

Dstny A/S

Independent auditor’s ISAE 3000 assurance report on information security and measures in relation to the data processing agreement.

Penneo dokument key: ASD3B-K6KLS-GKENO-WSLAI-N9H5A-WKJTC

bakertilly

Now, for tomorrow

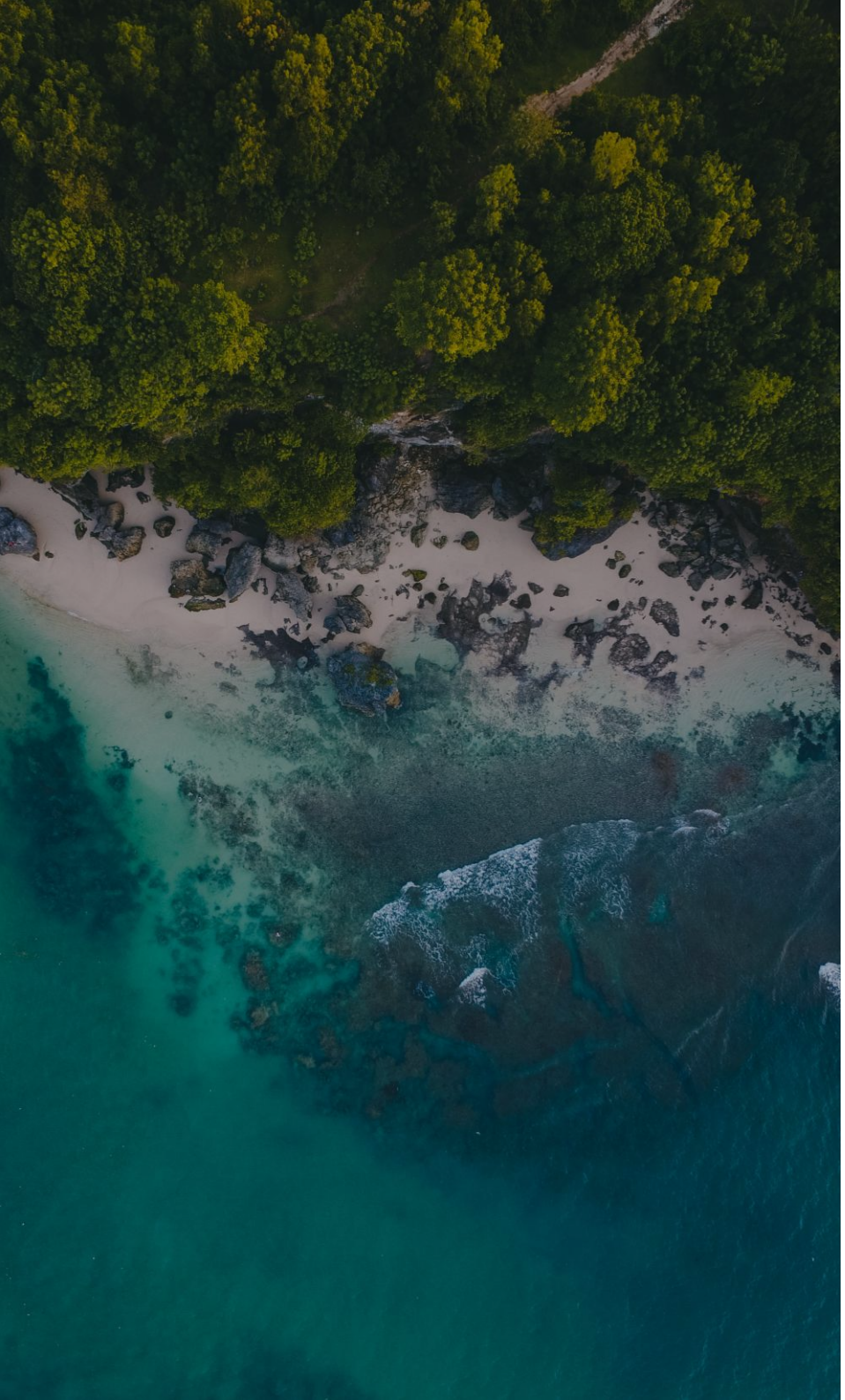


Table of contents

1	Management’s statement	Page	2
2	Independent auditor’s report	Page	4
3	Description of processing	Page	6
4	Control objectives, control activities, tests and results thereof	Page	9

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

1. Management’s statement

Dstny A/S processes personal data on behalf of customers pursuant to a data processing agreement, version 24 of 24 August 2026.

The accompanying description has been prepared for customers who have used Dstny A/S and who have a sufficient understanding to consider the description, together with other information, including information on controls operated by the data controllers themselves, when assessing whether the requirements of the EU Regulation “on the protection of natural persons with regard to the processing of personal data and on the free movement of such data” (hereinafter “the GDPR”) have been complied with. Dstny A/S confirms that:

a) The accompanying description fairly presents Dstny A/S, which has processed personal data for data controllers subject to the GDPR as at 29 September 2026. The criteria used in making this statement were that the accompanying description:

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

- The types of services provided, including the type of personal data processed
- The processes in both IT and manual systems used to initiate, record, process and, if necessary, correct, delete and restrict the processing of personal data
- The processes used to ensure that the data processing performed has taken place in accordance with the contract, instructions or agreement with the data controller
- The processes that ensure that the persons authorised to process personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality
- The processes that, upon termination of data processing, ensure that, at the data controller’s choice, all personal data are deleted or returned to the data controller, unless law or regulation requires retention of the personal data
- The processes that, in the event of a personal data breach, support the data controller in notifying the supervisory authority and informing the data subjects
- The processes that ensure appropriate technical and organisational security measures for the processing of personal data, taking into account the risks presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
- Controls that we, by reference to the delimitation of the services, have assumed would be implemented by the data controllers and which, if necessary to achieve the control objectives stated in the description, are identified in the description

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

1. Management’s statement (continued)

- Other aspects of our control environment, risk assessment process, information system (including the related business procedures) and communication, control activities and monitoring controls that have been relevant to the processing of personal data.

ii. Contains relevant information on changes to the data processor’s service for the processing of personal data made as at 29 September 2026.

iii. Does not omit or distort information relevant to the scope of the security measures described for the processing of personal data, taking into account that the description has been prepared to meet the general needs of a broad range of data controllers and therefore cannot include every aspect of the services that an individual data controller may consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated as at 29 September 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 the relevant risks did not prevent achievement of the stated control objectives, and

iii. The controls were applied consistently as designed, including that manual controls were performed by persons with appropriate competence and authority as at 29 September 2026.

c) Appropriate technical and organisational measures have been established and maintained to fulfil the agreements with the data controllers, good data processing practice and relevant requirements for data processors under the GDPR.

Nærum, 29 September 2026

Kåre Bo Jacobsen
Managing Director

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

2. Independent auditor’s report

Independent auditor’s ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with Dstny A/S’ customers related to the service.

To: Dstny A/S and Dstny A/S’ customers related to the service.

Scope
We have been engaged to report on Dstny A/S’ description of the service pursuant to the data processing agreement with data controllers, as at 29 September 2026, and on the design and operating effectiveness of controls related to the control objectives stated in the description.

Dstny A/S’ responsibility
Dstny A/S is responsible for the preparation of the description and the accompanying statement, including the completeness, accuracy and method of presentation of the description and the statement; for providing the services covered by the description; for stating the control objectives; and for designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor’s independence and quality management
Baker Tilly Denmark Godkendt Revisionsaktieselskab applies International Standard on Quality Management 1, ISQM 1, which requires us to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable law and regulation.

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

Auditor’s responsibility
Our responsibility is to express a conclusion, based on our procedures, on Dstny A/S’ description and on the design and operating effectiveness of controls related to the control objectives stated in that description.

We have conducted our work in accordance with ISAE 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information, and additional requirements under Danish auditor regulation. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether the description is, in all material respects, fairly presented and whether the controls are, in all material respects, suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor’s description of the service and about the design and operating effectiveness of the 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 the controls are not suitably designed or not operating effectively. Our procedures have included testing the operating effectiveness of such controls as 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 suitability of the objectives stated therein, and the suitability of the criteria specified and described by the data processor.

In our opinion, the evidence obtained is sufficient and appropriate to provide a basis for our conclusion.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

2. Independent auditor's report (continued)

Limitations of controls at a data controller
Dstny A/S' description has been prepared to meet the general needs of a broad range of data controllers and therefore does not necessarily include all aspects of the service that each individual data controller may consider important in their particular circumstances. Furthermore, because of their nature, controls at a data processor may not prevent or detect all personal data breaches. Also, the projection of any evaluation of operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Conclusion
Our conclusion has been formed on the basis of the matters set out in this report. The criteria we have used in forming our conclusion are those described in management's statement. In our opinion,

a) the description of the service, as designed and implemented as at 29 September 2026, is, in all material respects, fairly presented, and
b) the controls related to the control objectives stated in the description were, in all material respects, suitably designed as at 29 September 2026, and
c) the controls tested, which were those necessary to provide reasonable assurance that the control objectives in the description were achieved in all material respects, operated effectively as at 29 September 2026.

Description of tests of controls
The specific controls tested, and the nature, timing and results of those tests, are set out on pages 9-26.

Intended users and purpose
This report and the description of tests of controls on pages 9-26 are intended solely for data controllers who have used Dstny A/S' service and who have a sufficient understanding to consider it, together with other information, including information on controls operated by the data controllers themselves, when assessing whether the requirements of the GDPR have been complied with.

Copenhagen, 29 September 2026

Baker Tilly Denmark
Godkendt Revisionsaktieselskab
CVR no. 35 25 76 91

Michael Brink Larsen
State-Authorised Public Accountant
MNE no. mne23256

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

3. Description of processing

This system description concerns controls aimed at data protection and the protection of personal data in connection with the delivery of Dstny A/S' telephony, network and security services.

Since 25 May 2018, Dstny A/S has established controls relating to data protection and processing based on the GDPR. Dstny A/S continuously updates security as a result of ongoing assessments of the risks associated with the data that Dstny A/S processes on behalf of its customers.

The report concerns only the customer-facing area and how Dstny A/S processes and controls the processing of data on behalf of its customers. The report therefore does not cover Dstny A/S' internal processes, such as HR, IT, Marketing and Finance. Nor does the report address specific matters related to individual customer contracts.

With the above reservations and the system description below, Dstny A/S assesses that Dstny A/S has, in all material respects, maintained effective controls. Dstny A/S continuously follows developments in the data protection area and works continuously to improve the controls.

In addition to the GDPR, Dstny A/S is also subject to a large number of other legal requirements, including the Danish Data Retention Order (logningsbekendtgørelsen), the Danish Financial Statements Act (regnskabsloven) and the Danish Act on Electronic Communications Networks and Services.

Description of service

Dstny A/S provides cloud-based communication services. Customers choose for themselves which elements of the product portfolio they agree to, and the controls described are therefore not necessarily relevant to all customers.

The core service is Dstny A/S' cloud-based telephony and UC platform, which the customer accesses directly over the internet via its own connections. Mobile telephony is delivered via Dstny A/S' MVNO setup and is connected directly to the platform. As add-ons, the customer can agree to internet connectivity and managed network and security services, cf. the section "Network and security services (add-ons)".

The customer's own internet connections, local networks and terminal equipment are the customer's responsibility and are not covered by this description, unless otherwise agreed.

Telephony and PBX functionality

Dstny A/S provides telephony as an integrated cloud-based service that includes both fixed-line and mobile telephony as well as related functionality and add-on options. To deliver the requested functionality, Dstny A/S processes personal data about the customer's employees who use the telephony service, as described in the data processing agreement. The data are stored in the customer's setup on the platform and kept up to date on the basis of the customer's instructions. Upon termination of the customer relationship, the customer's setup and data are deleted in accordance with the data processing agreement.

Communication between the customer's equipment and Dstny A/S' platform takes place over the internet in encrypted form. Mobile telephony is run on the mobile network of Dstny A/S' MVNO partner. Security in the mobile network is the partner's responsibility and is not covered by this description.

In addition, Dstny A/S continuously processes billing data for the purpose of correct invoicing.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

3. Description of processing (continued)

Additional services
Dstny A/S provides a number of additional services that entail processing of further categories of data. These include call recording and storage, statistics tools and integrations with the customer's other systems.

For additional services, Dstny A/S processes the data that the customer has decided to collect. The customer can update and delete data itself and can thereby set up its own procedures for retention and deletion.

Dstny A/S has migrated all customers' users from the older Connect2 platform to the newest platform, which is built to support correct processing and documentation of the processing of personal data. A smaller number of customers, however, still use Connect2 for special services that are not supported by the new platform. Access to Connect2 is restricted, and Dstny A/S is working to phase out the platform completely. Connect2 has known limitations with regard to data protection, as encryption and deletion of data are a challenge.

Network and security services (add-ons)
Dstny A/S provides, as add-ons, internet connections and managed network and security services to a smaller group of customers, including MPLS, firewall, managed LAN, managed WiFi and redundant connections. The section is only relevant to customers who have agreed to these services.

Customers with MPLS are connected to Dstny A/S' centrally managed MPLS network. Dstny A/S is responsible for keeping the network and the CPEs that the customer has purchased or leased from Dstny A/S properly updated. Dstny A/S is not responsible for changes to the customer's own equipment made by the customer itself.

Firewall is provided as a standardised service hosted and operated by Dstny A/S. The customer selects the desired security functions and can configure the service within the agreed setup.

As a provider of electronic communications networks and services, Dstny A/S retains log files and session logging in accordance with the Danish Data Retention Order.

Management of compliance with requirements, etc.
Dstny A/S' work on data protection is integrated into the existing organisation for IT and information security. All processing of personal data, including changes to services and systems, is included in a security assessment, and personal data are handled by the IT security group in cooperation with Dstny A/S' DPO and management.

Policies and organisation
Dstny A/S has appointed a DPO, who participates in management meetings and in the ongoing work of the IT security group. The DPO advises on data protection matters and is involved in IT security matters of a principled nature.

Dstny A/S has prepared policies and instructions with the aim of securing the processing of customers' data. Group policies are owned and issued by the group's Group Information Security & Compliance Office and are supplemented by local policies. All policies are approved by management and are available to employees via the intranet. Overall responsibility for IT security rests with management.

The immediate manager communicates policies and guidelines to each employee, and annual awareness training is carried out, managed by Group ICT.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

3. Description of processing (continued)

Technical and organisational controls
Dstny A/S has established procedures and controls within, among other areas:

- Access management
- Encryption
- Physical security and environmental protection
- Operational security, including logging and monitoring
- Communications security
- Acquisition, development and maintenance of systems
- Management of security incidents and personal data breaches
- Emergency, contingency and recovery management
- Handling of customer instructions, including assistance to the customer, deletion

Enquiries from data controllers
Dstny A/S has a procedure for handling and documenting enquiries from data controllers relating to assistance with data subjects' rights (right of access, erasure, rectification, etc.). The documentation is handled in Dstny A/S' support system. If Dstny A/S receives an enquiry directly from a data subject, it is forwarded to the relevant data controller.

Dstny A/S assists, taking into account the nature of the processing, the data controller as far as possible by means of appropriate technical and organisational measures in fulfilling the obligation to respond to requests for the exercise of data subjects' rights under the GDPR. To the extent that Dstny A/S processes personal data on behalf of and on the instructions of the data controller, Dstny A/S assists the data controller in ensuring compliance with:

- the obligation to implement appropriate technical and organisational security measures
- the obligation to notify personal data breaches to the supervisory authority (the Danish Data Protection Agency) without undue delay and, where feasible, no later than 72 hours after the data controller has become aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons
- the obligation to communicate personal data breaches to the data subjects without undue delay where the breach is likely to result in a high risk to their rights and freedoms
- the obligation to carry out a data protection impact assessment where a type of processing is likely to result in a high risk
- the obligation to consult the Danish Data Protection Agency prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller

Dstny A/S notifies the data controller without undue delay after becoming aware of a personal data breach.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

Control objective 1:

Review of Information Security
Control objective: Ensuring that information security is implemented and continuously complied with in accordance with Dstny A/S' policies and procedures

No.	Control objective/control	Tests performed by Baker Tilly	Result of test
A.1	Written procedures exist that include a requirement that personal data may only be processed when instructions are available. The procedures are reviewed for updates on an ongoing basis – and at least annually.	Inspected that formalised procedures exist that ensure that personal data are processed only in accordance with instructions. Inspected that the procedures include a requirement for a minimum annual assessment of the need for updating, including upon changes in the data controller's instructions or changes in the data processing. Inspected that procedures have been updated.	No exceptions noted.
A.2	The data processor performs only the processing of personal data that follows from the instructions of the data controller.	Inspected that management ensures that the processing of personal data takes place only in accordance with instructions. Inspected, in a sample of 3 processing operations of personal data, that these are carried out in accordance with instructions.	No exceptions noted.
A.3	The data processor shall immediately inform the data controller if an instruction, in the data processor's opinion, infringes the GDPR or data protection provisions of other EU law or Member State national law.	Inspected that formalised procedures exist that ensure verification that the processing of personal data does not infringe the GDPR or other legislation. Inspected that procedures exist for notifying the data controller in cases where the processing of personal data is assessed to infringe legislation. Inspected that the data controller has been notified in cases where the processing of personal data has been assessed to infringe legislation.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

Control objective B:

Procedures and controls are complied with that ensure that the data processor has implemented technical measures to ensure appropriate security of processing.

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
B.1	Written procedures exist that include a requirement that agreed security measures are established for the processing of personal data in accordance with the agreement with the data controller. The procedures are reviewed for updates on an ongoing basis – and at least annually.	Inspected that formalised procedures exist that ensure that the agreed security measures are established. Inspected that procedures have been updated. Inspected, in a sample of 3 data processing agreements, that the agreed security measures have been established.	No exceptions noted.
B.2	The data processor has performed a risk assessment and, on that basis, implemented the technical measures assessed to be relevant to achieve appropriate security, including established the security measures agreed with the data controllers.	Inspected that formalised procedures exist that ensure that the data processor performs a risk assessment to achieve appropriate security. Inspected that the risk assessment performed has been updated and covers the current processing of personal data. Inspected that the data processor has implemented the technical measures that ensure appropriate security in accordance with the risk assessment. Inspected that the data processor has implemented the security measures agreed with the data controllers.	No exceptions noted.
B.3	Antivirus, which is updated on an ongoing basis, is installed on the systems and databases used for the processing of personal data.	Inspected that antivirus software is installed on the systems and databases used for the processing of personal data. Inspected that antivirus software has been updated.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
B.4	External access to systems and databases used for the processing of personal data takes place through a secured firewall.	Inspected that external access to systems and databases used for the processing of personal data takes place solely through a firewall. Inspected that the firewall is configured in accordance with internal policy.	No exceptions noted.
B.5	Internal networks are segmented to ensure restricted access to systems and databases used for the processing of personal data.	Enquired whether internal networks are segmented in order to ensure restricted access to systems and databases used for the processing of personal data. Inspected network diagrams and other network documentation to ensure appropriate segmentation.	No exceptions noted.
B.6	Access to personal data is restricted to users with a work-related need for it.	Inspected that formalised procedures exist for restricting users' access to personal data. Inspected that formalised procedures exist for follow-up on whether users' access to personal data is in accordance with their work-related needs. Inspected that the agreed technical measures support maintaining the restriction of users' work-related access to personal data. Inspected, in a sample of 2 users' access to systems and databases, that these are restricted to the employees' work-related needs.	No exceptions noted.
B.7	System monitoring with alerting has been established for the systems and databases used for the processing of personal data. The monitoring covers: • Devices • Systems • Databases.	Inspected that system monitoring with alerting has been established for systems and databases used for the processing of personal data. Inspected, in a sample of 2 alerts, that follow-up has been performed and that the data controllers have been informed to an appropriate extent.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
B.8	Effective encryption is used when transmitting confidential and sensitive personal data via the internet and by email.	Inspected that formalised procedures exist that ensure that the transmission of sensitive and confidential information over the internet is protected by strong encryption based on a recognised algorithm. Inspected that technological encryption solutions have been available and activated at the time of the report. Inspected that encryption is used for transmissions of sensitive and confidential personal data via the internet or by email. Enquired whether there have been unencrypted transmissions of sensitive and confidential personal data at the time of the report, and whether the data controllers have been appropriately informed thereof.	No exceptions noted.

B.9	Logging has been established in systems, databases and networks of the following matters:
	
	• Activities performed by system administrators and others with special privileges
	• Security incidents comprising:
	  • Changes to log settings, including deactivation of logging
	  • Changes to users' system privileges
	  • Failed log-on attempts to systems, databases and networks.
	
	Log information is protected against tampering and technical errors and is reviewed on an ongoing basis.
		Inspected that formalised procedures exist for setting up logging of user activities in systems, databases and networks used for the processing and transmission of personal data, including review of and follow-up on logs.
		
		Inspected that logging of user activities in systems, databases and networks used for the processing and transmission of personal data is configured and activated.
		
		Inspected that collected information on user activity in logs is protected against tampering and deletion.
		
		Inspected, in a sample of 1 day of logging, that log files have the expected content in relation to the setup, and that there is documentation of the follow-up performed and handling of any security incidents.
		
		Inspected, in a sample of 1 day of logging, that there is documentation of the follow-up performed on activities carried out by system administrators and others with special privileges.
			No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
B.10	Personal data used for development, testing or similar purposes are always in pseudonymised or anonymised form. Use takes place solely to serve the controller's purposes in accordance with the agreement and on its behalf.	Inspected that formalised procedures exist for the use of personal data for development, testing and similar purposes, which ensure that use takes place only in pseudonymised or anonymised form. Inspected, in a sample of 1 development and test databases, that personal data therein are pseudonymised or anonymised. Inspected, in a sample of 1 development and test databases where personal data are not pseudonymised or anonymised, that this was done in agreement with the data controller and on its behalf.	No exceptions noted.
B.11	The technical measures established are tested on an ongoing basis by vulnerability scans and penetration tests.	Inspected that formalised procedures exist for ongoing testing of technical measures, including performance of vulnerability scans and penetration tests. Inspected, by sampling, that there is documentation of ongoing tests of the technical measures established. Inspected that any deviations and weaknesses in the technical measures have been handled in a timely and satisfactory manner and communicated to the data controllers to an appropriate extent.	No exceptions noted.
B.12	Changes to systems, databases and networks follow established procedures that ensure maintenance with relevant updates and patches, including security patches.	Inspected that formalised procedures exist for handling changes to systems, databases and networks, including handling of relevant updates, patches and security patches. Inspected, by extracts of technical security parameters and setups, that systems, databases and networks have been updated with agreed changes and relevant updates, patches and security patches.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
B.13	A formalised business procedure exists for granting and revoking user access to personal data. Users' access is reassessed regularly, including that privileges can still be justified by a work-related need.	Inspected that formalised procedures exist for granting and revoking users' access to systems and databases used for the processing of personal data. Inspected, in a sample of 1 employee's access to systems and databases, that the user access granted has been approved and that there is a work-related need. Inspected, in a sample of 1 resigned employee, that the employee's access to systems and databases has been deactivated or removed in a timely manner. Inspected documentation of regular – at least annual – review and approval of granted user access.	No exceptions noted.
B.14	Access to systems and databases in which personal data are processed that entail a high risk for the data subjects takes place, as a minimum, using two-factor authentication.	Inspected that formalised procedures exist that ensure that two-factor authentication is used for the processing of personal data that entails a high risk for the data subjects. Inspected that users' access to perform processing of personal data that entails a high risk for the data subjects can only take place using two-factor authentication.	No exceptions noted.
B.15	Physical access security has been established so that only authorised persons can gain physical access to premises and data centres in which personal data are stored and processed.	Inspected that formalised procedures exist that ensure that only authorised persons can gain physical access to premises and data centres in which personal data are stored and processed. Inspected documentation that only authorised persons have had physical access to premises and data centres in which personal data are stored and processed, at the time of the report.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

Control objective C:

Procedures and controls are complied with that ensure that the data processor has implemented organisational measures to ensure appropriate security of processing.

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
C.1	The data processor's management has approved a written information security policy, which has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed. An assessment of whether the IT security policy should be updated is carried out on an ongoing basis – and at least once a year.	Inspected that an information security policy exists which management has considered and approved within the past year. Inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No exceptions noted.
C.2	The data processor's management has ensured 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 security measures and security of processing in data processing agreements entered into. Inspected, in a sample of 3 data processing agreements, that the requirements in the agreements are covered by the information security policy's requirements for security measures and security of processing.	No exceptions noted.
C.3	Screening of the data processor's employees is carried out in connection with employment.	Inspected that formalised procedures exist that ensure screening of the data processor's employees in connection with employment. Inspected, in a sample of 3 data processing agreements, that the requirements for screening of employees in the agreements are covered by the data processor's procedures for screening.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
C.4	Upon employment, employees sign a confidentiality agreement. In addition, the employee is introduced to the information security policy and procedures regarding data processing as well as other relevant information in connection with the employee's processing of personal data.	Inspected, in a sample of 1 newly hired employee at the time of the report, that the employee has signed a confidentiality agreement. Inspected, in a sample of 1 newly hired employee at the time of the report, that the employee has been introduced to: • The information security policy • Procedures regarding data processing and other relevant information.	No exceptions noted.
C.5	Upon resignation, the data processor has implemented a process that ensures that the user's privileges become inactive or cease, including that assets are collected.	Inspected procedures that ensure that resigned employees' privileges are deactivated or cease upon resignation, and that assets such as access cards, PC, mobile phone, etc. are collected. Inspected, in a sample of 1 resigned employee at the time of the report, that privileges have been deactivated or have ceased, and that assets have been collected.	No exceptions noted.
C.6	Upon resignation, the employee is informed that the signed confidentiality agreement remains in force and that the employee is subject to a general duty of confidentiality in relation to the processing of personal data that the data processor carries out for the data controllers.	Inspected that formalised procedures exist that ensure that resigned employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. Inspected, in a sample of 1 resigned employee at the time of the report, that there is documentation that the confidentiality agreement and general duty of confidentiality are maintained.	No exceptions noted.
C.7	Awareness training of the data processor's employees in relation to IT security in general and security of processing in relation to personal data is carried out on an ongoing basis.	Inspected that the data processor offers awareness training to employees covering general IT security and security of processing in relation to personal data. Inspected documentation that all employees who either have access to or process personal data have completed the awareness training offered.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

Control objective D:

Procedures and controls are complied with that ensure that personal data can be deleted or returned if an agreement to that effect is made with the data controller.

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
D.1	Written procedures exist that include a requirement that personal data are retained and deleted in accordance with the agreement with the data controller. The procedures are reviewed for updates on an ongoing basis – and at least annually.	Inspected that formalised procedures exist for retention and deletion of personal data in accordance with the agreement with the data controller. Inspected that the procedures have been updated.	No exceptions noted.
D.2	The following specific requirements for the data processor's retention periods and deletion routines have been agreed: *- The data owner must notify the data processor in writing no later than 30-90 days before the termination of the Main Agreement whether all personal data are to be deleted or returned to the data owner. Where the personal data are returned to the data owner, the data processor must also delete any copies. The data processor must ensure that any sub-processors likewise comply with the data owner's notification.* *- Deletion of personal data upon termination of the data processing agreement.*	Inspected that the existing procedures for retention and deletion contain the specific requirements for the data processor's retention periods and deletion routines. Inspected, in a sample of 3 data processing operations from the data processor's overview of processing activities, that there is documentation that personal data are retained in accordance with the agreed retention periods. Inspected, in a sample of 3 data processing operations from the data processor's overview of processing activities, that there is documentation that personal data have been deleted in accordance with the agreed deletion routines.	No exceptions noted.
D.3	Upon termination of the processing of personal data for the data controller, data are, in accordance with the agreement with the data controller: • Returned to the data controller and/or • Deleted, where this does not conflict with other legislation.	Inspected that formalised procedures exist for handling the data controller's data upon termination of the processing of personal data. Inspected, in a sample of 3 terminated data processing operations at the time of the report, that there is documentation that the agreed deletion or return of data has been carried out.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

Control objective E:

Procedures and controls are complied with that ensure that the data processor stores personal data only in accordance with the agreement with the data controller.

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
E.1	Written procedures exist that include a requirement that personal data are stored only in accordance with the agreement with the data controller. The procedures are reviewed for updates on an ongoing basis – and at least annually.	Inspected that formalised procedures exist to ensure that personal data are stored and processed only in accordance with the data processing agreements. Inspected that the procedures have been updated.	No exceptions noted.
E.2	The data processor's data processing, including storage, may only take place at the locations, countries or territories approved by the data controller.	Inspected that the data processor has a comprehensive and updated overview of processing activities stating locations, countries or territories. Inspected, in a sample of 3 data processing operations from the data processor's overview of processing activities, that there is documentation that the data processing, including storage of personal data, takes place only at the locations stated in the data processing agreement – or otherwise approved by the data controller.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

Control objective F:

Procedures and controls are complied with that ensure that only approved sub-processors are used, and that the data processor, in following up on their technical and organisational measures to protect the rights of data subjects and the processing of personal data, ensures satisfactory security of processing.

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
F.1	Written procedures exist that include a requirement that personal data are stored only in accordance with the agreement with the data controller. The procedures are reviewed for updates on an ongoing basis – and at least annually.	Inspected that formalised procedures exist for the use of sub-processors, including requirements for sub-processing agreements and instructions. Inspected that the procedures have been updated.	No exceptions noted.
F.2	The data processor uses only sub-processors for the processing of personal data that have been specifically or generally approved by the data controller.	Inspected that the data processor has a comprehensive and updated overview of the sub-processors used. Inspected, in a sample of 2 sub-processors from the data processor's overview of sub-processors, that there is documentation that the sub-processor's data processing is covered by the data processing agreements – or is otherwise approved by the data controller.	No exceptions noted.
F.3	In the event of changes in the use of generally approved sub-processors, the data controller is notified in good time so as to be able to object and/or withdraw personal data from the data processor. In the event of changes in the use of specifically approved sub-processors, these have been approved by the data controller.	Inspected that formalised procedures exist for notifying the data controller of changes in the use of sub-processors.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
F.4	The data processor has imposed on the sub-processor the same data protection obligations as those provided for in the data processing agreement or similar with the data controller.	Inspected that signed sub-processing agreements exist with the sub-processors used that appear in the data processor's overview. Inspected, in a sample of 2 sub-processing agreements, that these contain the same requirements and obligations as set out in the data processing agreements between the data controllers and the data processor.	No exceptions noted.
F.5	The data processor has an overview of approved sub-processors, stating: • Name • CVR no. • Address • Description of the processing.	Inspected that the data processor has a comprehensive and updated overview of sub-processors used and approved.	No exceptions noted.
F.6	The data processor, on the basis of an updated risk assessment of each sub-processor and the activity taking place at that sub-processor, carries out ongoing follow-up thereon through meetings, inspections, review of an audit report or similar. The data controller is informed of the follow-up carried out at the sub-processor.	Inspected that formalised procedures exist for follow-up on processing activities at the sub-processors and compliance with the sub-processing agreements. Inspected documentation that a risk assessment has been performed of each sub-processor and the current processing activity at that sub-processor. Inspected documentation that appropriate follow-up has been performed on technical and organisational measures, security of processing at the sub-processors used, third-country transfer basis and the like. Inspected documentation that information on follow-up at sub-processors is communicated to the data controller so that it can arrange any supervision.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

Control objective G:

Procedures and controls are complied with that ensure that the data processor transfers personal data to third countries or international organisations only in accordance with the agreement with the data controller on the basis of a valid transfer basis.

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
G.1	Written procedures exist that include a requirement that the data processor transfers personal data to third countries or international organisations only in accordance with the agreement with the data controller on the basis of a valid transfer basis. The procedures are reviewed for updates on an ongoing basis – and at least annually.	Inspected that formalised procedures exist that ensure that personal data are transferred to third countries or international organisations only in accordance with agreement with the data controller on the basis of a valid transfer basis. Inspected that the procedures have been updated.	No exceptions noted.
G.2	The data processor may only transfer personal data to third countries or international organisations on instructions from the data controller.	Inspected that the data processor has a comprehensive and updated overview of transfers of personal data to third countries or international organisations. Inspected, in a sample of 3 data transfers from the data processor's overview of transfers, that there is documentation that the transfer has been agreed with the data controller in the data processing agreement or subsequently approved.	No exceptions noted.
G.3	In connection with the transfer of personal data to third countries or international organisations, the data processor has assessed and documented that a valid transfer basis exists.	Inspected that formalised procedures exist for ensuring a valid transfer basis. Inspected that the procedures have been updated. Inspected, in a sample of 3 data transfers from the data processor's overview of transfers, that there is documentation of a valid transfer basis in the data processing agreement with the data controller, and that transfers have only taken place to the extent agreed with the data controller.	Activecampaign LLC, Zendesk Inc. and Microsoft Corporation are used as sub-processors. All three companies are registered under the EU–US Data Privacy Framework, and management has prepared a TIA for all three.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

Control objective H:

Procedures and controls are complied with that ensure that the data processor can assist the data controller with disclosure, rectification, erasure or restriction of information on the processing of personal data to the data subject.

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
H.1.	Written procedures exist that include a requirement that the data processor shall assist the data controller in relation to data subjects' rights. The procedures are reviewed for updates on an ongoing basis – and at least annually.	Inspected that formalised procedures exist for the data processor's assistance to the data controller in relation to data subjects' rights. Inspected that the procedures have been updated.	No exceptions noted.
H.2	The data processor has established procedures which, to the extent agreed, enable timely assistance to the data controller in relation to disclosure, rectification, erasure or restriction of, and information about, the processing of personal data to the data subject.	Inspected that the existing procedures for assistance to the data controller contain detailed procedures for: • Disclosure of information • Rectification of information • Erasure of information • Restriction of processing of personal data • Information about the processing of personal data to the data subject. Inspected documentation that the systems and databases used support the performance of the detailed procedures mentioned.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

Control objective I:

Procedures and controls are complied with that ensure that any security breaches can be handled in accordance with the data processing agreement entered into.

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
I.1	Written procedures exist that include a requirement that the data processor shall notify the data controllers in the event of a personal data breach. The procedures are reviewed for updates on an ongoing basis – and at least annually.	Inspected that formalised procedures exist that contain requirements for notifying the data controllers in the event of a personal data breach. Inspected that the procedure has been updated.	No exceptions noted.
I.2	The data processor has established the following controls for identifying any personal data breaches: • Employee awareness • Monitoring of network traffic • Follow-up on logging of access to personal data.	Inspected that the data processor offers awareness training to employees in relation to identifying any personal data breaches. Inspected documentation that network traffic is monitored and that follow-up takes place on anomalies, monitoring alerts, transfer of large files, etc. Inspected documentation that timely follow-up takes place on logging of access to personal data, including follow-up on repeated access attempts.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

4. Control objectives, control activities, tests and results thereof (continued)

No.	Data processor's control activity	Tests performed by Baker Tilly	Result of test
I.3	In the event of any personal data breaches, the data processor has notified the data controller without undue delay and no later than 24 hours after becoming aware that a personal data breach has occurred at the data processor or a sub-processor.	Inspected that the data processor has an overview of security incidents stating whether each incident has resulted in a personal data breach. Enquired of the sub-processors whether they have identified any personal data breaches at the time of the report. Inspected that the data processor has included any personal data breaches at sub-processors in the data processor's overview of security incidents. Inspected that all registered personal data breaches at the data processor or the sub-processors have been notified to the affected data controllers without undue delay and no later than 24 hours after the data processor became aware of the personal data breach.	No exceptions noted.
I.4	The data processor has established procedures for assisting the data controller in its notification to the Danish Data Protection Agency: • Nature of the personal data breach • Likely consequences of the personal data breach • Measures taken or proposed to be taken to address the personal data breach.	Inspected that the existing procedures for notifying the data controllers of personal data breaches contain detailed procedures for: • Description of the nature of the personal data breach • Description of the likely consequences of the personal data breach • Description of the measures taken or proposed to be taken to address the personal data breach. Inspected documentation that the existing procedures support that measures are taken to handle the personal data breach.	No exceptions noted.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

GDPR officer at Baker Tilly

Now, for tomorrow



Michael Brink Larsen
State-Authorised Public Accountant
+45 4041 5068
mbl@bakertilly.dk

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

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

Baker Tilly Denmark Godkendt Revisionsaktieselskab, which operates under the name Baker Tilly, is part of the global network Baker Tilly International Ltd., whose member firms are separate and independent legal entities.

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

The signatures in this document are legally binding. The document is signed via Penneo™ secure digital signature. The signatories' identities have been registered, and the information is listed below.

"By my signature I confirm the content and all dates in this document."

Michael Brink Larsen
AIDER Godkendt Revisionsaktieselskab CVR: 35257691
State-Authorised Public Accountant
On behalf of: Baker Tilly Denmark Godkendt Revisionsa…
Serial number: f0c28aad-9c66-4dd4-9020-15bb8d0b4494
IP: 91.221.xxx.xxx
2026-10-06 07:23:54 UTC

Kåre Valentiner Jacobsen
Managing Director
On behalf of: Kåre Bo Jacobsen
Serial number: 374ba3e9-cccc-45c0-8725-14c2786b5471
IP: 109.70.xxx.xxx
2026-10-06 09:22:48 UTC

Penneo document key: ASD3B-K6KLS-GKENU-WSLAI-N9H5A-WKJTC

This document is digitally signed via **Penneo.com.** The signed data are validated by means of the mathematical hash value of the original document. All cryptographic proofs are embedded in this PDF for validation in the future.

This document is sealed with a qualified electronic seal. For more information about Penneo's qualified trust services, see **https://eutl.penneo.com.**

How to verify that the document is original
When you open the document in Adobe Reader, you can see that it is certified by **Penneo A/S**. This proves that the content of the document has been unchanged since the time of signing. Proof of the individual signatories' digital signatures is attached to the document.

You can verify the cryptographic proofs using Penneo's validator, **https://penneo.com/validator,** or other validation services for digital signatures.