www.pwc.dk

# *Nuuday A/S*

## Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 April 2020 to 31 March 2021 pursuant to Nuuday's data processing agreement with Business Customers

July 2021

# Contents

# 1. Management's statement

Nuuday A/S (Nuuday) processes personal data on behalf of business customers in accordance with Nuudays standard data processing agreement.

The accompanying description has been prepared for data controllers who has used Nuuday's services; YouSee mail, TDC Secure Call Recording Pro, RecordIT, Hosted Switch Board solutions and Hosted Zylinc Switch board solutions (Nuuday 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" and "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (subsequently "the data protection rules") have been complied with.

Nuuday uses TDC NET A/S as a subprocessor for delivery of the service integrated into the Scale platform for Nuuday services; TDC Secure Call Recording Pro and Hosted Switch Board Solutions. This report uses the inclusive method and comprises controls that TDC NET A/S performs for Nuuday.

Nuuday uses Itadel A/S, Worldline, AWS Amazone, Unity Kakapo, Mircosoft Azure og Interxion as subprocessors for delivery of the service integrated into the platforms for Nuuday services; Hosted Zylinc Switch board solutions, YouSee mail, Hosted Switch Board Solutions, RecordIT and TDC Secure Call Recording Pro. This report uses the carve-out method for these subprocessors and does not comprise controls that these subprocessors performs for Nuuday A/S.

Nuuday confirms that:

a) The accompanying description in section 3 fairly presents the Nuuday services that has processed personal data for data controllers subject to the data protection rules throughout the period from 1 April 2020 to 31 March 2021. The criteria used in making this statement were that the accompanying description:

   (i) Presents how the Nuuday's services was designed and implemented, including:

   - The types of services provided, including the type of personal data processed;
   - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict processing of personal data;
   - The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller;
   - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
   - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation;
   - The procedures supporting, in the event of breach of personal data security, that the data controller may report this to the supervisory authority and inform the data subjects;
   - The procedures ensuring appropriate technical and organisational security measures in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

- Controls that we, in reference to the scope of the Nuuday's services 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 Nuuday's services in the processing of personal data in the period from 1 April 2020 to 31 March 2021;

(iii) Does not omit or distort information relevant to the scope of Nuuday services 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 Nuuday services 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 1 April 2020 to 31 March 2021, except concering the TDC Secure Call recording Pro service regarding the control objective "Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing". The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 April 2020 to 31 March 2021

c) Appropriate technical and organisational measures 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 data protection rules.

Copenhagen, 9 July 2021
Nuuday A/S

Lars Zahle Østergaard
Senior Vice President

# 2. Independent auditor's report

**Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 April 2020 to 31 March 2021 pursuant to Nuuday's data processing agreement with Business Customers**To management at Nuuday A/S (Nuuday) and Nuuday's business customers using the services; YouSee mail, TDC Secure Call Recording Pro, RecordIT, Hosted Switch Board solutions and Hosted Zylinc Switch board solutions (Nuuday services).

**Scope**

We have been engaged to provide assurance about Nuuday's description in section 3 of Nuuday services in accordance with Nuuday's standard data processing agreement with business customers throughout the period from 1 April 2020 to 31 March 2021 (the description) and about the design and operating effectiveness of controls related to the control objectives stated in the description.

Our report covers whether Nuuday has designed and effectively operated appropriate controls related to the control objectives stated in section 4. The report does not include an assessment of Nuuday general compliance with the requirements of the EU regulation on the "Protection of natural persons with regard to the processing of personal data and on the free movement of such data" and "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (subsequently "the data protection rules").

Nuuday uses TDC NET A/S as a subprocessor for delivery of the service integrated into the Scale platform for Nuuday services; TDC Secure Call Recording Pro and Hosted Switch Board Solutions. This report uses the inclusive method and comprises controls that TDC NET A/S performs for Nuuday.

Nuuday uses Itadel A/S, Worldline, AWS Amazone, Unity Kakapo, Mircosoft Azure og Interxion as subprocessors for delivery of the service integrated into the platforms for Nuuday services; Hosted Zylinc Switch board solutions, YouSee mail, Hosted Switch Board Solutions, RecordIT and TDC Secure Call Recording Pro. This report uses the carve-out method for these subprocessors and does not comprise controls that these subprocessors performs for Nuuday A/S.

We express reasonable assurance in our conclusion.

**Nuuday's responsibilities**

Nuuday is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing 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, which are based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct.

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

## Auditor's responsibilities

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

We conducted our engagement in accordance with ISAE 3000 (revised), "Assurance engagements other than audits or reviews of historical financial information", and additional requirements applicable in Denmark to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed 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 judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably 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 suitability of the objectives stated therein, and the suitability of the criteria specified by the data processor and described in the Management's statement section.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our modified opinion.

## Limitations of controls at a data processor

Nuuday's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of service that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect all personal data breaches. 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.

## Basis for modified opinion

As stated in 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", we have not been able to obtain in time all the inquired documentations regarding the technical measures to safeguard personal information regarding the service TDC Secure Call recording Pro. The control objective is therefore not achieved regarding the TDC Secure Call Recording Pro.

We have not found deviations that can be attributed to the identified weakness.

## Modified 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, except the matter described in the Basis for modified opinion, in all material respects:

a) The description fairly presents Nuuday's services as designed and implemented throughout the period from 1 April 2020 to 31 March 2021;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 April 2020 to 31 March 2021; and

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 April 2020 to 31 March 2021.

pwc

**Emphasis of matter**

Without modifying our conclusion, we inform that, in relation to control activity B.3, we have noted that Nuuday has not installed antivirus in the Unix environment for the RecordIT service. Furthermore, in relation to the RecordIT service, we have noted that the operational effectiveness has been insufficiently performed for several control activities under 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".

**Description of test of controls**

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

**Intended users and purpose**

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

Copenhagen, 9 July 2021
**PricewaterhouseCoopers**
Statsautoriseret Revisionspartnerselskab

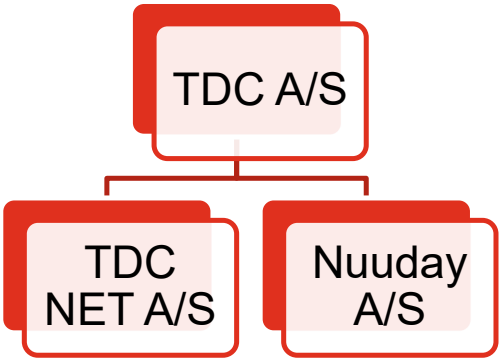
Jess Kjær Mogensen
State-Authorised Public Accountant

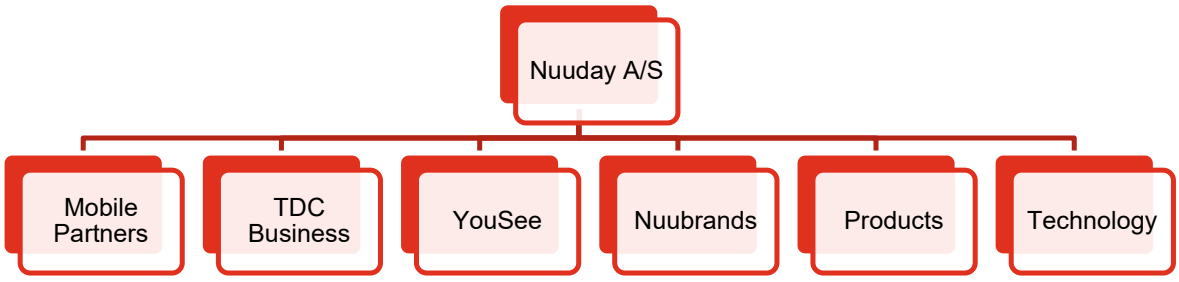
Bo Petersen
director

# 3. Nuuday's system description

## Introduction to Nuuday

TDC A/S is divided into three companies; TDC A/S, Nuuday A/S and TDC NET A/S with TDC A/S as the parent company owning Nuuday A/S and TDC NET A/S. TDC A/S and its subsidiaries are known as TDC Group.




Nuuday A/S (Nuuday) provides services to the customers where Nuuday is the data controller as well as services where Nuuday is the data processor. This report concerns the following services provided to Nuuday customers where Nuuday is the data processor and where a Nuuday standard data processing agreement has been agreed:

**YouSee mail (standard data processing agreement ver. 2.0)**

YouSee mail is a "mail only" service. The customer gets five mail addresses, storage for the mails, webmail access and access via PC, MAC and Mobile (POP3). The customer manages the YouSee mail service from "Mit YouSee". Support and information about the service is on yousee.dk. The service can be used by both private individuals and businesses; however, this report only covers the business customer part of the service.

**TDC Secure Call Recording Pro (standard data processing agreement ver. 2.0)**

TDC Secure Call Recording Pro is a service that can ensure recording and storage of calls. The service logs all kind of calls; both incoming and outgoing calls. The service is available to all business customers with TDC Scale services.

**RecordIT (Cloud Solutions) (standard data processing agreement ver. 2.2)**

RecordIT is a service that can ensure recording and storage of calls. The solution logs all kind of calls; both incoming and outgoing calls.

**Hosted Switch board Solutions (standard data processing agreement ver. 3.0)**

Hosted Switch board Solutions provides enhanced switchboard functions for TDC Scale and One solution. Hosted Switch board Solutions provides a conversion table function for receptionists in the company with extended functionality. Hosted Switch board Solutions consists of three parts:

- PC software for receptionists
- Server software for collecting phone and calendar status
- A client program for the individual employee that shows the colleagues' status.

The receptionist can use the switchboard function to operate the company's incoming call and see if the employees to be transferred to are busy or not and whether they are in attendance or available. The client program includes all commonly used features: Viewing call history, overview of telephone queues, overview of employees, buttons for handling calls, etc.

In addition, Hosted Switch board Solutions contains a very important feature: overview of each employee's calendar status. This is a requirement of many companies.

Furthermore, the service has:

- Full integration with Scale
- Calendar integration with Microsoft Exchange
- Display of the individual employee’s calendar and telephony status
- Danish user interface.

During the audit period, Hosted Switch board Solutions has been changed to a new platform (Unity) from Kakapo Systems Inc.

**Hosted Zylinc Switch board solutions (standard data processing agreement ver. 2.1)**

Zylinc is a complete switchboard solution that includes all the features the receptionist needs to be able to handle business calls efficiently. It is based on an integration between the TDC Scale and the Exchange environment and gives the receptionist an overview of the calendar and telephone status of all employees as well as the opportunity to search all parameters from AD and calendar. The program can be adapted to the company's individual needs, which gives the receptionist an optimal interface to work from.

The purpose is for communication use/working tool in Call Center and Contract Center to customers/clients.

# *Nuuday's personal data framework*

## *Nuuday Personal Data Policy*

Nuuday has formulated a series of policies which Nuuday have to follow and ensure is implemented in their organisations.

The primary policies are:

- HR policies
- Security policies
- GDPR policies.

Nuuday has also formulated a Personal Data Policy. This policy is stating that:

- Nuuday respects the right to privacy.
- Nuuday is a major player in the digital economy in Denmark, and privacy and protection of personal data is extremely important to us.
- We have processed personal data in an orderly manner for more than 135 years and in that regard we want to continue to be a trustworthy and transparent company that sets a good example for others.
- Nuuday is committed to comply with personal data legislation and good personal data practice, including:
  - **Transparency**: We are transparent about collection and use of personal data.
  - **Security**: We keep personal data secure and take appropriate measures to protect personal data.
  - **Legal protection**: We process personal data fairly and lawfully. We do this by adhering to applicable personal data legislation and following guidance and instructions from data protection authorities.
  - **Personal Data Compliance Framework**: We have implemented and maintain a Privacy Information Management System (PIMS) to support this policy and secure Nuuday's personal data compliance.
  - **Data Ethics**: Nuuday Board of Directors has approved "Nuuday's policy for data ethics and responsible handling of customers' personal data" which obliges us beyond personal data legislation.
  - **Awareness**: We educate our employees in personal data by use of e-learning and awareness campaigns and "Nuuday's 10 rules for treatment of personal data", included in the "Think before you type" document, directs our employees in how to treat personal data in a compliant way.

## *General Data Protection Regulation (GDPR) governance*

Within TDC Group, the governance related to fulfilling the requirements of the General Data Protection Regulation (GDPR) and the Danish Data Protection Act (commonly in the following denoted "personal data legislation") is as follows:

### TDC Board of Directors

TDC Board of Directors is ultimately accountable for setting directions for the implementation of personal data legislation as well as defining the Personal Data Compliance Framework within TDC.

### TDC Audit Committee

TDC Audit Committee is appointed by the Board of Directors to monitor the continuing suitability, adequacy and effectiveness of the Personal Data Compliance Framework.

### TDC Corporate Management Team

TDC Corporate Management Team (CMT) is ultimately accountable for ensuring implementation of the TDC Personal Data Policy and the policy's compatibility with the strategic direction of TDC. Furthermore, CMT shall ensure that the resources needed are available for implementation of the Personal Data Compliance Framework.

### TDC Group GDPR Committee

TDC Group GDPR Committee is appointed by CMT as accountable for ensuring implementation of the TDC Personal Data Policy and the policy's compatibility with the strategic direction of TDC.

Furthermore, TDC Group GDPR Committee is responsible for:

- ensuring the effectiveness of the Personal Data Compliance Framework;
- ensuring the integration of personal data requirements into TDC's processes;
- communicating the importance of an effective Personal Data Compliance Framework and of conforming to requirements in personal data legislation;
- ensuring that the Personal Data Compliance Framework achieves its intended outcome(s);
- directing and supporting individuals to contribute to the effectiveness of the Personal Data Compliance Framework; and
- promoting continual improvements.

### Heads of Business Lines/Tribe Sponsors

Heads of Business Lines/Tribe Sponsors are accountable for ensuring implementation of the TDC Personal Data Policy and personal data objectives within each of their Business Lines/Tribes.

Furthermore, Heads of Business Lines/Tribe Sponsors are accountable for:

- ensuring that the resources needed for the Personal Data Compliance Framework are available within the Business Line/Tribe;
- ensuring effectiveness of personal data implementation; and
- demonstrating leadership as it applies to their areas of responsibility.

### Nuuday Data Privacy Managers

Nuuday Data Privacy Managers (DPMs) are responsible for Business Lines' daily operation of demands stated in personal data legislation and for compliance with directions from supervisory authorities and management. Such responsibility may also be anchored within a group of DPMs appointed to ensure compliance with the General Data Protection Regulation (GDPR) across Business Lines/Tribes.

Responsibilities and tasks for the DPMs are described in the document "Description of Tasks for Data Privacy Managers" issued by Nuuday's Data Protection Officer (DPO) and approved by TDC Group GDPR Committee.

### Employees

In their daily work, Nuuday's employees are responsible for complying with personal data legislation as well as complying with directions from supervisory authorities and management.

**TDC DPO**

TDC's DPO is responsible for implementation of the Personal Data Compliance Framework, supporting the implementation of the TDC Personal Data Policy and for monitoring compliance with personal data legislation.

The supporting activities include the following tasks:

- Supporting DPMs so that they can fulfil their responsibility by:
  - issuing guidelines regarding implementation of specific requirements;
  - informing and advising of obligations pursuant to personal data legislation and directions from national authorities and management; and
  - providing advice – where requested – about privacy impact assessments (PIA) and data protection impact assessments (DPIA).

Furthermore, the DPO is responsible for:

- cooperating with the supervisory authorities;
- acting as contact point for the supervisory authorities with regards to issues relating to processing of personal data;
- consulting the supervisory authorities, where appropriate, about any other matter; and
- acting as a consultant for Nuuday Security's implementation of security controls regarding compliance with personal data requirements.

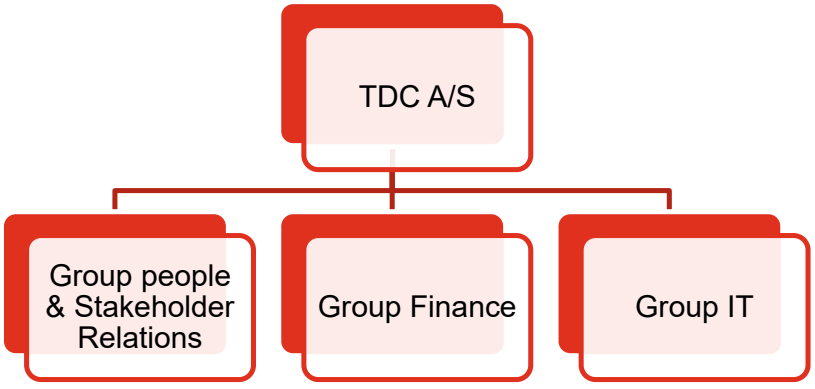
In the performance of his or her tasks, the DPO shall consider the risks associated with processing operations, including the nature, scope, context and purpose of the processing.

**TDC Group Security**

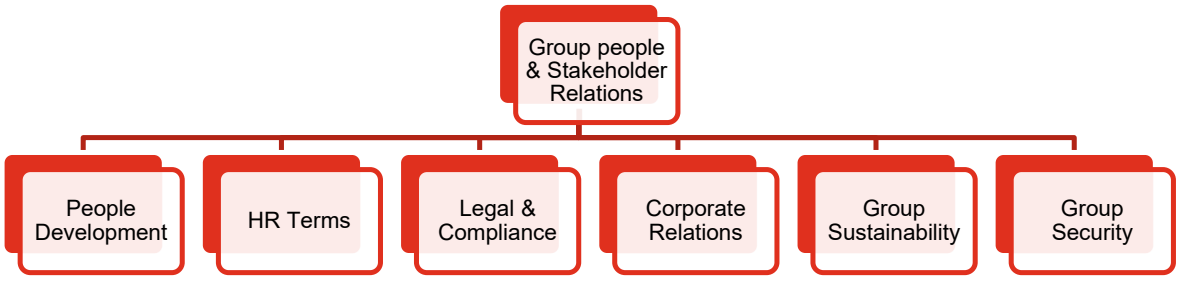
Together with Business line management, TDC Group Security is responsible for implementing organisational and technical security controls, ensuring compliance with personal data security requirements and ensuring the effectiveness of personal data security within Nuuday.

## *Organisation of GDPR handling at TDC Group level*

TDC Group is organised in the following manner:




TDC Group's DPO Office (in the following denoted "DPO Office") and TDC Group Security are a part of TDC Group People & Stakeholder Relations where the DPO Office is part of Legal & Compliance:




**GDPR responsibilities between the DPO Office and TDC Group Security**

The DPO Office and TDC Group Security both play a significant role in handling of the requirements in regard to GDPR, and there is current collaboration between the two entities.

*DPO Office*

The DPO Office is responsible for supporting the implementation of the TDC Group Personal Data Policy and for monitoring compliance with personal data legislation.

The supporting activities include the following tasks:

- Supporting the DPMs so that they can fulfil their responsibility by:
  - issuing guidelines regarding implementation of specific requirements;
  - informing and advising of obligations pursuant to personal data legislation and directions from national authorities and management; and
  - providing advice where requested about data protection impact assessments and monitoring its performance.
- Furthermore, the DPO is responsible for:
  - cooperating with the supervisory authority;
  - acting as contact point for the supervisory authority with regard to issues relating to processing of personal data;
  - consulting the supervisory authority, where appropriate, about any other matter; and
  - acting as a consultant for TDC Group Security's implementation of security controls regarding compliance of personal data requirements.

In the performance of his or her tasks, the DPO shall consider the risks associated with processing operations, including the nature, scope, context and purpose of the processing.

*TDC Group Security*

TDC Group Security is responsible for implementing security controls regarding compliance with personal data requirements and ensuring the effectiveness of technical and organisational security within TDC Group.

*Responsibilities in the organisation*

TDC Group has organised its compliance framework in a manner that gives each Business Line ownership over its own compliance. The DPO Office acts as an overarching compliance guidance and auditing office for all Business Lines, and it is responsible for contact to the supervisory authorities and reporting to the Board of Directors (Audit Committee), the CMT and the TDC GDPR Committee.

The role of the DPO Office has been entrenched in the PIMS where the Board of Directors has approved the governance model within TDC Group. The guidance from the DPO Office includes operational guidelines, procedures, templates and tools covering the following areas:

- Rights of the data subjects
- Personal data breaches
- Risk screening and mitigation
- Data processing agreements, including risk screening of vendors
- Data minimisation and storage limitation
- Data protection by design and by default.

In addition, the DPO Office supports awareness activities throughout the organisation and administration of the record of processing activities and provides daily assistance on specific matters related to personal data legislation.

The DPMs are the point of contact for all questions regarding personal data in their respective Business Lines. The DPMs play a role in education, awareness, audits, personal data breaches, fulfilment of data subject rights, data processing agreements, risk management, documentation and application/system improvements necessary to improve the safeguarding of personal data. Escalations regarding non-compliance or funding-related issues can be raised by the DPM to their Business Line's TDC GDPR Committee member. In the very unlikely situation where the escalation is ignored, the issue can be brought directly to the DPO Office.

Ensuring in practice that adequate security measures are in place in relation to the processing of personal data, collaboration between the DPMs, the DPO Office and TDC Group Security becomes essential. Therefore, the technical and organisational measures required to secure and safeguard the processing of personal data are incorporated into the policies and standards established by TDC Group Security.

## *Description of data processing*

Nuuday delivers a wide spectrum of telecommunication services, including mobile telephony, IP telephony and MPLS connections. When Nuuday delivers these kinds of services, Nuuday processes personal data as a data controller.

Nuuday also delivers special services such as cloud storage where Nuuday processes personal data as instructed by the customer. In these situations, Nuuday acts as a data processor for the customer. Nuuday follows the instructions set out by Datatilsynet: "*Vejledning om dataansvarlige og databehandlere,*" released November 2017, when assessing whether Nuuday is acting as a data controller or as a data processor.

When Nuuday acts as a data processor for a customer, the customer must enter into a data processing agreement with Nuuday. Nuuday has developed a standardised agreement which is used as a basis for the specific data processing agreements. The purposes of the processing in the services currently covered by a standardised agreement are as follows:

| **Service** | **Purpose of processing** |
|---|---|
| YouSee mail | Handling of emails |
| TDC Secure Call Recording Pro | Documentation of the content of telephone calls, especially in the financial sector for documentation of trades |
| RecordIT (Cloud Solutions) | Documentation of the content of telephone calls, especially in the financial sector for documentation of trades |
| Hosted Switch Board Solutions | To operate a switching solution |
| Hosted Zylinc Switch board solutions | To operate a switching solution |

# *Personal data handled by Nuuday as a processor*

Nuuday has made three separate classifications of personal data: normal, confidential and sensitive. Where Nuuday acts as a data processor, the data processed is considered 'normal' – see overview below. A non-exhaustive list with examples of personal data that Nuuday considers 'confidential' is as follows:

1. Passwords
2. Information about who the customer has called, including call lists/specified bills (part of CDR data)
3. Remaining payment information, payment reminders and repayments
4. NemID data
5. URL and contents, surf information
6. Music listened to by the customer via music services in Nuuday
7. SMS/MMS content
8. Personnel files
9. Who has sent SMS/MMS to whom and when (part of CDR data)
10. Information about secret of exempted numbers
11. Other information about the customer's financial status
12. Geolocation data, information about the location of the device from cell towers (part of CDR data)
13. Customer's use of films from Blockbuster, YouSee TV, etc.
14. Voicemail contents and call numbers
15. Credit status
16. CPR number.

In the services currently covered by a standardised agreement where Nuuday acts as the data processor for the customers, the following categories of personal data are processed by Nuuday:

| **Service** | **Data types processed by Nuuday** | **Personal Data Category processed by Nuuday** |
|---|---|---|
| YouSee mail | • Email addresses<br>• IP addresses<br>• Personal data in email*<br>• Personal data in contacts<br>• Personal data in calendar | Normal personal data* |
| TDC Secure Call Recording Pro | • Names of customer's employees<br>• Persons with whom a call is made<br>• Personal information in the recorded call* | Sensitive personal data* |
| RecordIT | • Telephone numbers<br>• Personal information in the recorded call* | Sensitive personal data* |
| Hosted Switch Board solutions | • Names of customer's employees<br>• Telephone numbers<br>• Email addresses<br>• Availability (calendar/telephone)<br>• Performance information (employee availability, calls divided into number of calls and length)<br>• Welcome speak when calling main number<br>• IP addresses<br>• Browser and operating system (type and version) | Normal personal data |

| Service | Data types processed by Nuuday | Personal Data Category processed by Nuuday |
|---|---|---|
| Hosted Zylinc Switch board solutions | • Names of customer's employees<br>• Addresses of customer's employees<br>• Telephone numbers<br>• Email addresses<br>• IP addresses<br>• Access code to Nuuday's self-service<br>• MAC address of equipment used to connect to solution<br>• Personal information in chat messages* | Normal personal data* |

*Nuuday neither has access nor control of personal data types stored in the service, and it is the responsibility of the data controller to determine what categories of personal data it will accept.

## *Description of use of subcontractors*

Nuuday is using subcontractors for delivering the below-mentioned services where Nuuday acts as a data processor for a customer. Data processor agreements with the subcontractors have been signed.

The following subcontractors are used for delivering the services:

| **TDC NET A/S**<br>Teglholmsgade 1, 0900 København C, Denmark<br>CVR no. 40075267 | |
|---|---|
| **Nuuday service**<br>Secure Call Recording Pro<br><br>Hosted Switch Board Solutions – Vouquant<br><br>Hosted Switch Board Solutions – Unity from Kakapo Systems Inc. | **Subcontractor service**<br>Delivery of the service integrated into the Scale platform<br><br>Delivery of the service integrated into the Scale platform<br><br>Delivery of the service integrated into the Scale platform |

| **Itadel A/S**<br>Skanderborgvej 190, 8260 Viby J, Denmark<br>CVR no. 37032034 | |
|---|---|
| **Nuuday service**<br>Hosted Zylinc Switch board solutions | **Subcontractor service**<br>Delivery of hosting service of operating platform |

| **Worldline**<br>River Ouest 80 Quai Voltaire, 95870 Bezons, France<br>Business reg. no. 378 901 946 | |
|---|---|
| **Nuuday service**<br>YouSee mail | **Subcontractor service**<br>Delivery of hosting and operating service |

| **AWS Amazon**<br>One Burlington Plaza, Burlington Road, Dublin 4, Ireland | |
|---|---|
| **Nuuday service**<br>New Hosted Switch Board Solutions – Unity from Kakapo Systems Inc. | **Subcontractor service**<br>Delivery of hosting and operating platform for licence control server |

| **RecordIT (Touch Call Recording ApS)**<br>Skomagervej 4L, 7100 Vejle, Denmark<br>CVR no. 27489761 | |
|---|---|
| **Nuuday service**<br>RecordIT | **Subcontractor service**<br>Only handling of phone numbers |

| Mircosoft Azure<br>Microsoft Ireland, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland | |
|---|---|
| **Nuuday Service**<br>Old decommissioned Hosted Switch Board Solutions – Vouquant | **Subcontractor service**<br>Delivery of hosting and operating platform for handling present information of clients. |

| **Interxion Danmark ApS**<br>Industriparken 20A, 2750 Ballerup, Denmark<br>CVR no. 25147022 | |
|---|---|
| **Nuuday service**<br>RecordIT | **Subcontractor service**<br>Delivery of housing. |

| **Kakapo Systems Ltd**<br>International House 24, Holborn Viaduct, London, UK, EC1A 2BN | |
|---|---|
| **Nuuday service**<br>New Hosted Switch Board Solutions – Unity from Kakapo Systems Inc. | **Subcontractor service**<br>Provider of Hosted Switch Board software and performing license control. |

## *Risk assessment*

When processing personal data, Nuuday has a responsibility to assess the risks associated with the process itself. To screen all the processes in Nuuday's record of processing activities, the DPO Office has created a risk screening template for process owners to use. The risks assessed in the screening relate to the fundamental principles of the GDPR (defined in Article 5).

The DPMs are responsible for performing a risk screening on new processes and systems in their respective Business Lines. In addition, an initial risk screening of existing processes has been performed throughout 2019 to capture the as-is state regarding personal data risks associated with processing activities. The risk screening shall provide output to the conductor of the screening, the DPM and Business Line management in the form of instructions on whether a mitigation plan and/or a data protection impact assessment is necessary.

The DPM is responsible for sharing the risk screening with the DPO Office if the risk screening results in any risks outside the defined risk appetite. Where the risk screening results in 'Medium' risks, the DPM shall initiate a mitigation plan locally and add the risk to their Business Line GDPR Risk Tracker. Where

the risk screening results in 'High' risks, the DPM shall contact the DPO Office which will assist with and track the risk in the DPO GDPR Risk Tracker.

Accountability for risk management and the Risk Management Policy in relation to the GDPR is anchored in the TDC GDPR Committee.

Management of risks related to information security within Nuuday and suppliers is as follows:

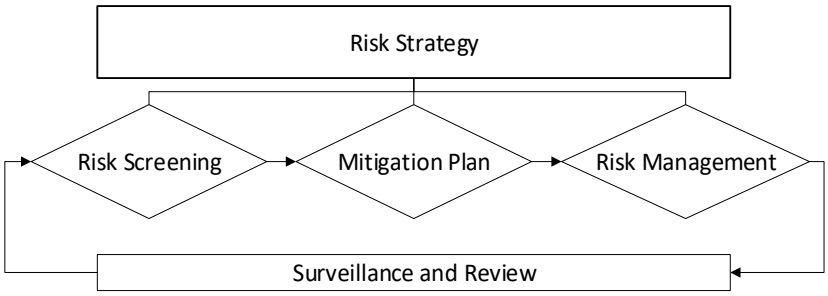
- Product / service
  It is the data controller's responsibility to perform risk assessments. The product owner / product manager in Nuuday can, with consent from the data controller, take part in the performance of a risk assessment in relation to the information security of the specific service/service.

- Development / test environments
  The entity responsible for operations and technical support is responsible for the performance of risk assessments on development / test environments.

- Hosted environments
  The entity responsible for operations and technical support is responsible for the performance of risk assessments on hosted environments.

The Risk Management Policy and the risk screenings performed are reviewed yearly or more often if changes are made that could affect the processing activity. Status on 'high' risks is a fixed item on the agenda and are addressed during each TDC GDPR Committee meeting.

The managing of risks related to personal data follows the high-level model below:




*Risk Strategy:*

- High-level overview of how risks related to the processing of personal data are managed.
- In general, the Risk Strategy involves cyclical iterations where risks are identified, improvements are planned, implemented and monitored, and after that the cycle continues.

*Risk Screening:*

- Using a standard template, all processes where personal data is processed shall undergo a risk screening.
- The screening involves an initial assessment of the process in relation to specified risks
  - Likelihood, consequence and the type of data processed are the parameters used to determine a risk score.
- Risk screening will provide the conductor, the DPM, and Business Line management with next steps.
- 'Low' risks identified in the Risk Screening are considered to be within the risk appetite, and no further actions are required but risks will be logged and monitored.
- For 'Medium' and 'High' risks identified, a mitigation plan shall be filled out.

- In addition, 'Medium' risks shall be registered and tracked by the Business Line locally while any 'High' risks shall be registered and tracked by the DPO Office.

*Mitigation Plan (for risk identified as Medium or High risks):*

- Using a standard template, any risks identified in the risk screening to be outside of the defined risk appetite shall be registered and tracked
  - Descriptions of measures to be taken to lower the risk, expected and actual start/end dates, milestones, funding information and the to-be likelihood, consequence and type of data processed are among the parameters registered and tracked.
- There are four options to choose from in the mitigation plan:
  - Accept
  - Avoid
  - Mitigate
  - Transfer.
- If the Mitigation Plan indicates that the risk will be brought within the risk appetite within a month, no further tracking of the risk is deemed necessary.
- If the Mitigation Plan indicates that a 'Medium' risk will remain after a month, the risk shall be registered and tracked by the Business Line locally.
- If the Mitigation Plan indicates that a 'High' risk will remain after a month, the risk shall be registered and tracked by the DPO office.

*Risk Management:*

- Subsequent to completion of the Mitigation Plan, the risk must be managed.
- The method chosen to manage the risk varies depending on the severity, scope, the systems involved, the budgeting, etc.

*Surveillance and Review:*

- After implementation of mitigating measures, the measures are monitored to ensure that the risk level decreases in alignment with the goal.
- If the risk does not decrease as expected, additional measures shall be taken.
- At a minimum, all risks shall be revisited once a year.
- If changes occur in a processing activity that could affect the risk level, a new risk screening shall be performed.

# Control objectives

TDC Group Security has based its work on the Information Security Management System (ISMS) model as described in the international standard ISO/IEC 27001:2013 (Information technology – Security techniques Information security management systems Requirements). In addition, Nuuday's Security Policy is based on the international standard ISO/IEC 27001:2013, and it is implemented by a set of security policies and standards.

The security policies and standards are updated or reviewed at least once a year. The governance model established ensures that all policies and standards are approved by a Security Steering Committee.

The following control objectives identify the scope of this audit report. Each year, on a periodical basis, a regular assessment is carried out by Nuuday as to whether these objectives need to be updated.

***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. (Control objectives A)***

Nuuday has implemented written procedures regarding requirements ensuring that personal data must only be processed where there is a lawful basis. These procedures include requirements that a standardised data processing agreement with an instruction has been approved by the data controller.

The data processing agreement is based on Nuuday 's standard template for data processing agreements, which contain a summary of the basis on which the processing of personal data is carried out.

The standard template covers the following areas:

- The subject of the processing
- The duration of processing
- The nature and purpose of the processing
- The type of personal data
- The categories of data subjects.

Each year, on a periodical basis, a regular assessment is carried out as to whether data processing agreements and the standard template need to be updated.

Nuuday has implemented written procedures to ensure that Nuuday only processes personal data when instructions from the customer exist or is stated in standard processing agreements.

In addition, written procedures have been implemented to ensure that individuals authorised to process personal data receive continuous training in data protection rules, including requirements on confidentiality as well as procedures and controls implemented by Nuuday to comply with the data protection rules.

Nuuday has implemented written procedures to ensure that the standard data processing agreements are updated when needed.

***Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing. (Control objectives B)***

A description of the use of subprocessors exists, including a description that the subprocessors' technical and organisational measures to protect the rights of the data subject and the processing of personal data are at least in line with Nuuday's standard data processing agreement.

Nuuday has implemented written procedures to manage the termination of data processing agreements with subprocessors.

Nuuday has implemented written procedures and controls to ensure that the data processor can provide the adequate security and organisational measures are taken.

These areas include:

- Information security policy
- General risk assessment
- Physical security measures
- Authentication and authorisation
- Antivirus, malware and phishing protection
- Vulnerability scans and penetration tests
- Network components and security
- Log management
- Patch management
- Handling of test data
- User management
- Mobile devices
- Backup and restore.

***Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing. (Control objectives C)***

Nuuday has implemented written procedures to ensure that individuals authorised to process personal data at Nuuday have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. In addition, Nuuday's employment contracts determine requirements to employees as regards security of processing and confidentiality during and after employment.

Each year, on a periodical basis, a regular assessment is carried out as to whether the procedure for entering confidentiality is still up-to-date and adequate.

***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. (Control objectives D)***

Nuuday has implemented written procedures that describe how the processor, at the choice of the data controller, erases or returns all the personal data to the data controller after the end of the provision of services relating to processing, and erases existing copies unless European Union or Member State law requires storage of the personal data.

***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. (Control objectives E)***

Nuuday has implemented written procedures to ensure that only personal data is stored in accordance with the agreements with the data controller.

An assessment is made on an ongoing basis - and at least once a year - of whether the procedures need to be updated.

Nuuday's data processing including storage takes place at the locations, countries or rural areas specified in the data processor agreements.

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

Nuuday has implemented written procedures to ensure that – when using a subprocessor for carrying out specific processing activities on behalf of the data controller – the subprocessor is subject to the same data protection obligations as those assumed by the data processor itself by means of a data processing agreement. Nuuday ensures that a risk assessment is carried out when using a subprocessor, including an evaluation of the subprocessor's established organisational and technical measures for handling personal data.

In addition, Nuuday has implemented written procedures that the subprocessor enables and contributes to audits, inspections, etc. carried out by Nuuday. Furthermore, Nuuday has implemented written procedures to ensure that changes is updated in the standard data processing agreements.

An overview of approved subprocessors as well as descriptions of Nuuday's own controls have been drawn up to ensure that subprocessors comply with the same data processing obligations as those defined in the data processing agreement between the customer as a data controller and Nuuday.

***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. (Control objectives G)***

Nuuday has implemented written procedures to ensure that the processing of personal data, including transfer of personal data to a third country or international organisation, is only performed under documented instructions from the data controller or pursuant to European Union law or national law. In addition, written procedures describe the transfer of personal data to a third country or international organisation recognised by the Commission.

Nuuday uses the subcontractors AWS Amazon and Microsoft Azure, which Nuuday regards as having processing in third part countries even though the datacenters for each of the subcontractors are placed in EU/EEA.

***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. (Control objectives H)***

The services in scope are all "self-service" products and therefore the customers are themselves able to fulfil requests from data subjects regarding:

- The request to access
- The right to erasure
- The right to data portability
- Other rights of the data subject.

If necessary, Nuuday can assist the customers in fulfilling the request. In such case, the customer has to issue a service request according to contract.

Nuuday assists in ensuring that obligations related to the handling of personal data breaches are complied with, and furthermore Nuuday assists in ensuring that obligations with regard to carrying out impact assessments are complied with.

Regarding system development activities, Nuuday has implemented written procedures to assess security. These include requirements for separation of environments and personnel.

***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. (Control objectives I)***

Nuuday has implemented written procedures to ensure that the data controller is notified in a timely and adequate manner in the event of a personal data breach. Furthermore, a record has been implemented that document all personal data breaches, including the facts relating to the breach, its effects and the remedial action taken.

Nuuday has implemented written procedures to ensure the ability to deliver documentation comprising, as a minimum, the facts relating to the breach, its effects and the remedial action taken to the data controller.

## *Data controller's supplementary control measures*

Transmission of data is the basic service behind all services delivered by Nuuday. Regardless of whether Nuuday acts as a data controller or as a data processor, the customer has the main responsibility for the data that is being transferred whereas Nuuday's responsibility is to perform the transfer of the data.

In situations where Nuuday acts as a data processor for the customer, the customer, as the data controller, has the overall responsibility which includes but is not limited to:

- Adherence to the general principles relating to the processing of personal data mentioned in Article 5 of the GDPR
- Assurance that personal data being processed is done lawfully and in accordance with Article 6 of the GDPR
- Ensuring that the instructions for processing given to the data processor do not infringe any laws
- Obligations regarding information to be provided to the customer's customers
- Setting specific requirements for logging
- Notifying relevant authorities and, if necessary, the data subject in case of a data breach
- Ensuring that the personal data registered about their customers is legal at any time according to the personal data regulation
- Establishing satisfactory controls in relation to the administration of own users. This includes, however not limited to, periodic review of users and assessment of user access and their continuous need for access.
- Making sure that the instructions received by Nuuday are legally completed at any time according to the personal data regulation
- Informing Nuuday if changes occur in the customer instructions and/or data processing requirements
- Ensuring that the data controller has received written consent to the processing of personal data
- Ensuring that information on the processing of personal data can be provided in a transparent, easily accessible and understandable form
- Ensuring that the processing of the personal data is correct and according to the purpose of processing
- Ensuring that the personal data is processed on a timely basis and that registrant's rights are withheld at all times
- Performing risk assessment which identifies risks, assessing which technical and organisational measures are appropriate, and informing Nuuday of the outcome and changes
- Conducting data privacy impact assessments on data protection – to the extent that the customer is obliged to – and inform Nuuday of the outcome and changes.
- Ensuring that any integrations to other systems and entities comply with the legislation.

It is assumed that the customer organises and complies with the necessary controls in relation to handling above responsibilities.

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

**Control objective A:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| A.1 | Written procedures are in place which include a requirement that personal data must only be processed when instructions to this effect are available.<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 formalised procedures are in place to ensure that personal data are only processed according to instructions.<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>Checked by way of inspection that procedures are up to date. | No exceptions noted. |
| A.2 | The data processor only processes personal data stated in the instructions from the data controller. | Checked by way of inspection that Management ensures that personal data are only processed according to instructions.<br>Checked by way of inspection of a sample of personal data processing operations that these are conducted consistently with instructions. | No exceptions noted. |

**Control objective A:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| A.3 | The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions. | Checked by way of inspection that formalised procedures are in place ensuring verification that personal data are not processed against the Data Protection Regulation or other legislation.<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 considered to be against legislation.<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. | No exceptions noted. |

**Control objective B:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.1 | Written procedures are in place which include a requirement that security measures agreed are established for the processing of personal data in accordance with the agreement with the data controller.<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 formalised procedures are in place to ensure establishment of the security measures agreed.<br>Checked by way of inspection that procedures are up to date.<br>Checked by way of inspection of a sample of 6 data processing agreements that the security measures agreed have been established. | No exceptions noted. |
| B.2 | The data processor has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the security measures agreed with the data controller. | Checked by way of inspection that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security.<br>Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data.<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.<br>Checked by way of inspection that the data processor has implemented the security measures agreed with the data controller. | We have noted that the risk assessments have not been performed for all services included in this report.<br>We have been informed that these services existed before 25th May 2018 and are expected to have undergone risk assessment by Q3 2021.<br>We have observed that all services implemented after 25th May 2018 have undergone a proper risk assessment.<br>No further exceptions noted. |

**Control objective B:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.3 | For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis. | Checked by way of inspection that antivirus software has been installed for the systems and databases used in the processing of personal data.<br>Checked by way of inspection that antivirus software is up to date. | We have noted in our sample test that antivirus is not installed in the Unix environment for the service RecordIT.<br><br>Regarding the TDC Secure Call Recording Pro: We have not received the inquired documentation regarding the TDC Secure Call Recording Pro in time, and we have therefore not been able to test the operational effectiveness for this control activity for the TDC Secure Call Recording Pro.<br><br>No further exceptions noted. |

**Control objective B:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.4 | External access to systems and databases used in the processing of personal data takes place through a secured firewall. | 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>Checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy. | We have noted in our sample test of firewalls the following weaknesses for the services Zylinc and RecordIT:<br>• Devices are running on outdated software versions.<br>• Devices allow unencrypted protocols.<br>• Super users have been created directly on the firewalls.<br>• Review of firewall rules are done Ad Hoc<br><br>Regarding the TDC Secure Call Recording Pro: We have not received the inquired documentation regarding the TDC Secure Call Recording Pro in time, and we have therefore not been able to test the operational effectiveness for this control activity for the TDC Secure Call Recording Pro.<br><br>No further exceptions noted. |

**Control objective B:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.5 | Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. | Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.<br>Inspected network diagrams and other network documentation to ensure appropriate segmentation. | Regarding the TDC Secure Call Recording Pro: We have not received the inquired documentation regarding the TDC Secure Call Recording Pro in time, and we have therefore not been able to test the operational effectiveness for this control activity for the TDC Secure Call Recording Pro.<br><br>No further exceptions noted. |
| B.6 | Access to personal data is isolated to users with a work-related need for such access. | Checked by way of inspection that formalised procedures are in place for restricting users' access to personal data.<br>Checked by way of inspection that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need.<br>Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data.<br>Checked by way of inspection that no employees have been granted access the assurance period for the services in scope. | We have noted that for one of the services, that the internal responsibilities regarding user management in Nuuday are vaguely defined. In addition, user access creations and terminations are not managed sufficiently for the service Zylinc.<br>Regarding the TDC Secure Call Recording Pro: We have not received the inquired documentation regarding the TDC Secure Call Recording Pro in time, and we have therefore not been able to test the operational effectiveness for this control activity for the TDC Secure Call Recording Pro.<br>No further exceptions noted. |

**Control objective B:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.7 | System monitoring with an alarm feature has been established for the systems and databases used in the processing of personal data. | Checked by way of inspection that system monitoring with an alarm feature has been established for systems and databases used in the processing of personal data.<br>Checked by way of inspection that, in a sample of 0 alarms, these were followed up on and that the data controllers were informed thereof as appropriate. | We have noted in our sample test that log configurations are set in an insufficient manner on the Windows environment for the service RecordIT. Furthermore, we have noted that no log triggers are set.<br><br>We have noted for one of the services that no remote log agreement has been entered with the vendor for the service Zylinc.<br><br>Regarding the TDC Secure Call Recording Pro: We have not received the inquired documentation regarding the TDC Secure Call Recording Pro in time, and we have therefore not been able to test the operational effectiveness for this control activity for the TDC Secure Call Recording Pro.<br><br>No further exceptions noted. |

**Control objective B:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.8 | Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email. | Checked by way of inspection that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm.<br>Checked by way of inspection that technological encryption solutions have been available and active throughout the assurance period.<br>Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.<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 exceptions noted. |

**Control objective B:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.9 | Logging of the following matters has been established in systems, databases and networks:<br>• Activities performed by system administrators and others holding special rights<br>• Security incidents comprising:<br>  ○ Changes in log set-ups, including disabling of logging<br>  ○ Changes in users' system rights<br>  ○ Failed attempts to log on to systems, databases or networks<br>Logon data are protected against manipulation and technical errors and are reviewed regularly. | Checked by way of inspection that formalised procedures are in place for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs.<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.<br>Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.<br>Checked by way of inspection of a sample of 25 days of logging that the content of log files is as expected compared to the set-up and that documentation confirms the follow-up performed and the response to any security incidents.<br>Checked by way of inspection of a sample of 25 days of logging that documentation confirms the follow-up performed on activities carried by system administrators and others holding special rights. | We have noted in our sample test that log configurations are set in an insufficient manner on the Windows environment for the service RecordIT. Furthermore, we have noted that no log triggers are set.<br><br>We have noted for one of the services that no remote log agreement has been entered with the vendor for the service Zylinc.<br><br>Regarding the TDC Secure Call Recording Pro: We have not received the inquired documentation regarding the TDC Secure Call Recording Pro in time, and we have therefore not been able to test the operational effectiveness for this control activity for the TDC Secure Call Recording Pro.<br><br>No further exceptions noted. |

**Control objective B:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.10 | Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf. | Checked by way of inspection that formalised procedures are in place for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form.<br>Checked by way of inquiry that personal data are not applied for test purposes. | No exceptions noted. |
| B.11 | The technical measures established are tested on a regular basis in vulnerability scans and penetration tests. | Checked by way of inspection that formalised procedures are in place for regularly testing technical measures, including for performing vulnerability scans and penetration tests.<br>Checked by way of inspection of samples that documentation confirms regular testing of the technical measures established.<br>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. | Regarding the TDC Secure Call Recording Pro: We have not received the inquired documentation regarding the TDC Secure Call Recording Pro in time, and we have therefore not been able to test the operational effectiveness for this control activity for the TDC Secure Call Recording Pro.<br><br>No further exceptions noted |

**Control objective B:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.12 | Changes to systems, databases or networks are made consistently with established procedures that ensure maintenance using relevant updates and patches, including security patches. | Checked by way of inspection that formalised procedures are in place for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches.<br>Checked by way of inspection of extracts from technical security parameters and set-ups that systems, databases or networks have been updated using agreed changes and relevant updates, patches and security patches. | We have noted in our sample test some Windows servers for one of the services are not patched according to Nuuday's baselines for the services Zylinc and RecordID.<br><br>We have also noted in our sample test that, Nuuday has updated the patches on the MSSQL databases in end of 2020 to a proper software version for the service Zylinc.<br><br>Regarding the TDC Secure Call Recording Pro: We have not received the inquired documentation regarding the TDC Secure Call Recording Pro in time, and we have therefore not been able to test the operational effectiveness for this control activity for the TDC Secure Call Recording Pro.<br><br>No further exceptions noted. |

**Control objective B:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.13 | A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need. | Checked by way of inspection that formalised procedures are in place for granting and removing users' access to systems and databases used for processing personal data.<br>Checked by way of inspection of a sample of employees' access to systems and databases that the user accesses granted have been authorised and that a work-related need exists.<br>Checked by way of inspection of a sample of resigned or dismissed employees that their access to systems and databases was deactivated or removed on a timely basis. | We have noted that for one of the services, that the internal responsibilities regarding user management in Nuuday are vaguely defined. In addition, user access creations and terminations are not managed sufficiently for the service Zylinc.<br>Furthermore, we have noted that no periodic review of certain user accounts and access rights has been performed.<br>Regarding the TDC Secure Call Recording Pro: We have not received the inquired documentation regarding the TDC Secure Call Recording Pro in time, and we have therefore not been able to test the operational effectiveness for this control activity for the TDC Secure Call Recording Pro.<br><br>No further exceptions noted. |
| B.14 | Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication. | Checked by way of inspection that formalised procedures are in place to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects.<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 exceptions noted. |

**Control objective B:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.15 | Physical access security measures have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed. | Checked by way of inspection that formalised procedures are in place to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed.<br>Checked by way of inspection of documentation that, throughout the assurance period, only authorised persons have had physical access to premises and data centres at which personal data are stored and processed. | No exceptions noted. |

**Control objective C:**

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

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

**Control objective C:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| C.3 | The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant:<br>• References from former employers<br>• Certificates of criminal record<br>• Driver´s license | Checked by way of inspection that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process.<br>Checked by way of inspection af sample of data processing agreements that the requirements therein for screening employees are covered by the data processor's screening procedures.<br>Checked by way of inspection of a sample of employees appointed during the assurance period that documentation exists of the screening having comprised:<br>• References from former employers<br>• Certificates of criminal record<br>• Driver´s license | No exceptions noted. |
| C.4 | Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data. | Checked by way of inspection a sample of employees appointed during the assurance period that the relevant employees have signed a confidentiality agreement.<br>Checked by way of inspection a sample of employees appointed during the assurance period that the relevant employees have been introduced to:<br>• The information security policy<br>• Procedures for processing data and other relevant information. | No exceptions noted. |

**Control objective C:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| C.5 | For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned. | Inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned.<br>Checked by way of inspection of samples of employees resigned or dismissed during the assurance period that rights have been deactivated or terminated and that assets have been returned. | No exceptions noted. |
| C.6 | Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers. | Checked by way of inspection that formalised procedures are in place to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality.<br>Checked by way of inspection of 6 employees resigned or dismissed during the assurance period that documentation confirms the continued validity of the confidentiality agreement and the general duty of confidentiality. | No exceptions noted. |
| C.7 | Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data. | 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>Inspected documentation stating that all employees who have either access to or process personal data have completed the awareness training provided. | No exceptions noted. |

**Control objective D:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| D.1 | Written procedures are in place which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.<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 formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller.<br>Checked by way of inspection that procedures are up to date. | No exceptions noted. |
| D.2 | The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines. | 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>Checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation states that personal data are stored in accordance with the agreed storage periods.<br>Checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation states that personal data are deleted in accordance with the agreed deletion routines. | We have been informed that Nuuday has not received any request for deletions of data and we can therefore not test the operation effectiveness of the control.<br>No further exceptions noted. |
| D.3 | Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been:<br>• Returned to the data controller and/or<br>• Deleted if this is not in conflict with other legislation. | Checked by way of inspection that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data.<br>Checked by way of inspection of a sample of terminated data processing sessions during the assurance period that documentation states that the agreed deletion or return of data has taken place. | We have been informed that Nuuday has not received any request for terminations of data and we can therefore not test the operation effectiveness of the control.<br>No further exceptions noted. |

Control objective E:

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| E.1 | Written procedures are in place which include a requirement that personal data must only be stored in accordance with the agreement with the data controller.<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 formalised procedures are in place for only storing and processing personal data in accordance with the data processing agreements.<br>Checked by way of inspection that procedures are up to date.<br>Checked by way of inspection of a sample of data processing sessions that documentation states that data processing takes place in accordance with the data processing agreement. | 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. | Checked by way of inspection that the data processor has a complete and updated list of processing activities stating localities, countries or regions.<br>Checked by way of inspection of a sample of data processing sessions that documentation states that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller. | No exceptions noted. |

**Control objective F:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| F.1 | Written procedures are in place which include requirements for the data processor when using subprocessors, including requirements for subprocessing agreements and instructions.<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 formalised procedures are in place for using subprocessors, including requirements for subprocessing agreements and instructions.<br>Checked by way of inspection that procedures are up to date. | No exceptions noted. |
| F.2 | The data processor only uses subprocessors 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 subprocessors used.<br>Checked by way of inspection of a sample of 7 subprocessors from the data processor's list of subprocessors that documentation states that the processing of data by the subprocessor follows from the data processing agreements – or otherwise as approved by the data controller. | We have noted that Amazon and Microsoft are not mentioned as approved subprocessors in the data processing agreements.<br>No further exceptions noted. |
| F.3 | When changing the generally approved subprocessors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved subprocessors used, this has been approved by the data controller. | Checked by way of inspection that formalised procedures are in place for informing the data controller when changing the subprocessors used.<br>Inspected documentation stating that the data controller was informed when changing the subprocessors used throughout the assurance period. | No exceptions noted. |

**Control objective F:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| F.4 | The data processor has subjected the subprocessor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller. | Checked by way of inspection for existence of signed subprocessing agreements with subprocessors used, which are stated on the data processor's list.<br>Checked by way of inspection of a sample of 7 subprocessing 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 exceptions noted. |
| F.5 | The data processor has a list of approved subprocessors disclosing:<br>• Name<br>• Company registration no.<br>• Address<br>• Description of the processing. | Checked by way of inspection that the data processor has a complete and updated list of subprocessors used and approved.<br>Checked by way of inspection that, as a minimum, the list includes the required details about each subprocessor. | We have noted that in some of the data procession agreements with the subdataprocessors, the CVR and description of the purpose with data processing are not disclosed.<br><br>No further exceptions noted. |

**Control objective F:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| F.6 | Based on an updated risk assessment of each subprocessor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the subprocessor. | Checked by way of inspection that formalised procedures are in place for following up on processing activities at subprocessors and compliance with the subprocessing agreements.<br>Checked by way of inspection of documentation that each subprocessor and the current processing activity at such processor are subjected to risk assessment.<br>Checked by way of inspection of documentation that technical and organisational measures, security of processing at the subprocessors used, third countries' bases of transfer and similar matters are appropriately followed up on.<br>Checked by way of inspection of documentation that information on the follow-up at subprocessors is communicated to the data controller so that such controller may plan an inspection. | No exceptions noted. |

**Control objective G:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| G.1 | Written procedures are in place which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.<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 formalised procedures are in place to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.<br>Checked by way of inspection that procedures are up to date. | No exceptions noted. |
| G.2 | The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller. | Checked by way of inspection that the data processor has a complete and updated list of transfers of personal data to third countries or international organisations.<br>Checked by way of inspection of a sample of data transfers that documentation states that such transfers were arranged with the data controller in the data processing agreement or subsequently approved. | 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. | Checked by way of inspection that formalised procedures are in place for ensuring a valid basis of transfer.<br>Checked by way of inspection that procedures are up to date.<br>Checked by way of inspection of a sample of data transfers that documentation confirms a valid basis of transfer in the data processing agreement with the data controller and that transfers have only taken place insofar as this was arranged with the data controller. | No exceptions noted. |

**Control objective H:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| H.1 | Written procedures are in place which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects.<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 formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects.<br>Checked by way of inspection that procedures are up to date. | No exceptions noted. |
| H.2 | The data processor has established procedures that, insofar as this was agreed, enable timely assistance to the data controller in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects. | Checked by way of inspection that the procedures in place for assisting the data controller include detailed procedures for:<br>• Handing out data<br>• Correcting data<br>• Deleting data<br>• Restricting the processing of personal data<br>• Providing information about the processing of personal data to data subjects.<br>Checked by way of inspection of documentation that the systems and databases used support the performance of the relevant detailed procedures. | No exceptions noted. |

**Control objective I:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| I.1 | Written procedures are in place which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches.<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 formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches.<br>Checked by way of inspection that procedures are up to date. | No exceptions noted. |
| I.2 | The data processor has established the following controls to identify any personal data breaches:<br>• Awareness of employees<br>• Monitoring of network traffic<br>• Follow-up on logging of access to personal data | Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches.<br>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.<br>Checked by way of inspection of documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on in a timely manner. | No exceptions noted. |

**Control objective I:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| I.3 | If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than 24 hours after having become aware of such personal data breach at the data processor or a subprocessor. | 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>Made inquiries of the subprocessors as to whether they have identified any personal data breaches throughout the assurance period.<br>Checked by way of inspection that the data processor has included any personal data breaches at subprocessors in the data processor's list of security incidents.<br>Checked by way of inspection that all personal data breaches recorded at the data processor or the subprocessors have been communicated to the data controllers concerned without undue delay and no later than 24 hours after the data processor became aware of the personal data breach. | No exceptions noted. |
| I.4 | The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency. These procedures must contain instructions on descriptions of:<br>• The nature of the personal data breach<br>• Probable consequences of the personal data breach<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 instructions for:<br>• Describing the nature of the personal data breach<br>• Describing the probable consequences of the personal data breach<br>• Describing measures taken or proposed to be taken to respond to the personal data breach.<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 exceptions noted. |

# 5. Additional information from Nuuday A/S

The information included in this section is prepared by Nuuday A/S (Nuuday) to provide the customer with further information. The section should not be regarded as a part of the system description. The information in this section is not covered by audit procedures performed to assess whether the system description is fairly presented, whether the controls supporting the control objectives presented in section 4 have been suitably designed and whether they operated effectively throughout the period. Thus, PwC's opinion in section 2 does not cover the information in section 5.

Management of Nuuday A/S has strong focus on remediation of the observations identified in this audit report. Management has prepared the following action plan for sharing progress regarding the basis for modified opinion in section 2:

Nuuday will ensure that an allonge to this audit report is prepared covering the technical measurement regarding the TDC Secure Call Recording Pro service, which will address all the relevant control activities from 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" in section 3. This will be done as soon as Nuuday has received all relevant documentation from the subcontractor. The allonge is expected to be finished no later than the end of Q3 2021.