</p>	<p>Checked by way of inspection of one newly appointed employee that the employee has signed a confidentiality agreement.</p> <p>Checked by way of inspection of one newly appointed employee that the employee has been introduced to:</p> <ul style="list-style-type: none"> • The information security policy • Procedures for processing data and other relevant information. 	No exceptions noted.
C.5	<p>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.</p>	<p>Inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned.</p> <p>Checked by way of inspection of one employee resigned or dismissed that rights have been deactivated or terminated and that assets have been returned.</p>	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.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
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 the data processor for the data controllers.	<p>Checked by way of inspection that formalised procedures are in place to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality.</p> <p>Checked by way of inspection of one employee resigned or dismissed that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality.</p>	No exceptions noted.
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.	<p>Checked by way of inspection that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data.</p> <p>Inspected documentation stating that all employees who have either access to or process personal data have completed the awareness training provided.</p>	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
D.1	<p>Written procedures are in place which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Checked by way of inspection that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
D.2	<p>Specific requirements regarding storage and deletion of data have been agreed with respect to the data processor's in individual data processing agreements.</p>	<p>Checked by way of inspection that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines.</p> <p>Checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities that documentation states that personal data are stored in accordance with the agreed storage periods.</p> <p>Checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities that documentation states that personal data are deleted in accordance with the agreed deletion routines.</p>	No exceptions noted.
D.3	<p>Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been:</p> <ul style="list-style-type: none"> • Returned to the data controller and/or • Deleted if this is not in conflict with other legislation. 	<p>Checked by way of inspection that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data.</p> <p>Checked by way of inspection of one terminated data processing session that documentation states that the agreed deletion or return of data has taken place.</p>	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
E.1	<p>Written procedures are in place which include a requirement that personal data must only be stored in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Checked by way of inspection that formalised procedures are in place for only storing and processing personal data in accordance with the data processing agreements.</p> <p>Checked by way of inspection that procedures are up to date.</p> <p>Checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities that documentation states that data processing takes place in accordance with the data processing agreement.</p>	No exceptions noted.
E.2	<p>Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.</p>	<p>Checked by way of inspection that the data processor has a complete and updated list of processing activities stating localities, countries or regions.</p> <p>Checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities that documentation states that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller.</p>	No exceptions noted.

Control objective F:

Procedures and controls are complied with to ensure that only approved subprocessors 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.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
F.1	<p>Written procedures are in place which include requirements for the data processor when using subprocessors, including requirements for sub-processing agreements and instructions.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Checked by way of inspection that formalised procedures are in place for using subprocessors, including requirements for subprocessing agreements and instructions.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
F.2	<p>The data processor only uses subprocessors to process personal data that have been specifically or generally approved by the data controller.</p>	<p>Checked by way of inspection that the data processor has a complete and updated list of subprocessors used.</p> <p>Checked by way of inspection of a sample of one subprocessor from the data processor's list of subprocessors that documentation states that the processing of data by the subprocessor follows from the data processing agreement – or otherwise as approved by the data controller.</p>	No exceptions noted.
F.3	<p>When changing the generally approved subprocessors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved subprocessors used, this has been approved by the data controller.</p>	<p>Checked by way of inspection that formalised procedures are in place for informing the data controller when changing the subprocessors used.</p>	No exceptions noted.
F.4	<p>The data processor has subjected the subprocessor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.</p>	<p>Checked by way of inspection for existence of signed subprocessing agreements with subprocessors used, which are stated on the data processor's list.</p> <p>Checked by way of inspection of a sample of one sub-processing agreement that it includes the same requirements and obligations as are stipulated in the data processing agreement between the data controller and the data processor.</p>	No exceptions noted.

Control objective F:

Procedures and controls are complied with to ensure that only approved subprocessors 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.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
F.5	<p>The data processor has a list of approved subprocessors disclosing:</p> <ul style="list-style-type: none"> • Name • Company registration no. • Address • Description of the processing. 	<p>Checked by way of inspection that the data processor has a complete and updated list of subprocessors used and approved.</p> <p>Checked by way of inspection that, as a minimum, the list includes the required details about each subprocessor.</p>	No exceptions noted.
F.6	<p>Based on an updated risk assessment of each subprocessor 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 subprocessor.</p>	<p>Checked by way of inspection that formalised procedures are in place for following up on processing activities at subprocessors and compliance with the sub-processing agreements.</p> <p>Checked by way of inspection of documentation that each subprocessor and the current processing activity at such processor are subjected to risk assessment.</p> <p>Checked by way of inspection of documentation that technical and organisational measures, security of processing at the subprocessors used, third countries' bases of transfer and similar matters are appropriately followed up on.</p> <p>Checked by way of inspection of documentation that information on the follow-up at subprocessors is communicated to the data controller so that such controller may plan an inspection.</p>	No exceptions noted.

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.

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
G.1	<p>Written procedures are in place 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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Checked by way of inspection that formalised procedures are in place to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
G.2	<p>The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.</p>	<p>Checked by way of inspection that the data processor has a complete and updated list of transfers of personal data to third countries or international organisations.</p> <p>Checked by way of inspection of a sample of one data transfer from the data processor's list of transfers that documentation states that such transfers were arranged with the data controller in the data processing agreement or subsequently approved.</p>	No exceptions noted.
G.3	<p>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.</p>	<p>Checked by way of inspection that formalised procedures are in place for ensuring a valid basis of transfer.</p> <p>Checked by way of inspection that procedures are up to date.</p> <p>Checked by way of inspection of a sample of one data transfer from the data processor's list of transfers that documentation confirms a valid basis of transfer in the data processing agreement with the data controller and that transfers have only taken place insofar as this was arranged with the data controller.</p>	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
H.1	<p>Written procedures are in place which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Checked by way of inspection that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
H.2	<p>The data processor has established procedures that, insofar as this was agreed, 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.</p>	<p>Checked by way of inspection that the procedures in place for assisting the data controller include detailed procedures for:</p> <ul style="list-style-type: none"> • Handing out data • Correcting data • Deleting data • Restricting the processing of personal data • Providing information about the processing of personal data to data subjects. <p>Checked by way of inspection of documentation that the systems and databases used support the performance of the relevant detailed procedures.</p>	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
I.1	<p>Written procedures are in place which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Checked by way of inspection that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches.</p> <p>Checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
I.2	<p>The data processor has established the following controls to identify any personal data breaches:</p> <ul style="list-style-type: none"> • Awareness of employees • Monitoring of network traffic • Follow-up on logging of access to personal data 	<p>Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches.</p> <p>Checked by way of inspection of documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on.</p> <p>Checked by way of inspection of 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.</p>	No exceptions noted.
I.3	<p>If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than 72 hours after having become aware of such personal data breach at the data processor or a subprocessor.</p>	<p>Checked by way of inspection that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.</p> <p>Made inquiries as to whether personal data breaches have been identified at subprocessors and checked by way of inspection that these breaches are included in the list of security incidents.</p>	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.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
I.4	<p>The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency. These procedures must contain instructions on descriptions of:</p> <ul style="list-style-type: none"> • The nature of the personal data breach • Probable consequences of the personal data breach • Measures taken or proposed to be taken to respond to the personal data breach. 	<p>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 instructions for:</p> <ul style="list-style-type: none"> • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach. <p>Checked by way of inspection of documentation that the procedures available support that measures are taken to respond to the personal data breach.</p>	No exceptions noted.

PENNEO

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

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

Thomas Juel

Kunde

Serienummer: 3210bc9b-85c6-40cf-8623-bb09a46bdced

IP: 80.62.xxx.xxx

2023-04-26 07:44:53 UTC



Rico Lundager

PwC-medunderskriver

Serienummer: CVR:33771231-RID:30016557

IP: 83.136.xxx.xxx

2023-04-26 08:06:58 UTC



Jesper Parsberg Madsen

Statsautoriseret revisor

Serienummer: d928e935-d26a-4251-b316-bc64d31db8a2

IP: 83.136.xxx.xxx

2023-04-26 08:10:26 UTC



Penneo dokumentnøgle: YTC10-1N8TQ-Y488D-Q47BC-H8HFO-YQSF4

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt

Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet

i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service** <penneo@penneo.com>. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser i indlejret i dokumentet ved at anvende Penneos validator på følgende websted: <https://penneo.com/validator>