inforevision

# Dialogue One A/S

Trekronergade 126F, 2.
2500 Valby

ISAE 3000, type 2

# Independent auditor's ISAE 3000 assurance report on the description of controls aimed at information security and processing of personal data for the period 1st June 2020 to 30th September 2021

CVR.NR. 26 84 57 85

**Table of content**





S.nr. 302840

JR/SO

# 1. Management's statement

Dialogue One A/S processes personal data on behalf of our costumers who are the data controllers with reference to the data processing agreements.

The accompanying description has been prepared for the data controllers, who has used Dialogue One A/S's sales, marketing and services, and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation) have been complied with.

Dialogue One A/S confirms that:

a) The accompanying description, in section 2, provides an accurate description of Dialogue One A/S's service, that processes personal data for data controllers covered by the Regulation throughout the period from 1st June 2020 to 30th September 2021. The criteria used in making this statement were that the accompanying description:

(i) Presents how Dialogue One A/S's systems 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 controllers;
- The procedures ensuring that the persons authorized to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
- The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation;
- The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects;
- The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- Controls that we have assumed would be implemented by the data controllers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description;
- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data;

(ii) Includes relevant information about changes in the service in the processing of personal data in the period from 1st June 2020 to 30th September 2021;

(iii) Does not omit or distort information relevant to the scope of the service being described for the processing of personal data while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the service that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1st June 2020 to 30th September 2021. The criteria used in making this statement were that:

(i) The risks that threatened the achievement of the control objectives stated in the description were identified;

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1st June 2020 to 30th September 2021.

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

Valby, 17th November 2021
Dialogue One A/S

Ole Klitgaard
CEO

# 2. Description of processing

Dialogue One A/S is a sales and service organisation whose primary objective is to deliver market activity solutions to Danish and German clients in their selected areas.

The sustainability of the concepts is also being tested in other geographic markets and has so far also shown its strength and durability for Norwegian clients and is also expected to be applicable to the UK. The treatment and support of data will be developed in line with the requirements of a new market.

Client agreements are individualized and adapted with a particular focus on the client's business situation and need for flexibility, transparency and value creation. The Client collaboration has a significant degree of integration and interaction in systems and processes and is thus limited in number.

Dialogue One A/S 's role is therefore primarily to be a data processor for their clients. The client is the data controller. The Client and Dialogue One A/S enter a data processing agreement that reflects this.

To deliver the services at competitive prices, Dialogue One A/S uses up-to- date IT -based dialogue tools and highly qualified Danish and German employees supporting an efficient and secure organization.

Dialogue One A/S is an innovative, modern and attractive workplace that attracts, maintains and develops competent and motivated employees.

### The nature of the data processing

Dialogue One A/S ’s main activity is collection, storage, processing, use and distribution of business data on behalf of clients for the purpose of maintaining and developing clients' markets.

Dialogue One A/S thus processes personal data (non-sensitive), which is business critical for our clients and therefore maintains a high level of information security.

Dialogue One A/S uses suppliers/sub-data processors to deliver the services and to manage the personal data of the employees. Dialogue One A/S has data processing agreements with all significant suppliers.

### Personal data

As a data processor, Dialogue One A/S is working under instructions from our clients. The instructions given are individual for each client. The data processing agreements include, but are not limited to, the following types of personal data

- Company Name
- Person Name
- Position/function/Field/industry
- Business Address
- E-mail
- Telephone number – Direct or mobile phone No.
- Dialog history

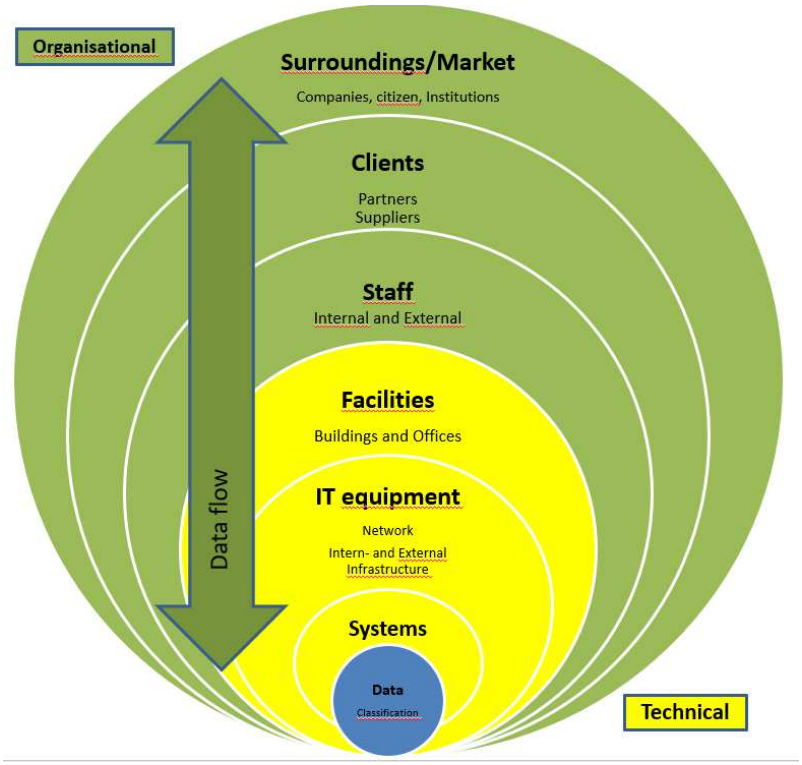
Categories of registered persons subject to the data processing Agreement:

- Employees/stakeholders in private and public companies, associations and stakeholder organizations

None of the data recorded for clients is of a particularly sensitive nature, nor of a quantity and scope that would require the designation of a DPO – Data Protection Officer.

## Operational actions – Data protection

The protection of the business-critical client data and Dialogue One A/S 's own data is based on the following model, where data flows generate technical and organizational measures to protect the data




The desire to maintain a high level of data protection is achieved through technical and organizational measures focusing on:

- Confidentiality, integrity, and availability of systems and data in relation to the IT risk assessment established for each system/data.
- Protection of IT assets, staff competencies, organisation's image and information/data in Dialogue One A/S 's custody.

In order to maintain and develop the high level of safety Dialogue One A/S

- Develop guidelines and business processes that make information security an integral part of the operations and daily work
- Contractual and supplier management ensures that the use of external consultants, partners and suppliers does not compromise the level of information security
- A systematic and structured follow-up to information security ensures the optimization and ongoing maintenance of information security policy.

The digital data protection is ensured by using Microsoft 365 among other measures. Microsoft 365 includes some of the market's most secure data protection solutions including encryption, firewall and antivirus and corresponding requirements for physical protection in Dialogue One A/S 's premises and at hosting partners.

## Risk assessment

The Board of Directors and the Executive Board of Dialogue One A/S shall continuously assess which elements of operations constitute a risk. These are listed and for each element the risk/threat is assessed

- Likelihood of the threat occurring
- Impact on financials, operations and the outside world/stakeholders
- Preventive actions to reduce the overall risk

The risk assessment includes, but is not limited to, an assessment of threats to the

- The client's data
- The organization of suppliers, consultants and co-operative partners
- Physical and digital data protection

The development of the scope of client and own data is continuously followed, and processes and systems adapted to this development. Thus, a sharp increase in the number of employees in Dialogue One A/S means a need for automation and stronger system support to increase security and general attention to data processing. A similar need can be expected in the processing of client data.

## Internal controls – self-checks

It is Dialogue One A/S s policy to ensure that the daily operations are carried out within the framework of the information security policies and thus to constantly improve the security. Dialogue One A/S therefore conducts structured and systematic self-checks.

Dialogue One A/S makes simultaneous use of external IT audits to monitor and maintain information security and carry out checks that ensure compliance with relevant legislation.

Self-monitoring is ensuring, but not limited to

- Suppliers – or sub-data processing contractors - who require ISAE3402 or equivalent statement that these are updated and applicable and that any requirements for self-checks in Dialogue One A/S are respected
- Registers with clients, employees and suppliers are up-to-date, including agreements and other documentation
- Storing and deletion of data is done according to the applicable instructions

The completed self-checks are documented.

## Complementary checks at the data controllers

The data controllers – Dialogue One A/S 's clients – have in addition to the self controls made by Dialogue One A/S, the following obligations:

- Ensure that the instructions for processing data are accurate, appropriate and in accordance with the data processing agreement and include the data collected and processed
- Ensure that the data covered by the instructions are not sensitive data
- Ensure that the registered rights, when contacted, can be complied, including that the data controller's users are aware of the data processing agreement and the related Framework Agreement

# 3. Independent auditor's ISAE 3000 assurance report on the description of controls aimed at information security and processing of personal data

**To the management of Dialogue One A/S and their customers.**

**Scope**
We were engaged to provide assurance about Dialogue One A/S's description in section 2 of service for processing personal data in accordance with the data processing agreement with the data controllers throughout the period from 1st June 2020 to 30th September 2021 ("the Description") and about the design and operating effectiveness of the controls related to the control objectives stated in the Description.

We express reasonable assurance in our conclusion.

**Dialogue One A/S's responsibility**
Dialogue One A/S is responsible for: preparing the Description and the accompanying statement in section 1, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

**Auditor's independence and quality control**
We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by FSR - Danish Auditors (Code of Ethics for Professional Accountants), which are based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional conduct.

**Info**revision is subject to the International Standard on Quality Control (ISQC 1) and accordingly uses and maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

**Auditor's responsibilities**
Our responsibility is to express an opinion on to express an opinion on Dialogue One's Description and on the design and operating effectiveness of the controls related to the control objectives stated in that Description, based on our procedures.

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

An assurance engagement to report on the Description, design and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its service and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in section 1.

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 controller**
Dialogue One A/S's Description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the service that the individual data controller may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

**Opinion**
Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the *Management's statement* in section 1. In our opinion, in all material respects:

(a) The Description fairly presents the service designed and implemented throughout the period from 1st June 2020 to 30th September 2021;

(b) The controls related to the control objectives stated in the Description were appropriately designed throughout the period from 1st June 2020 to 30th September 2021;

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from 1st June 2020 to 30th September 2021.

**Description of tests of controls**
The specific controls tested and the nature, temporal location, and results of those tests are listed in section 4.

**Intended users and purpose**
This report and the description of tests of controls in section 4 are intended only for data controllers who have used Dialogue One A/S's service, who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with.

Søborg, 17th November 2021

**info**revision
statsautoriseret revisionsaktieselskab

John Richardt Søbjærg
State Authorized Public Accountant

Simon Okkels
IT Auditor, CISA

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

### 4.1 Objective and scope

Our work has been performed in accordance with ISAE 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information.*

Our test of the design and implementation of the controls has included the control objectives and associated control activities selected by the management, which are stated in section 4.3. Any other control objectives, associated controls and controls at Dialogue One A/S's customers are not covered by our tests.

### 4.2 Tests Performed

The tests performed to evaluate design and implementation of controls are mentioned below:

| Method | Description |
|---|---|
| Inspection | Review and assessment of policies, procedures and documentation regarding the execution of controls |
| Inquiries | Inquiries of appropriate staff at the company, regarding controls |
| Observation | Observation of how controls are performed |
| Re-execution of control | We have repeated or observed the performance of the control in order to verify that the control are working as assumed. |

**Control objective A (Instruction)**

**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. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
|---|---|---|---|
| A1 | Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Checked by way of inspection that formalized procedures exist to ensure that personal data are only processed according to instructions.<br><br>Checked by way of inspection that the procedures include a requirement to assess at least once a year the need for updates, including in case of changes in the data controller's instructions or changes in the data processing.<br><br>Checked by way of inspection that procedures are up to date. | No deviations noted. |
| A2 | The data processor only processes personal data stated in the instructions from the data controller. | Checked by way of inspection that Management ensures that personal data are only processed according to instructions.<br><br>Checked by way of inspection of a sample of personal data processing operations that these are conducted consistently with instructions. | No deviations noted. |
| A3 | The data processor immediately informs the data controller if an instruction, in the data processor's opinion, | Checked by way of inspection that formalized procedures exist ensuring verification that personal data are not | No deviations noted. |

| Control objective A (Instruction)<br><br>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. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| | infringes the Regulation or other European Union or member state data protection provisions. | processed against the Regulation or other legislation.<br><br>Checked by way of inspection that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation.<br><br>Checked by way of inspection that the data controller was informed in cases where the processing of personal data was evaluated to be against legislation. | |

| Control objective B (Technical measures)<br><br>Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| No. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| B1 | 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.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Checked by way of inspection that formalized procedures exist to ensure establishment of the safeguards agreed.<br><br>Checked by way of inspection that procedures are up to date.<br><br>Checked by way of inspection of a sample of 3 data processing agreements that the safeguards agreed have been established. | No deviations noted. |
| B2 | The data processor has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller. | Checked by way of inspection that formalized procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security.<br><br>Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data.<br><br>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. | No deviations noted. |

| Control objective B (Technical measures)<br><br>Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| No. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| | | Checked by way of inspection that the data processor has implemented the safeguards agreed with the data controller. | |
| B3 | For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis. | Checked by way of inspection that, for the systems and databases used in the processing of personal data, antivirus software has been installed.<br><br>Checked by way of inspection that antivirus software is up to date. | No deviations noted. |
| B4 | External access to systems and databases used in the processing of personal data takes place through a secured firewall. | Checked by way of inspection that external access to systems and databases used in the processing of personal data takes place only through a secured firewall.<br><br>Checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy. | No deviations noted. |
| B5 | Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. | Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.<br><br>Inspected network diagrams and other network documentation to ensure appropriate segmentation. | No deviations noted. |
| B6 | Access to personal data is isolated to users with a work-related need for such access. | Checked by way of inspection that formalized procedures are in place for restricting users' access to personal data.<br><br>Checked by way of inspection that formalized procedures are in place for following up on users' access to personal data being consistent with their work-related need.<br><br>Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data.<br><br>Checked by way of inspection of a sample of 9 users' access to systems and databases that such access is restricted to the employees' work- | No deviations noted. |

| Control objective B (Technical measures)<br><br>Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| No. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| | | related need. | |
| B7 | For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. | Checked by way of inspection that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. | No deviations noted. |
| B8 | Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email. | Checked by way of inspection that formalized procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognized algorithm.<br><br>Checked by way of inspection that technological encryption solutions have been available and active throughout the assurance period.<br><br>Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.<br><br>Inquired whether any unencrypted transmission of sensitive and confidential personal data has taken place during the assurance period and whether the data controllers have been appropriately informed thereof. | No deviations noted. |
| B9 | Logging of the relevant matters has been established in systems, databases and networks<br><br>Log data are protected against manipulation and technical errors and are reviewed regularly.<br><br>Logging of events performed by system administrators and others with special privileges, has been established.<br><br>Logging of security incidents such as failed log-on attempts to systems, databases and networks, has been established. | Checked by way of inspection that formalized 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.<br><br>Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.<br><br>Checked by way of inspection that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated. | We have found that there are no guidelines regarding the proactive use of logging to detect adverse events.<br><br>No further deviations noted. |

| Control objective B (Technical measures)<br><br>Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| No. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| B10 | Personal data used for development, testing or similar activity are always in pseudonymized or anonymized form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf. | Checked by way of inspection that formalized procedures exist for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymized or anonymized form. | We have been informed that there are no examples of the use of test data.<br><br>No deviations noted. |
| B11 | The technical measures established are tested on a regular basis in vulnerability scans and penetration tests. | Checked by way of inspection that formalized procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests. | We have been informed that it has not been found necessary to perform external vulnerability or penetration tests.<br><br>No further deviations noted. |
| B12 | Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches. | Checked by way of inspection that formalized procedures exist for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches.<br><br>Checked by way of inspection of extracts from technical security parameters and setups that systems, databases or networks have been updated using agreed changes and relevant updates, patches and security patches. | No deviations noted. |
| B13 | A formalized procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need. | Checked by way of inspection that formalized procedures exist for granting and removing users' access to systems and databases using to process personal data.<br><br>Checked by way of inspection of a sample of 9 employees' access to systems and databases that the user accesses granted have been authorized and that a work-related need exists.<br><br>Checked by way of inspection of a sample of 34 resigned or dismissed employees that their access to systems and databases was deactivated or removed on a timely basis.<br><br>Checked by way of inspection that documentation exists that user accesses granted are evaluated and authorized on a regular basis – and at least once a year. | We have found cases where individual terminated employees have not been deactivated in accordance with the procedures, just as these have not been captured in the ongoing user reviews. The management has stated that the design of the procedures for user review and employee off-boarding, respectively, is evaluated with a view to improvement. Management has further stated that the accounts in question have not been used after the termination of employment.<br><br>No further deviations noted. |

| Control objective B (Technical measures)<br><br>Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| No. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| B14 | Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication. | Checked by way of inspection that formalized 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.<br><br>Checked by way of inspection that users' access to processing personal data that involve a high risk for the data subjects may only take place by using two-factor authentication. | No deviations noted. |
| B15 | Physical access safeguards have been established so as to only permit physical access by authorized persons to premises and data centres at which personal data are stored and processed. | Checked by way of inspection that formalized procedures exist to ensure that only authorized persons can gain physical access to premises and data centres at which personal data are stored and processed.<br><br>Checked by way of inspection of documentation that, throughout the assurance period, only authorized persons have had physical access to premises and data centres at which personal data are stored and processed. | No deviations noted. |

| Control objective C (Organizational measures)<br><br>Procedures and controls are complied with to ensure that the data processor has implemented organizational measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| No. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| C1 | 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.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated. | Checked by way of inspection that an information security policy exists that Management has considered and approved within the past year.<br><br>Checked by way of inspection of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees. | No deviations noted. |

| Control objective C (Organizational measures)<br><br>Procedures and controls are complied with to ensure that the data processor has implemented organizational measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| No. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| C2 | Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into. | Inspected documentation of Management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered into.<br><br>Checked by way of inspection of a sample of 3 data processing agreements that the requirements in these agreements are covered by the requirements of the information security policy for safeguards and security of processing. | No deviations noted. |
| C3 | The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant:<br><br>· Diplomas<br><br>· Interview<br><br>· Screening questions | Checked by way of inspection that formalized procedures are in place to ensure screening of the data processor's employees as part of the employment process.<br><br>Checked by way of inspection of 3 employees appointed during the assurance period that documentation exists of the relevant screening. | No deviations noted. |
| C4 | Employees, that gain access to GDPR data, sign a confidentiality agreement, and they are introduced to relevant information regarding processing of personal data processing, including security policy. | Checked by way of inspection of 2 employees appointed during the assurance period that the relevant employees have signed a confidentiality agreement.<br><br>Checked by way of inspection of 2 employees appointed during the assurance period that the relevant employees have been introduced to:<br><br>· Information security policy;<br><br>· Procedures for processing data and other relevant information. | No deviations noted. |
| C5 | For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned. | Inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned. | No deviations noted. |

| Control objective C (Organizational measures)<br><br>Procedures and controls are complied with to ensure that the data processor has implemented organizational measures to safeguard relevant security of processing. | | | |
|---|---|---|---|
| No. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| C6 | Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers. | Checked by way of inspection that formalized 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.<br><br>Checked by way of inspection of 3 employees resigned or dismissed during the assurance period that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality. | No deviations noted. |
| C7 | Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data. | Checked by way of inspection that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data.<br><br>Inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided. | We have been informed that there are plans for implementing a system for implementation and follow-up of employees' awarenes training.<br><br>No deviations noted. |

| Control objective D (Deletion and returning data)<br><br>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. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| D1 | Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Checked by way of inspection that formalized procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller.<br><br>Checked by way of inspection that the procedures are up to date. | No deviations noted. |

| Control objective D (Deletion and returning data)<br><br>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. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| D2 | The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines:<br><br>Maximum of 1 year. | 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.<br><br>Checked by way of inspection of a sample of 1 data processing sessions from the data processor's list of processing activities that documentation exists that personal data are stored in accordance with the agreed storage periods.<br><br>Checked by way of inspection of a sample of 1 data processing sessions from the data processor's list of processing activities that documentation exists that personal data are deleted in accordance with the agreed deletion routines. | No deviations noted. |
| D3 | Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been:<br><br>· Returned to the data controller; and/or<br><br>· Deleted if this is not in conflict with other legislation. | Checked by way of inspection that formalized procedures are in place for processing the data controller's data upon termination of the processing of personal data.<br><br>Checked by way of inspection of 1 terminated data processing sessions during the assurance period that documentation exists that the agreed deletion or return of data has taken place. | No deviations noted. |

| Control objective E (Storing of personal data)<br><br>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. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| E1 | Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Checked by way of inspection that formalized procedures exist for only storing and processing personal data in accordance with the data processing agreements.<br><br>Checked by way of inspection that the procedures are up to date.<br><br>Checked by way of inspection of a sample of 3 data processing sessions from the data processor's list of processing activities that documentation exists that data processing takes place in accordance with the data processing agreement. | No deviations noted. |
| E2 | Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller. | Checked by way of inspection that the data processor has a complete and updated list of processing activities stating localities, countries or regions.<br><br>Checked by way of inspection of a sample of 3 data processing sessions from the data processor's list of processing activities that documentation exists that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller. | No deviations noted. |

| Control objective F (Sub-data-processors)<br><br>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 organizational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing. | | | |
|---|---|---|---|
| No. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| F1 | Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-data processing agreements and instructions.<br><br>Assessments are made on a regular basis – and at least once a year – as to | Checked by way of inspection that formalized procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions.<br><br>Checked by way of inspection that procedures are up to date. | No deviations noted. |

| Control objective F (Sub-data-processors)<br><br>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 organizational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing. | | | |
|---|---|---|---|
| No. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| | whether the procedures should be updated. | | |
| F2 | The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller. | Checked by way of inspection that the data processor has a complete and updated list of sub-data processors used.<br><br>Checked by way of inspection of a sample of 2 sub-data processors from the data processor's list of sub-data processors that documentation exists that the processing of data by the sub-data processor is stated in the data processing agreements – or otherwise as approved by the data controller. | No deviations noted. |
| F3 | When changing the generally approved sub-data processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-data processors used, this has been approved by the data controller. | Checked by way of inspection that formalized procedures are in place for informing the data controller when changing the sub-data processors used.<br><br>Inspected documentation that the data controller was informed when changing the sub-data processors used throughout the assurance period. | We have found that there is no clearly defined procedure for informing customers of any replacement of sub-processors.<br><br>No further deviations noted. |
| F4 | The data processor has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller. | Checked by way of inspection for existence of signed sub-data processing agreements with sub-data processors used, which are stated on the data processor's list.<br><br>Checked by way of inspection of a sample of 2 sub-data processing agreements that they include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor. | No deviations noted. |

| Control objective F (Sub-data-processors)<br><br>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 organizational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing. | | | |
|---|---|---|---|
| No. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| F5 | The data processor has a list of approved sub-data processors disclosing:<br><br>· Name<br><br>· Business Registration No.<br><br>· Address<br><br>· Description of the processing | Checked by way of inspection that the data processor has a complete and updated list of sub-data processors used and approved.<br><br>Checked by way of inspection that, as a minimum, the list includes the required details about each sub-data processor. | No deviations noted. |
| F6 | Based on an updated risk assessment of each sub-data processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-data processor. | Checked by way of inspection that formalized procedures are in place for following up on processing activities at sub-data processors and compliance with the sub-data processing agreements.<br><br>Checked by way of inspection of documentation that each sub-data processor and the current processing activity at such processor are subjected to risk assessment.<br><br>Checked by way of inspection of documentation that technical and organizational measures, security of processing at the sub-data processors used, third countries' bases of transfer and similar matters are appropriately followed up on.<br><br>Checked by way of inspection of documentation that information on the follow-up at sub-data processors is communicated to the data controller so that such controller may plan an inspection. | No deviations noted. |

| Control objective G (Transfer to third countries)<br><br>Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organizations in accordance with the agreement with the data controller by using a valid basis of transfer. | | | |
|---|---|---|---|
| No. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| G1 | Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organizations in accordance with the agreement with the data controller by using a valid basis of transfer.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Checked by way of inspection that formalized procedures exist to ensure that personal data are only transferred to third countries or international organizations in accordance with the agreement with the data controller by using a valid basis of transfer.<br><br>Checked by way of inspection that procedures are up to date. | No deviations noted. |

| Control objective H (Data subject rights)<br><br>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. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| H1 | Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Checked by way of inspection that formalized procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects.<br><br>Checked by way of inspection that procedures are up to date. | No deviations noted. |
| H2 | The data processor has established procedures in so far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects. | Checked by way of inspection that the procedures in place for assisting the data controller include detailed procedures for:<br><br>· Handing out data<br><br>· Correcting data<br><br>· Deleting data<br><br>· Restricting the processing of personal data<br><br>· Providing information about the processing of personal data to data subjects.<br><br>Checked by way of inspection of documentation that the systems and | No deviations noted. |

| Control objective H (Data subject rights)<br><br>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. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| | | databases used support the performance of the relevant detailed procedures. | |

| Control objective I (Security breaches)<br><br>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. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| I1 | Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches.<br><br>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated. | Checked by way of inspection that formalized procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches.<br><br>Checked by way of inspection that procedures are up to date. | No deviations noted. |
| I2 | The data processor has established the following controls to identify any personal data breaches:<br><br>· Awareness of employees | Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches. | No deviations noted. |
| I3 | If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than 72 hours after having become aware of such personal data breach at the data processor or a sub-data processor. | Checked by way of inspection that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.<br><br>Made inquiries of the sub-data processors as to whether they have identified any personal data breaches throughout the assurance period.<br><br>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. | We have been informed that there have been no cases of data breaches during the period which have had an impact on the company's processing of personal data on behalf of their customers.<br><br>No deviations noted. |

| Control objective I (Security breaches)<br><br>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. | Dialogue One A/S' control activity | Auditors test activity | Result of auditors test |
| I4 | The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency:<br><br>· Nature of the personal data breach<br><br>· Probable consequences of the personal data breach<br><br>Measures taken or proposed to be taken to respond to the personal data breach. | Checked by way of inspection that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for:<br><br>· Describing the nature of the personal data breach<br><br>· Describing the probable consequences of the personal data breach<br><br>· Describing measures taken or proposed to be taken to respond to the personal data breach.<br><br>Checked by way of inspection of documentation that the procedures available support that measures are taken to respond to the personal data breach. | No deviations noted. |

PENNEO

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

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

**Ole Klitgaard**
**Direktør**
*Serienummer: PID:9208-2002-2-503171905939*
*IP: 87.60.xxx.xxx*
*2021-11-18 08:51:27 UTC*
NEM ID

**Simon Okkels**
**IT-revisor**
*Serienummer: CVR:19263096-RID:63988234*
*IP: 93.165.xxx.xxx*
*2021-11-18 09:23:19 UTC*
NEM ID

**John Richardt Søbjærg**
**Statsautoriseret revisor**
*Serienummer: CVR:19263096-RID:1265358432438*
*IP: 93.165.xxx.xxx*
*2021-11-18 09:26:01 UTC*
NEM ID