



Agillic A/S

Independent auditor's ISAE 3000 type 2 assurance report on information security and measures regarding Agillic's data processing agreements with clients using the SaaS platform throughout the period from 1 January 2024 to 31 December 2024.

Table of contents

1. Independent auditor's report	1
2. Management's statement	4
3. Description of processing	6
4 Agillic's control objectives, control activities, tests and test results	12

1. Independent auditor's report

Independent auditor's ISAE 3000 type 2 assurance report on information security and measures regarding Agillic's data processing agreements with clients using the SaaS platform throughout the period from 1 January 2024 to 31 December 2024

To: Agillic and Agillic's clients

Scope

We were engaged to provide assurance about Agillic's description, in section 3, of Agillic's SaaS platform in accordance with the data processing agreement with data controllers throughout the period from 1 January 2024 to 31 December 2024 ("the description") and about the design and effectiveness of controls related to the control objectives stated in the description.

Agillic uses the sub-data processors GlobalConnect, Amazon Web Services and SAC-IT for hosting the Agillic application, Code4Nord for third-level engineering and LINK Mobility Group for mobile gateway and Unit-IT for managed data centre and infrastructure. The description includes only the control objectives and related controls at Agillic while excluding the control objectives and related controls at the sub-data processors

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

Agillic's responsibilities

Agillic is responsible for: preparing the description and the accompanying statement in section 2 of this report, including the completeness, accuracy and the method of presentation of the description and statement; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Deloitte's independence and quality control

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

Deloitte's responsibilities

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

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information", and additional requirements under Danish audit regulation, to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of the Agillic SaaS platform 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 design and operating effectiveness of controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

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

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

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

Opinion

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

- a) The description fairly presents Agillic's SaaS platform as designed and implemented throughout the period from 1 January 2024 to 31 December 2024;
- b) The controls related to the control objectives stated in the description were appropriately designed and implemented throughout the period from 1 January 2024 to 31 December 2024;
- c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2024 to 31 December 2024.

Description of tests of controls

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

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for data controllers who have used Agillic's SaaS platform and who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves, in assessing whether the requirements of the EU Regulation have been complied with.

Copenhagen, 11 April 2025

Deloitte

Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56



Thomas Kühn
Partner, state-authorized public accountant



Michael Bagger
Partner, CISA

2. Management's statement

Agillic A/S ("Agillic") processes personal data on behalf of clients in accordance with the data processing agreements with data controllers.

The accompanying description has been prepared for the clients of Agillic who have used the Agillic SaaS platform and who have a sufficient understanding to consider the description along with other information, including information about controls operated by the sub-data processors and the data controllers themselves, in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with.

Agillic confirms that:

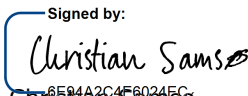
- a) The accompanying description in section 3 fairly presents Agillic's SaaS platform, which is used for processing personal data for data controllers subject to the General Data Protection Regulation throughout the period from 1 January 2024 to 31 December 2024. The criteria used in making this statement were that the accompanying description:
 - (i) Presents how Agillic's activities and controls in relation to the Agillic SaaS platform 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 organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
 - Services performed by a sub-service organisation, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
 - Controls that we, in reference to the scope of Agillic's SaaS platform, 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;
 - 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) Contains relevant information about changes in the data processor's services in the processing of personal data made throughout the period from 1 January 2024 to 31 December 2024.
 - (iii) Does not omit or distort information relevant to the scope of the Agillic SaaS platform 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 Agillic's SaaS platform that the individual data controllers might consider important in their particular circumstances.

- b) The controls associated with the control objectives listed in the accompanying description were appropriately designed and operated effectively throughout the period from 1 January 2024 to 31 December 2024. 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.
 - (iii) The controls were consistently applied as designed and that manual controls were performed by persons with appropriate competence and skills throughout the period from 1 January 2024 to 31 December 2024.
- c) Appropriate technical and organisational measures were established and maintained to comply with the agreements with the data controllers, good data processing practices and relevant requirements for data processors in accordance with the General Data Protection Regulation.

11 April 2025

Agillic A/S

Signed by:

Christian Samsø
CEO

3. Description of processing

Agillic A/S is a Danish software company offering brands a platform through which they can work with data-driven insights and content to create, automate and send personalised communication to millions.

The company has a two-pronged, go-to-market model, and cooperation with best-of-breed technology partners and global solution partners. Apart from Denmark, markets of particular interest are the DACH region and Norway. Target clients are digitally mature and data-driven B2C-businesses in industries such as retail, finance, travel & leisure, NGO and charities, and subscription businesses in e.g. entertainment and gaming, energy and utilities, media and publishing, and technology and software.

3.1. Application/platform/service description

The Agillic platform is created, developed and operated by the company itself. Operations and software development follow commonly established design patterns, industry best practices, and internal codes of conduct, ensuring a secure SaaS platform.

Security policies and processes are based on the relevant ISO 27001 controls and the requirements stipulated in data processor agreements with the clients. The Agillic platform is a Software-as-a-Service (SaaS) platform hosted in secure data centres operated by specialised hosting providers.

3.2. Sub-data processors

Agillic uses the following sub-data processors:

Sub-processor	Brief Description
GlobalConnect , Hørskættens 3, 2630 Taastrup, Denmark, reg. no. 26759722	GlobalConnect provides a managed data centre and infrastructure. Data is encrypted at rest and in transit.
SAC-IT , C/O Frydenlundsvej 30, Bygning E, Frydenlundsvej 30, 2950 Vedbæk, Denmark, reg. no. 28892977	SAC-IT provides a managed data centre and infrastructure. Data is encrypted at rest and in transit.
Amazon Web Services , 1 Burlington Plaza, Burlington Road, Dublin 4, Ireland (part of Amazon Web Services EMEA SARL, Luxembourg, reg. no. B186284)	AWS provides a managed data centre and infrastructure. Data is encrypted at rest and in transit. Encryption keys are not stored in AWS and only kept on a secure location in Denmark.
Code4Nord , Str. Barbu Ștefănescu Delavrancea 8-10, Cluj-Napoca, Romania, reg. no. RO33361133	Code4Nord provides 3rd level engineering services for software development.
<u>Only for clients using Agillic SMS services:</u> LINK Mobility Group , Universitetsgata 2, 0164 Oslo, Norway, reg. no. 984066910	LINK Mobility provides a mobile gateway service.
Unit-IT , Strandvejen 7, 5500 Middelfart, Denmark, reg.no. 15660945	Unit-IT provides a managed data centre and infrastructure. Recipients' personal data is processed and stored via the Agillic platform on managed infrastructure. Data is encrypted at rest and in transit.

3.3. The nature of processing

The Agillic platform is used to create and deliver automated and personalised marketing campaigns across multiple channels, including but not limited to, emails, text messages (SMS), app notifications and in-app messaging, landing pages, and print.

3.4. Personal data

The client designs the data model, including the type of data that the client wants to store about their customers. The client does this without any assistance from Agillic, who does not offer professional services.

The type of personal data being processed is primarily general personal data, including identification data, such as email address, first name, last name, address, postal code and phone number. Other data can be membership data, purchases, permissions, etc. For very few clients, Agillic processes special categories of data.

Categories of typical data subjects falling within the scope of the data processing agreement:

- Client's customers
- Client subscribers and memberships

3.5. Risk assessment

Agillic has performed a risk assessment focusing on business impact and continuity, as well as privacy impact. The risk assessment is based on the information assets and processes that pose a potential risk to the business and/or the privacy of the data subjects, i.e., the recipients' personal data, including the risk of a potential data breach and unauthorised access to personal data.

Agillic has performed the risk assessment by assessing each of the assets for adversarial or accidental threats. Each risk is recorded in the "Asset and Risk Register" and assessed by a risk scoring system based on likelihood, business impact and privacy impact. The risks are reassessed for residual risk upon risk treatment, e.g., controls, mitigation, transfer, etc. The final classification results in a risk score of "Very low".

3.6. Control measures

Agillic has implemented an information security management system (ISMS) based on ISO 27001. As part of the policies, processes and controls in the ISMS, Agillic has implemented controls for processing personal data in the following areas:

- Data processing agreements and instructions (control objective A)
- Technical security measures (control objective B)
- Organisational measures (control objective C)
- Erasure and return of personal data (control objective D)
- Retention of personal data (control objective E)
- Use of sub-processors (control objective F)
- Transfer to third countries (control objective G)
- Assistance to the data controller (control objective H)
- Security breach management (control objective I).

A detailed description of a selection of relevant control measures is available below.

3.6.1. Data processing agreements and instructions (control objective A)

Control objective

Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently in relation to the data processing agreement entered into.

Agillic has data processing agreements in place with all clients and sub-processors compliant with Danish and EU guidelines and does not enter into any agreement which conflicts with Danish law and/or EU regulations.

3.6.2. Technical security measures (control objective B)

Control objective

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

IT security policy

Agillic has in place an IT security policy, which all employees must comply with. The IT security policy is part of the onboarding process that new employees are being introduced to and an annual awareness training for all employees.

Risk assessment

Agillic has a structured risk assessment process in place that takes into consideration possible privacy impacts related to the transfer of data.

Anti-virus

All Agillic workstations are provided with an anti-virus program.

Network segmentation and firewall

Agillic networks and VPN connections are segmented to the effect that unrelated servers cannot communicate directly with each other. A firewall is placed on top of the networks. The network in the office is segmented in two networks; there is a Wi-Fi network for employees and one for guests. The guest network cannot access any internal systems.

User creation

A user is created when a new person is hired as part of the onboarding process. The privileges of the user are determined prior to the onboarding process according to the specific job function.

User termination

Upon termination of a user, it is first assessed whether the accounts contain information that Agillic might need in the future. If the user accounts are assessed as not containing information needed by Agillic in the future, the accounts and data are removed. If the user accounts are assessed as containing information needed by Agillic in the future, the accounts have their passwords reset, and the accounts are locked to ensure that there is no access to the user until needed. An offboarding document is created where the removal of certain access, accounts, etc. is documented.

Privileged access rights

Privileges are documented in the onboarding document and can be cross-checked directly at any given time. Privileged access is only granted if an employee needs it to perform their job function.

System monitoring

All servers have a monitoring agent that sends data to an alerting system to create alarms that are monitored 24/7 by humans with automatic escalation procedures.

Encryption

All communication from the front end to the back end is encrypted using TLS.

Logging

All systems are logged, and the logs are sent to a separate server for handling except for certain low-risk systems, where logs are kept locally.

Change management

All releases are going through a change management process where the changes are approved by a qualified engineer with proper training.

Data in use

To the highest degree feasible, data in at rest or in transit must be secured by one of the following actions:

- Hashing
- Encryption
- Pseudonymisation

Personal data used for development, testing or similar activity is always in a 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.

Vulnerability and penetration scans

All client-faced servers are scanned on a regular basis. The results are documented and vulnerabilities are assessed and handled by the responsible system owner.

Security patching

Agillic systems are upgraded on a regular basis. In the event of a new-found vulnerability with an attached CVE, the systems are manually patched as soon as possible.

Two-factor authentication

Agillic enforces two-factor (2FA) authentication on internal access to clients' data and provides clients with the option to enable 2FA on the Agillic Platform.

3.6.3. Organisational measures (control objective C)

Control objective

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

Agillic has segregation of duties in place at all levels and processes. Agillic also has in place an Information Security Committee, which checks that daily operations are in line with the policies and processes agreed upon. The committee follows up on risk assessments and ensures that the Information Security Management System is effective, and that its documents are reviewed at planned intervals.

All employees are bound by confidentiality agreements and new hires are screened prior to employment. Freelancers and externals must sign NDAs before being granted access to Agillic premises and systems.

3.6.4. Erasure and return of personal data (control objective D)

Control objective

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

Agillic has procedures in place ensuring that personal data can be erased and/or returned. In either case, it is highlighted that the requester must be verified prior to erasure/return of personal data.

Recipient data collected by our clients can be deleted by the clients via the Agillic platform UI. In case a client terminates its engagement with Agillic, procedures are in place to ensure that all data will be deleted.

3.6.5. Storage of personal data (control objective E)

Control objective

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

Clients are responsible for designing the data model, which involves defining the type of data they want to process. In case Agillic employees must support and/or access client data, this is only done in accordance with the data processing agreement and upon written request by the client.

Requests are documented in our service management tool, and all access to client data is logged.

3.6.6. Use of sub-processors (control objective F)

Control objective

Procedures and controls are implemented to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

Agillic will not engage sub-processors without the prior specific or general written authorisation of clients and at least 30 days notification prior to the engagement of new sub-processors, and clients may object to any such change.

Where Agillic engages a sub-processor, the same data protection obligations as set out for Agillic shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR.

In the event of bankruptcy, Agillic's sub-processors are instructed to delete all data. Data cannot be returned by sub-processors directly to clients as the data is pseudonymised, encrypted, impossible for the sub-processor to decrypt, and sub-processors do not know who Agillic's clients are.

3.6.7. Transfer to third countries (control objective G)

Control objective

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

Agillic only transfers personal data to third countries or international organisations based on a written agreement and documented instructions from the data controller. This is further outlined in the data processing agreements that have been entered into with Agillic's clients, where it is stated that personal data must only be transferred to third countries or international organisations in accordance with an agreement with the data controller on the basis of a valid transfer. Agillic uses Amazon Web Services EMEA SARL, Luxembourg as a sub-processor for hosting. Data is stored in Ireland in accordance with Datatilsynet's Guidance on the use of cloud.

In certain cases, clients may want to upload parts of their data to Alphabet (Google) or Meta (Facebook) where data can be transferred to third countries. However, this requires that the client activates the ability to perform the transfers to Google or Facebook in the Agillic platform, and then actually carries out the specific transfers themselves. In such cases, Agillic will make sure to implement a secure transfer mechanism and that all transfers to Alphabet (Google) or Meta (Facebook) are encrypted with a SHA 256 algorithm for hashing and that every transfer is logged by the Agillic platform.

3.6.8. Assistance to data controller (control objective H)

Control objective

Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting or restricting information on the processing of personal data to the data subject.

Agillic has in place procedures supporting its clients in handling their obligations regarding data subjects' rights, if requested.

Agillic will also, if requested, help the clients in ensuring compliance with the obligations pursuant to articles 32 (implementing appropriate technical and organisational measures), 35 (carrying out data protection impact assessments) and 36 (consulting the data protection authorities prior to processing) of the GDPR, however, taking into account the nature of processing and the information available to Agillic.

3.6.9. Security breach management (control objective I)

Control objective

Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.

Agillic has implemented a procedure ensuring that all presumed data breaches are reported to the data controller without any delay. There is a detailed list of information that Agillic must report to the data controller in order for the controller to assess whether or not there is any risk for the data subject.

Agillic will assist the data controller in the analysis, if asked to.

The sub-processors are obliged to report to Agillic without any delay in case they suspect any data breach.

3.7 Complementary controls at the data controllers

The system owner on the Agillic platform on the client side is determined by the individual client, and it is the system owner's (on the client side) responsibility that the individual system's users on the Agillic platform (on the client side) are only granted access based on a work-related need. Access to the Agillic platform is only created at the requests of the system owner or other authorised employees. Furthermore, users are only terminated at the request of the system owner or other authorised employees (on the client side), and it is the responsibility of the client to ensure that users are terminated in a timely manner by notifying Agillic thereof.

We expect our clients to take upon them their data controller responsibility, ensuring that:

- Recipients have given their valid consent where needed;
- Processing is fair and lawful;
- The data minimisation principle is used as a guideline for collecting data;
- Data subjects are given instructions on how to exercise their rights;
- The data controller requests Agillic in cases of data erasure of data subjects if the data controller needs assistance to delete data in the Agillic Platform UI;
- A legal basis for processing data exists at the time of transfer of personal data to Facebook and Google – including that any consent is freely given, specific, informed, unambiguous as well as explicit, if required;
- Any breaches of personal data are reported to the Danish Protection Agency.

4 Agillic's control objectives, control activities, tests and test results

4.1 Introduction

This report is intended to provide Agillic's clients with information about Agillic's controls that may affect the processing of personal data and at the same time to inform data controllers on behalf which Agillic processes personal data of the functionality of the controls that were tested. This section, when combined with an understanding and assessment of the controls of the data controllers, is intended to assist the data controllers in assessing the risks associated with the outsourced processing of personal data that may be affected by the controls of Agillic.

Our testing of Agillic's controls is limited to the control objectives and related controls listed in the control matrix below in this section and is not extended to include all controls stated in the system description and the controls expected to be implemented by the data controllers to meet the control objectives.

It is the responsibility of the data controller to evaluate this information in relation to the controls that exist with the data controller. If certain complementary controls are not present at the data controller, Agillic's controls may not be able to compensate for such weaknesses.

4.2 Test of controls

The tests performed when determining the controller's functionality consist of one or more of the following methods:

Method	Description
Inquiry	Inquiry with Agillic's selected personnel
Observation	Observation of the execution of the control
Inspection	Inspection of documents and reports which contain an indication of the execution of controls. This includes, among other things, reading through and considering reports and other documentation to assess whether specific controls are designed and implemented effectively. Furthermore, it is assessed whether controls are monitored and supervised sufficiently and at appropriate intervals.
Re-performance	Repetition of the relevant control to verify that the control functions as intended.

4.3 Control objective, control activity and test results

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

4.4 Control objectives, control activities, tests and results

Control objective A Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
A.1	<p>Written procedures exist which include a requirement that personal data must be processed when instructions to this effect are available.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte checked by way of inspection that formalised procedures exist to ensure that personal data is only processed according to instructions.</p> <p>Deloitte 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 data processing.</p> <p>Deloitte checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	<p>Deloitte checked by way of inspection that Management ensures that personal data is only processed according to instructions.</p> <p>Deloitte has inspected samples of data processing agreements and checked by way of inspection that processes of personal data take place in accordance with instructions.</p>	No exceptions noted.
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or Member State data protection provisions.	<p>Deloitte checked by way of inspection that formalised procedures exist ensuring verification that personal data is not processed against the Regulation or other legislation.</p> <p>Deloitte checked by way of inspection that procedures are in place for informing the data controller of cases where the processing of personal data is deemed against legislation.</p>	<p>We have been informed that there has not been any cases where the processing of personal data has infringed the Regulation or other European Union or Member State data protection provisions during the assurance period.</p> <p>No exceptions noted.</p>

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
B.1	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte checked by way of inspection that formalised procedures exist to ensure establishment of the safeguards agreed.</p> <p>Deloitte checked by way of inspection that procedures are up to date.</p> <p>Deloitte checked by way of inspection of samples of a data processing agreement that the safeguards agreed have been established.</p>	No exceptions noted.
B.2	The data processor has performed a risk assessment for all client-facing systems 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.	<p>Deloitte checked by way of inspection that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security.</p> <p>Deloitte checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data.</p> <p>Deloitte checked by way of inspection that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment.</p> <p>Deloitte has checked by way of inspection that the data processor has implemented the safeguards agreed with the data controller.</p>	No exceptions noted.
B.3	For the systems and databases used in the processing of personal data, anti-virus software has been installed, which is updated on a regular basis.	Deloitte checked by way of inspection of samples that for the systems and databases used in the processing of personal data, anti-virus software has been installed.	No exceptions noted.

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
		Deloitte checked by way of inspection that anti-virus software is up to date.	
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	<p>Deloitte checked by way of inspection that external access to systems and databases used in the processing of personal data takes place only through a secured firewall.</p> <p>Deloitte has checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy.</p>	No exceptions noted.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	<p>Deloitte inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.</p> <p>Deloitte inspected network diagrams and other network documentation to ensure appropriate segmentation.</p>	No exceptions noted.
B.6	Access to personal data is restricted to users with a work-related need for such access.	<p>Deloitte checked by way of inspection that formalised procedures are in place for restricting users' access to personal data.</p> <p>Deloitte 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 needs.</p> <p>Deloitte checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data.</p>	No exceptions noted.

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
		Deloitte inspected samples of users access to systems and databases and confirmed that such access rights are restricted to a work-related need.	
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: <ul style="list-style-type: none"> - System availability - Capacity - Memory 	Deloitte checked by way of inspection of samples that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. Deloitte inspected samples of registered system alarms that follow-up actions were performed.	No exceptions noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	Deloitte 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. Deloitte checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email. Deloitte inquired about incidents regarding unencrypted transmission of sensitive and confidential personal data has taken place during the assurance period and whether data controllers have been appropriately informed thereof.	No exceptions noted.

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
B.9	<p>Logging of the following matters has been established in systems, databases and networks:</p> <ul style="list-style-type: none"> Activities performed by system administrators and others holding special rights; Security incidents comprising: <ul style="list-style-type: none"> Changes in log setups, including disabling of logging; Changes in users' system rights; Failed attempts to log on to systems, databases or networks. <p>Logon data is protected against manipulation and technical errors and are reviewed regularly.</p>	<p>Deloitte 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.</p> <p>Deloitte checked by way of inspection of samples that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated.</p> <p>Deloitte checked by way of inspection that user activity data collected in logs is protected against manipulation or deletion.</p>	<p>No exceptions noted.</p>
B.10	<p>Personal data used for development, testing or similar activity is always in a pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.</p>	<p>Deloitte 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 a pseudonymised or anonymised form.</p>	<p>Deloitte has noted that Agillic uses "dummy data" in development and test environments.</p> <p>No exceptions noted.</p>
B.11	<p>The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.</p>	<p>Deloitte checked by way of inspection that formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests.</p> <p>Deloitte checked by way of inspection of samples that documentation exists regarding regular testing of the technical measures established.</p>	<p>No exceptions noted.</p>

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
		Deloitte 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.	
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.	<p>Deloitte checked by way of inspection that formalised procedures exist for handling changes to systems, databases or networks, including handling of releases of relevant updates, patches and security patches.</p> <p>Deloitte checked by way of inspection of samples that approved updates, patches and security patches, including system-, databases- or network releases have been deployed using established change procedures.</p>	No exceptions noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	<p>Deloitte checked by way of inspection that formalised procedures exist for granting and removing users' access to systems and databases used to process personal data.</p> <p>Deloitte checked by way of inspection samples of employees' access to systems and databases and confirmed that the user access granted has been authorised and that a work-related need exists.</p> <p>Deloitte checked by way of inspection of samples of resigned employees that their access to systems and databases was deactivated or removed on a timely basis.</p>	No exceptions noted.

Control objective B Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
		Deloitte checked by way of inspection that documentation exists that user access granted is evaluated and authorised on a regular basis – and at least once a year.	
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	<p>Deloitte 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.</p> <p>Deloitte checked by way of inspection that users can only process personal data that involve a high risk for the data subjects by using two-factor authentication.</p>	No exceptions noted.
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 is stored and processed.	<p>Deloitte 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 is stored and processed.</p> <p>Deloitte checked by way of inspection of documentation that only authorised persons have physical access to premises and data centres at which personal data is stored and processed.</p>	No exceptions noted.

Control objective C Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
C.1	<p>The 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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.</p>	<p>Deloitte checked by way of inspection that an information security policy exists that Management has considered and approved within the past year.</p> <p>Deloitte inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.</p>	No exceptions noted.
C.2	<p>The management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.</p>	<p>Deloitte 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.</p> <p>Deloitte inspected samples of data processing agreements to confirm that the requirements in these agreements are covered by the requirements of the information security policy for safeguards and security of processing.</p>	No exceptions noted.
C.3	<p>Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.</p>	<p>Deloitte checked by way of inspection of samples of employees appointed during the assurance period that the relevant employees have signed a confidentiality agreement.</p> <p>Deloitte checked by way of inspection of employees appointed during the assurance period that the relevant employees has been introduced to the information security policy and the procedures for processing data, as well as other relevant information.</p>	No exceptions noted.

Control objective C Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.			
C.4	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, and that assets are returned.	<p>Deloitte inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets, such as access cards, computers, mobile phones, etc., are returned.</p> <p>Deloitte checked by way of inspection of employees resigned during the assurance period that their rights have been deactivated or terminated and that assets have been returned.</p>	No exceptions noted.
C.5	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	<p>Deloitte 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.</p> <p>Deloitte checked by way of inspection of employees resigned during the assurance period that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality.</p>	No exceptions noted.
C.6	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	<p>Deloitte checked by way of inspection that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data.</p> <p>Deloitte inspected documentation that employees who have either access to or process personal data have completed the awareness training provided.</p>	No exceptions noted.

Control objective D Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
D.1	<p>Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte checked by way of inspection that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller.</p> <p>Deloitte checked by way of inspection that the procedures are up to date.</p>	No exceptions noted.
D.2	<p>The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines:</p> <ul style="list-style-type: none"> The data controllers can both delete and return a data subject's personal data themselves in the system. 	<p>Deloitte checked by way of inspection that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines.</p> <p>Deloitte checked by way of inspection that the data controllers can both delete and return a data subject's personal data themselves in the system.</p>	No exceptions noted.
D.3	<p>Upon termination of the processing of personal data for the data controller, data has, in accordance with the agreement with the data controller, been:</p> <ul style="list-style-type: none"> Returned to the data controller; and/or Deleted if this is not in conflict with other legislation. 	<p>Deloitte checked by way of inspection that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data.</p> <p>Deloitte checked by way of inspection of terminated data processing sessions during the assurance period that documentation exists that the agreed deletion or return of data has taken place.</p>	No exceptions noted.

Control objective E Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
E.1	<p>Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte checked by way of inspection that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements.</p> <p>Deloitte checked by way of inspection that the procedures are up to date.</p> <p>Deloitte has checked by way of inspection of a sample of 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.</p>	No exceptions noted.
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	<p>Deloitte inspected that the data processor has a complete and up-to-date list of processing activities stating localities, countries or regions.</p> <p>Deloitte checked by way of inspection of samples of data processing session 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.</p>	No exceptions noted.

Control objective F

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

No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
F.1	<p>Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-data processing agreements and instructions.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte 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.</p> <p>Deloitte checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
F.2	<p>The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.</p>	<p>Deloitte checked by way of inspection that the data processor has a complete and up-to-date list of sub-data processors used.</p> <p>Deloitte checked by way of inspection of one sub-data processor 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 agreement – or otherwise as approved by the data controller.</p>	No exceptions noted.
F.3	<p>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.</p>	<p>Deloitte checked by way of inspection that formalised procedures are in place for informing the data controller when changing the sub-data processors used.</p> <p>Deloitte inspected documentation that the data controller was informed when changing the sub-data processors used throughout the assurance period.</p>	No exceptions noted.
F.4	<p>The data processor has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement with the data controller or similar document.</p>	<p>Deloitte 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.</p>	No exceptions noted.

Control objective F

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

No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
		Deloitte checked by way of inspection of a sample of one sub-data processing agreement that it includes the same requirements and obligations as those stipulated in the data processing agreements between the data controllers and the data processor.	
F.5	The data processor has a list of approved sub-processors disclosing: <ul style="list-style-type: none">• Name;• Business registration no.;• Address;• Description of the processing activities.	Deloitte checked by way of inspection that the data processor has a complete and up-to-date list of sub-data processors used and approved. Deloitte checked by way of inspection that the list at least includes the required details about each sub-data processor.	No exceptions noted.
F.6	Based on an up-to-date 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.	Deloitte checked by way of inspection that formalised procedures are in place for following up on processing activities at sub-data processors and complying with the sub-data processing agreements. Deloitte inspected documentation that each sub-data processor and the current processing activity at such processor are subjected to risk assessment. Deloitte inspected 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.	No exceptions noted.

Control objective G Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
G.1	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte checked by way of inspection that formalised procedures exist to ensure that personal data is only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.</p> <p>Deloitte checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions from the data controller.	<p>Deloitte checked by way of inspection that the data processor has a complete and up-to-date list of transfers of personal data to third countries or international organisations.</p> <p>Deloitte checked by way of inspection of a sample of 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.</p>	No exceptions noted.
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	<p>Deloitte checked by way of inspection that formalised procedures are in place for ensuring a valid basis of transfer.</p> <p>Deloitte checked by way of inspection that procedures are up to date.</p> <p>Deloitte checked by way of inspection of a sample of data transfer 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</p>	No exceptions noted.

Control objective G

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

No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
		far as this was arranged with the data controller.	

Control objective H Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting or restricting information on the processing of personal data to the data subject.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
H.1	<p>Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte checked by way of inspection that formalised procedures are in place for the data processor's provision of assistance to the data controller in relation to the rights of data subjects.</p> <p>Deloitte checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
H.2	The data processor has established procedures, in so far as this was agreed, that enable timely assistance to the data controller in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects.	<p>Deloitte checked by way of inspection that the procedures in place for assisting the data controller include detailed procedures for:</p> <ul style="list-style-type: none"> • Handing out personal data; • Correcting personal data; • Deleting personal data; • Restricting the processing of personal data; • Providing information about the processing of personal data to data subjects. <p>Deloitte checked by way of inspection of documentation that the systems and databases used support the performance of the relevant detailed procedures.</p>	<p>We were informed that no requests for assistance by the data controllers were received during the assurance period.</p> <p>No exceptions noted.</p>

Control objective I Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
I.1	<p>Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Deloitte checked by way of inspection that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches.</p> <p>Deloitte checked by way of inspection that procedures are up to date.</p>	No exceptions noted.
I.2	<p>The data processor has established the following controls to identify any personal data breaches:</p> <ul style="list-style-type: none"> • Awareness of employees; • Monitoring of network traffic; • Follow-up on logging of access to personal data. 	<p>Deloitte checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches.</p> <p>Deloitte checked by way of inspection of documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on.</p> <p>Deloitte 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 a timely basis.</p>	No exceptions noted.
I.3	<p>If any personal data breach occurred, the data processor informed the data controller without undue delay after having become aware of such personal data breach at the data processor or a sub-data processor.</p>	<p>Deloitte checked by way of inspection that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.</p> <p>Deloitte 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.</p>	<p>We were informed that no personal data breaches occurred during the assurance period.</p> <p>No exceptions noted.</p>

Control objective I Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.			
No.	Agillic's control activity	Test performed by Deloitte	Deloitte's test results
		Deloitte has 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.	
I.4	<p>The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency:</p> <ul style="list-style-type: none"> • Nature of the personal data breach; • The probable consequences of the personal data breach; • Measures taken or proposed to be taken to respond to the personal data breach. 	<p>Deloitte 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:</p> <ul style="list-style-type: none"> • Describing the nature of the personal data breach; • Describing the probable consequences of the personal data breach; • Describing measures taken or proposed to be taken to respond to the personal data breach. <p>Deloitte checked by way of inspection of documentation that the procedures available support that measures are taken to respond to the personal data breach.</p>	<p>We were informed that no requests for assistance on reporting were received during the assurance period.</p> <p>No exceptions noted.</p>