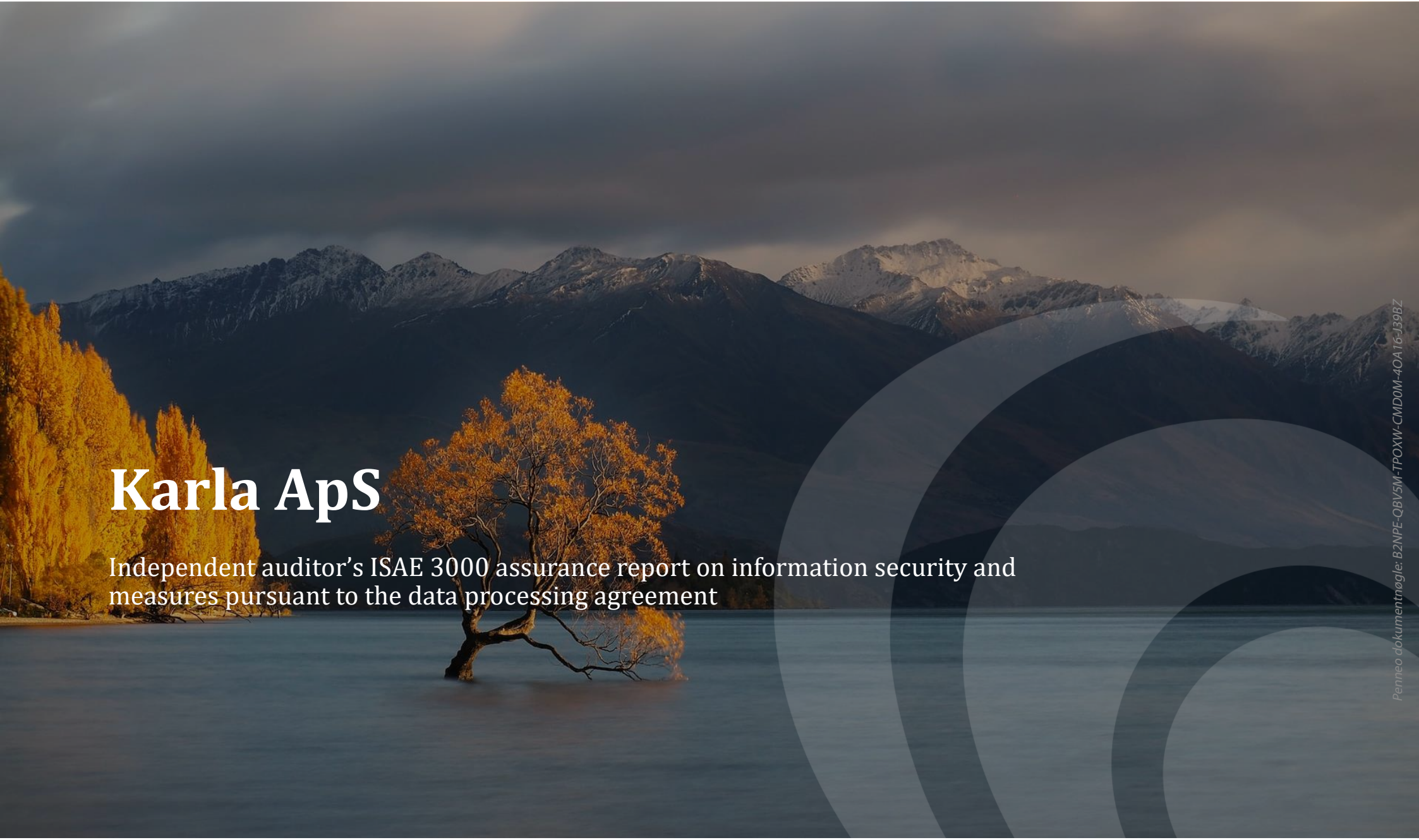

Karla ApS

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement

ADVISORY • ASSURANCE • TAX

Now, for tomorrow

bakertilly

Table of content

1 Management’s statement

2 Independent auditor’s report

3 System Description

4 Control objectives, control activity, tests and test results

1. Management statement

Karla ApS (Data Processor) processes personal data for several Customers (Data Controllers) in accordance with a signed data processing agreement with customers.

The accompanying description has been prepared for our Customers, who use our AI-powered solutions, 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 "GDPR") have been complied with. Karla ApS confirms that:

a) The accompanying description fairly presents the AI-powered solutions, which has processed personal data for data controllers and is subject to GDPR in the period 15 March 2025 to 14 March 2026. The criteria used in making this statement were that the accompanying description:

   i. Presents how the AI-powered solutions were designed and implemented, including:

      - The types of services provided, including the type of personal data processed.
      - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete, and restrict processing of personal data;
      - The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller;
      - The procedures ensuring that the persons 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 organizational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
      - Controls that we, in reference to the scope of the AI-powered solutions, 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 AI-powered solutions in the processing of personal data in the period 15 March 2025 to 14 March 2026**;**

iii. Does not omit or distort information relevant to the scope of the AI-powered solutions 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 AI-powered solutions 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 in the period 15 March 2025 to 14 March 2026**.** 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, in the period 15 March 2025 to 14 March 2026.

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

Copenhagen 7 July 2026

Carl Magnus Illum Smed
CEO

Karla ApS
Niels Hemmingsens Gade 20B
DK-1153 Copenhagen
Office: +45 4242 0055
Website: getkarla.ai
CVR number: 43786911

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with customers of Karla ApS

To: Karla ApS and the customers of Karla ApS

Scope

We were engaged to provide assurance about Karla ApS´ description of the AI-powered solutions processes in accordance with the data processing agreement with Data Controllers throughout the period from 15 March 2025 to 14 March 2026 and the design and operating effectiveness of controls related to the control objectives stated in the Description.

We express reasonable assurance in our conclusion.

Karla ApS' responsibilities

Karla ApS is responsible for the preparation of the System Description in section 3 and the related statement in section 4, including the completeness, accuracy, and the method of presentation of the System Description and statement, for the delivery of services covered by the System Description; for specifying the control objectives; and for the design, implementation, and effective operation of controls to achieve the stated control objectives.

Auditor's independence and quality control

Baker Tilly Denmark Godkendt Revisionsaktieselskab applies International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

We are independent of the Company in accordance with the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (IESBA Code) and the additional ethical requirements applicable in Denmark, and we have fulfilled our other ethical responsibilities in accordance with these requirements and the IESBA Code, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

Auditor's responsibilities

Our responsibility is to express an opinion on Karla ApS´ System Description and on the design and operating 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 in the period 15 March 2025 to 14 March 2026.

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 AI-powered solutions processes 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 and described 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

Karla ApS´ description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the AI-powered solutions processes 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 the AI-powered solutions processes as designed and implemented throughout the period from 15 March 2025 to 14 March 2026
b) The controls related to the control objectives stated in the description were in all material respects appropriately designed throughout the period from 15 March 2025 to 14 March 2026
c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were in all material respects achieved and were operated effectively throughout the period from 15 March 2025 to 14 March 2026

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 are intended only for data controllers who have used the AI-powered solutions processes of Karla ApS, 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.

Copenhagen 7 July 2026

Baker Tilly Denmark
Godkendt Revisionsaktieselskab
CVR number 35257691

Michael Brink Larsen
State-Authorised Public Accountant
MNE number: mne23256

3. System Description

Karla ApS
Karla ApS is a Danish company specializing in AI-powered solutions designed to automate support processes, provide advanced search capabilities, and enhance user experiences for both public institutions and private companies.

The management team oversees responsibilities related to data protection, including managing data processing agreements, addressing customer inquiries, and ensuring compliance with relevant policies.

SaaS Solutions

Karla ApS offers several Software-as-a-Service (SaaS) products, namely Karla Chat, Karla Search, Karla Insights, Karla Inbox, and Karla Actions, under contractual agreements with customers. These cloud-based applications are developed in Denmark and hosted at a German data center managed by Google as a sub-processor.

The SaaS solutions are designed to handle and analyze user inquiries through text-based interactions. The solutions are not intended to process personal information, unless instructed by the Data Controller to do so.

However, there is a risk that personal information may be unintentionally entered into the system. To mitigate this risk, a combination of data minimization and a structured deletion policy has been implemented to identify and remove potentially personal information as quickly as possible. Specific storage periods and deletion routines are set out in the control activities under control objective D.

Practical Measures

The management team is responsible for maintaining IT security and ensuring adherence to established policies, customer agreements, and data processing contracts. Key security measures include:

- Clearly defined procedures for employee hiring, termination, and access management.
- Confidentiality agreements effective during and after employment.
- Encryption of all company IT equipment and use of antivirus software.
- Implementation of role-based access controls.
- Regular employee training on IT security and personal data management.
- Mandatory two-factor authentication (2FA) for systems handling personal information.

The SaaS solutions are protected by backup methods, system monitoring, firewall protection, and detailed logging.

Organizational Security Measures

Employees are contractually obligated to maintain confidentiality regarding company activities, customer relationships, and personal data. Karla ApS strictly enforces robust password practices, screen-lock policies, and general IT security standards. Security measures undergo regular reviews.

Karla ApS aligns its security practices with ISO/IEC 27002:2022 standards, including:

- Restricting data processing geographically within the EU.
- Regularly conducting security audits and compliance assessments.
- Ensuring encryption of data both at rest and in transit.
- Comprehensive system activity monitoring and logging.

Risk Assessment

Karla ApS continuously evaluates risks associated with processing personal data. Through the use of European data centers, geographical restrictions, and a structured deletion policy, a proactive approach to GDPR compliance is ensured. The absence of Follow-the-Sun support and the geographical restrictions are designed to keep processing within the EU's regulatory framework.

Controls

Control measures implemented by Karla ApS align with its internal IT and information security policies and cover the following main areas:

- Risk assessment and management
- Information security policies
- Asset management
- Access and role management
- Encryption practices
- IT and network operations
- System development and maintenance
- Management of security incidents.

Reference is also made to section 4, which describes the specific control activities.

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

4.1 Purpose and scope

We have conducted our engagement in accordance with ISAE 3000 – assurance engagements other than audits or review of historical financial information.

Our tests of the design, functionality, and implementation of controls have included controls that we have assessed necessary to establish reasonable assurance, that the articles stated cf. section 4.3 have been complied with throughout the period from 15 March 2025 to 14 March 2026. Additional control objectives and activities of affiliated companies are not covered by our test procedures.

The requirements and rules of the regulation cannot be deviated from, but the regulation must include and take into account the purpose, the nature of processing and the category of personal data etc. at all levels, and as a result it is of a more general and overarching nature in several areas. The implementation of the security can thus, according to the partners' choice, be adapted to the individual agreement. Thus, individual customer contracts may also have a scope that goes beyond the general requirements of the Data Protection Regulation or the Data Protection Act. Such additional requirements are not covered by the following.

4.2 Test procedures performed

In connection with the performance of tests of control activities, we have performed the following actions:

Method	Description
Inquiries	Interview with appropriate personnel at Karla ApS about the performance of significant control activities.
Inspection	The procedures, policies and documentation established by the customer have been reviewed and decided upon, with a view to assessing whether the specific controls have been designed and implemented so that they can be expected to be effective. In the technical platforms, including databases, network components, etc. we have tested the specific system statement to ensure that the controls are designed, implemented and effective. In addition, it is assessed whether the controls have been adequately monitored and at appropriate intervals.
Observation	Observing how controls are performed.
Re-performance of controls	We have performed or observed a repeated performance of the control, with the aim of verifying that the control works as assumed.

4. Control objectives, control activity, tests and test results (continued)

Control objective A

Instructions regarding the processing of personal data are followed in accordance with the concluded data processor agreement.

No.	Data processor's control activity	Test performed by Baker Tilly	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.	Checked by way of inspection that formalised procedures exist to ensure that personal data are only processed according to instructions. 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. Checked by way of inspection that procedures are up to date.	No comments.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	Checked by way of inspection that Management ensures that personal data are only processed according to instructions. Checked by way of inspection of a sample of 2 personal data processing operations that these are conducted consistently with instructions.	No comments.
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.	Checked by way of inspection that formalised procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation. Checked by way of inspection that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation. Checked by way of inspection that the data controller was informed in cases where the processing of personal data was evaluated to be against legislation.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective B

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

No.	Data processor's control activity	Test performed by Baker Tilly	Result of auditor's test
B.1	Written procedures exist which include a requirement that safeguards agreed 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.	Checked by way of inspection that formalised procedures exist to ensure establishment of the safeguards agreed. Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of 2 data processing agreements that the safeguards agreed have been established.	No comments.
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 the safeguards agreed with the data controller.	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. Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data. 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. Checked by way of inspection that the data processor has implemented the safeguards agreed with the data controller.	No comments.
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.	Checked by way of inspection that, for the systems and databases used in the processing of personal data, antivirus software has been installed. Checked by way of inspection that antivirus software is up to date.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective B

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

No.	Data processor's control activity	Test performed by Baker Tilly	Result of auditor's test
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	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. Checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy.	No comments.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. Inspected network diagrams and other network documentation to ensure appropriate segmentation.	No comments.
B.6	Access to personal data is isolated to users with a work-related need for such access.	Checked by way of inspection that formalised procedures are in place for restricting users' access to personal data. 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. Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data. Checked by way of inspection of a sample of 2 users' access to systems and databases that such access is restricted to the employees' work-related need.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective B

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

No.	Data processor's control activity	Test performed by Baker Tilly	Result of auditor's test
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. This monitoring comprises as mentioned above.	Checked by way of inspection that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. Checked by way of inspection that, in a sample of 2 alarms, these were followed up on and that the data controllers were informed thereof as appropriate.	No comments.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	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. Checked by way of inspection that technological encryption solutions have been available and active throughout the assurance period. Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email. Inquired whether any unencrypted transmission of sensitive and confidential personal data has taken place during the assurance period and whether the data controllers have been appropriately informed thereof.	Encryption is enabled both in transit and at rest; however, it is not considered materially relevant in this context, as no personal data of this nature is processed. No further comments

4. Control objectives, control activity, tests and test results (continued)

Control objective B

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

No.	Data processor's control activity	Test performed by Baker Tilly	Result of auditor's test
B.9	Logging of the following matters has been established in systems, databases and networks: o Activities performed by system administrators and others holding special rights; o Security incidents comprising: o Changes in log setups, including disabling of logging; o Changes in users' system rights; o Failed attempts to log on to systems, databases or networks; Logon data are protected against manipulation and technical errors and are reviewed regularly.	Checked by way of inspection that formalised procedures exist 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. 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. Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion. Checked by way of inspection of a sample of 1 days of logging that the content of log files is as expected compared to the setup and that documentation exists regarding the follow-up performed and the response to any security incidents. Checked by way of inspection of a sample of 1 days of logging that documentation exists regarding the follow-up performed for activities carried by system administrators and others holding special rights.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective B

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

No.	Data processor's control activity	Test performed by Baker Tilly	Result of auditor's test
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.	Checked by way of inspection that formalised procedures exist for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. Checked by way of inspection of a sample of 1 development or test databases that personal data included therein are pseudonymised or anonymised. Checked by way of inspection of a sample of 1 development or test databases 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.	No comments.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	Checked by way of inspection that formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests. Checked by way of inspection of samples that documentation exists regarding regular testing of the technical measures established. Checked by way of inspection that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner and communicated to the data controllers as appropriate.	No comments.
B.12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	Checked by way of inspection that formalised procedures exist for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches. Checked by way of inspection of extracts from technical security parameters and setups that systems, databases or networks have been updated using agreed changes and relevant updates, patches and security patches.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective B

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

No.	Data processor's control activity	Test performed by Baker Tilly	Result of auditor's test
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.	Checked by way of inspection that formalised procedures exist for granting and removing users' access to systems and databases using to process personal data. Checked by way of inspection of a sample of 2 employees' access to systems and databases that the user accesses granted have been authorised and that a work-related need exists. Checked by way of inspection of a sample of 3 resigned or dismissed employees that their access to systems and databases was deactivated or removed on a timely basis. Checked by way of inspection that documentation exists that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	No comments.
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.	Checked by way of inspection that formalised procedures exist to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects. 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.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective B

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

No.	Data processor's control activity	Test performed by Baker Tilly	Result of auditor's test
B.15	Physical access safeguards 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.	Checked by way of inspection that formalised procedures exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. Checked by way of inspection of documentation that, throughout the assurance period, only authorised persons have had physical access to premises and data centres at which personal data are stored and processed.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective C

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

No.	Data processor's control activity	Test performed by Baker Tilly	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 risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	Checked by way of inspection that an information security policy exists that Management has considered and approved within the past year. Checked by way of inspection of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No comments.
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	Inspected documentation of Management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered into. Checked by way of inspection of a sample of 2 data processing agreements that the requirements in these agreements are covered by the requirements of the information security policy for safeguards and security of processing.	No comments.
C.3	The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant: · References from former employers; · Certificates of criminal record; · Diplomas;	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. Checked by way of inspection of a sample of 2 data processing agreements that the requirements therein for screening employees are covered by the data processor's screening procedures. Checked by way of inspection of 1 employee appointed during the assurance period that documentation exists of the screening having comprised:	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective C

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

No.	Data processor's control activity	Test performed by Baker Tilly	Result of auditor's test
C.4	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.	Checked by way of inspection of 2 employee appointed during the assurance period that the relevant employee have signed a confidentiality agreement. Checked by way of inspection of 2 employee appointed during the assurance period that the relevant employee have been introduced to: · Information security policy; · Procedures for processing data and other relevant information.	No comments.
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 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. Checked by way of inspection of 2 employee resigned or dismissed during the assurance period that rights have been deactivated or terminated and that assets have been returned.	No comments.
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.	Checked by way of inspection that formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. Checked by way of inspection of 2 employee resigned or dismissed during the assurance period that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality.	No comments.
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.	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. Inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective D

Personal data can be deleted or returned if agreed upon with the data controller.

No.	Data processor's control activity	Test performed by Baker Tilly	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.	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. Checked by way of inspection that the procedures are up to date.	No comments.
D.2	The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines: - Chat and Search conversations are kept for 12 months, then deleted automatically. - Inbox (mail) is kept for 30 days, then deleted automatically. - The data controller can set a shorter period (1, 3, 14, 30 or 90 days, 6 or 12 months). This setting takes priority. - The data controller can ask for specific data to be deleted at any time. This is done within 14 days.	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. Checked by way of inspection of a sample of 2 data processing sessions from the data processor's list of processing activities that documentation exists that personal data are stored in accordance with the agreed storage periods. Checked by way of inspection of a sample of 2 data processing sessions from the data processor's list of processing activities that documentation exists that personal data are deleted in accordance with the agreed deletion routines.	No comments.
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.	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. Checked by way of inspection of 2 terminated data processing sessions during the assurance period that documentation exists that the agreed deletion or return of data has taken place.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective E

The data processor only stores personal data in accordance with the agreement with the data controller.

No.	Data processor's control activity	Test performed by Baker Tilly	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.	Checked by way of inspection that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. Checked by way of inspection that the procedures are up to date. Checked by way of inspection of a sample of 2 data processing sessions from the data processor's list of processing activities that documentation exists that data processing takes place in accordance with the data processing agreement.	No comments.
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.	Checked by way of inspection that the data processor has a complete and updated list of processing activities stating localities, countries or regions. Checked by way of inspection of a sample of 2 data processing sessions from the data processor's list of processing activities that documentation exists 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.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective F

Only approved sub-processors are used, and the data processor ensures adequate processing security by following up on these technical and organizational measures to protect the rights of the data subjects and the processing of personal data.

No.	Data processor's control activity	Test performed by Baker Tilly	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.	Checked by way of inspection that formalised procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions. Checked by way of inspection that procedures are up to date.	No comments.
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.	Checked by way of inspection that the data processor has a complete and updated list of sub-data processors used. Checked by way of inspection of a sample of 2 sub-data processors from the data processor's list of sub-data processors that documentation exists that the processing of data by the sub-data processor is stated in the data processing agreements – or otherwise as approved by the data controller.	No comments.
F.3	When changing the generally approved sub-data processors 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 sub-data processors used, this has been approved by the data controller.	Checked by way of inspection that formalised procedures are in place for informing the data controller when changing the sub-data processors used. Inspected documentation that the data controller was informed when changing the sub-data processors used throughout the assurance period.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective F

Only approved sub-processors are used, and the data processor ensures adequate processing security by following up on these technical and organizational measures to protect the rights of the data subjects and the processing of personal data.

No.	Data processor's control activity	Test performed by Baker Tilly	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.	Checked by way of inspection for existence of signed sub-data processing agreements with sub-data processors used, which are stated on the data processor's list. Checked by way of inspection of a sample of 2 sub-data processing agreements that they include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.	No comments.
F.5	The data processor has a list of approved sub-data processors disclosing: · Name; · Business Registration No.; · Address; · Description of the processing.	Checked by way of inspection that the data processor has a complete and updated list of sub-data processors used and approved. Checked by way of inspection that, as a minimum, the list includes the required details about each sub-data processor.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective F

Only approved sub-processors are used, and the data processor ensures adequate processing security by following up on these technical and organizational measures to protect the rights of the data subjects and the processing of personal data.

No.	Data processor's control activity	Test performed by Baker Tilly	Result of auditor's test
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.	Checked by way of inspection that formalised procedures are in place for following up on processing activities at sub-data processors and compliance with the sub-data processing agreements. Checked by way of inspection of documentation that each sub-data processor and the current processing activity at such processor are subjected to risk assessment. Checked by way of inspection of documentation that technical and organisational measures, security of processing at the sub-data processors used, third countries' bases of transfer and similar matters are appropriately followed up on. Checked by way of inspection of documentation that information on the follow-up at sub-data processors is communicated to the data controller so that such controller may plan an inspection.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective G

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

No.	Data processor's control activity	Test performed by Baker Tilly	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.	Checked by way of inspection that formalised procedures exist 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. Checked by way of inspection that procedures are up to date.	No comments.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	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. Checked by way of inspection of a sample of 0 data transfers from the data processor's list of transfers that documentation exists that such transfers were arranged with the data controller in the data processing agreement or subsequently approved.	There have been no transfers outside the EU No further comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective G

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

No.	Data processor's control activity	Test performed by Baker Tilly	Result of auditor's test
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. Checked by way of inspection of a sample of 0 data transfers from the data processor's list of transfers that documentation exists of a valid basis of transfer in the data processing agreement with the data controller and that transfers have only taken place in so far as this was arranged with the data controller.	Google Inc, Microsoft Corporation and Redis Ltd are utilized as sub-data processors. Google Inc. and Microsoft Corporation are registered under the EU-US Data Privacy Framework. Redis Ltd's processing is protected by SCC's which Karla Management considers sufficient for the protection of customers' personal data

4. Control objectives, control activity, tests and test results (continued)

Control objective H

The data processor can assist the data controller in providing, correcting, deleting, or restricting information about the processing of personal data to the data subject.

No.	Data processor's control activity	Test performed by Baker Tilly	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.	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. Checked by way of inspection that procedures are up to date.	No comments.
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.	Checked by way of inspection that the procedures in place for assisting the data controller include detailed procedures for: · Handing out data; · Correcting data; · Deleting data; · Restricting the processing of personal data; · Providing information about the processing of personal data to data subjects. Checked by way of inspection of documentation that the systems and databases used support the performance of the relevant detailed procedures. OR IF ASSISTANCE HAS BEEN PROVIDED DURING THE PERIOD Checked by way of inspection that requests by the data controller for assistance in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects have been documented in a correct and timely manner.	No comments.

4. Control objectives, control activity, tests and test results (continued)

Control objective I

Procedures and controls are followed to ensure that any security breaches can be handled in accordance with the concluded data processor agreement.

No.	Data processor's control activity	Test performed by Baker Tilly	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.	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. Checked by way of inspection that procedures are up to date.	No comments.
I.2	The data processor has established the following controls to identify any personal data breaches: · Awareness of employees; · Monitoring of network traffic; · Follow-up on logging of access to personal data;	Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches. 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. 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 on a timely basis.	No breaches at the used subdata processors have been identified. No other comments

4. Control objectives, control activity, tests and test results (continued)

Control objective I

Procedures and controls are followed to ensure that any security breaches can be handled in accordance with the concluded data processor agreement.

No.	Data processor's control activity	Test performed by Baker Tilly	Result of auditor's test
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than 24 hours after having become aware of such personal data breach at the data processor or a sub-data processor.	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. Made inquiries of the sub-data processors as to whether they have identified any personal data breaches throughout the assurance period. Checked by way of inspection that the data processor has included any personal data breaches at sub-data processors in the data processor's list of security incidents. Checked by way of inspection that all personal data breaches recorded at the data processor or the sub-data processors have been communicated to the data controllers concerned without undue delay and no later than 72 hours after the data processor became aware of the personal data breach.	No comments.
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency: · 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.	Checked by way of inspection that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for: · Describing the nature of the personal da-ta 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. Checked by way of inspection of documentation that the procedures available support that measures are taken to respond to the personal data breach. OR IF BREACHES OCCURRED DURING THE PERIOD Checked by way of inspection of documentation that, when a personal data breach occurred, measures were taken to respond to such breach.	No comments.

Baker Tilly GDPR-ansvarlig

Now, for tomorrow

Michael Brink Larsen
Statsautoriseret revisor
+45 4041 5068
mbl@bakertilly.dk

Baker Tilly Denmark
Godkendt Revisionsaktieselskab

Copenhagen
Poul Bundgaards Vej 1, 1
2500 Valby
T: +45 3345 1000

Sorø
Storgade 24A
4180 Sorø
T: +45 3345 1000

Odense
Hjallesevej 126
5230 Odense M
T: +45 6613 0730

bakertilly.dk

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."

Michael Brink Larsen
BAKER TILLY DENMARK GODKENDT REVISIONSAKTIESELSKAB
CVR: 35257691
Statsautoriseret revisor
På vegne af: Baker Tilly Denmark Godkendt Revisionsp…
Serienummer: f0c28aad-9c66-4dd4-9020-15bb8d0b4494
IP: 80.209.xxx.xxx
2026-07-08 10:43:11 UTC

Mit ID

Carl Magnus Illum Smed
CEO
På vegne af: Karla ApS
Serienummer: 679865a8-ed10-40d1-83fc-067b4c244825
IP: 152.115.xxx.xxx
2026-07-08 10:47:08 UTC

Mit ID