Unik System Design A/S

Independent service auditor's ISAE 3000 assurance report on information security and measures pursuant to the Appendix 4 - data processing agreement with Unik System Design as of 30 November 2024

Contents

1 Management's statement

Unik System Design (hereafter Unik) processes personal data for data controller in accordance with the data processing agreement, Appendix 4 to the main agreement.

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

Unik uses several subservice organizations accounted for in section 3. Most importantly is GlobalConnect for operations/housing and Sentia Danmark which delivers and operates the physical infrastructure for the virtual hosting environment. Sentia also provides data backup. The Description includes only the control objectives and related controls of Unik and excludes the control objectives and related controls of the subservice organizations. Certain control objectives specified in the Description can be achieved only if subservice organizations controls assumed in the design of our controls are suitably designed and implemented. The Description does not extend to controls of the subservice organizations.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Unik's controls are suitably designed and operating effectively, along with related controls at the data processor. The Description does not extend to controls of the data controller.

Unik System Design confirms that:

a) The accompanying description in section 3, fairly presents Unik services, which has processed personal data for data controllers subject to the Regulation as of 30 of November 2024. The criteria used in making this statement were that the accompanying description:

   (i) Presents how Unik 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 safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
- Controls that we, in reference to the scope of Unik 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) Does not omit or distort information relevant to the scope of Unik's 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 Unik System Design 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 as of 30 of November 2024, if controls at subservice organisations are working effectively, and data controller applied the complementary user entity controls assumed in the design of Unik System Design's controls as of 30 of November 2024. The criteria used in making this statement were that:

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

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

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

Vejle, 13. December 2024
Unik System Design A/S

Jens Find
CEO

2 Independent service auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to Appendix 4 - data processing agreement with Unik System Design

To: Unik System Design and its customers

Scope

We were engaged to provide assurance about Unik System Design's (hereafter Unik) description in section 3 of Unik's services in accordance with Appendix 4 - data processing agreement as of 30 November 2024 ("the Description") and on the design of controls related to the control objectives stated in the Description. We express reasonable assurance in our conclusion.

We did not perform any procedures regarding the operating effectiveness of controls included in the description and, accordingly, do not express an opinion thereon.

The Description indicates that certain control objectives can only be achieved if the complementary user entity controls assumed in the design of Unik's controls are suitably designed and operating effectively, along with related controls at Unik System Design. Our engagement did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Unik uses several subservice organizations accounted for in section 3. Most importantly is GlobalConnect for operations/housing and Sentia Danmark which delivers and operates the physical infrastructure for the virtual hosting environment. Sentia also provides data backup. The Description includes only the Control Objectives and related controls of Unik and excludes the control objectives and related controls of subservice organizations. Certain Control Objectives specified by Unik can be achieved only if subservice organization controls assumed in the design of Unik controls are suitably designed and operating effectively, along with the related controls at Unik. Our engagement did not extend to controls of subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such subservice organization controls.

Unik System Design's responsibilities

Unik is responsible for: preparing the Description and the accompanying statement in section 1, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; identifying the risks that threaten the achievement of the Control Objectives, selecting the criteria presented in the statement, and designing, implementing and effectively operating controls to achieve the stated control objectives.

Our independence and quality control

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

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

Our responsibilities

Our responsibility is to express an opinion on Unik System Design's Description and on the design of controls related to the control objectives stated in that Description, based on our procedures.

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "*Assurance Engagements Other than Audits or Reviews of Historical Financial Information*", and

additional requirements under Danish audit regulation, to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are appropriately designed.

An assurance engagement to report on the Description and design of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its different services used to process personal data and about the design of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not appropriately designed.

An assurance engagement of this type also includes evaluating the overall presentation of the Description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by Unik System Design and the described in section 1.

As noted above, we did not perform any procedures regarding the operating effectiveness of controls included in the Description and, accordingly, do not express an opinion thereon.

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

Limitations of controls at a data controller

Unik System Design's Description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Unik System Design's services 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.

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 section 1 "Management's statement". In our opinion, in all material respects:

a) The Description fairly presents Unik services as designed and implemented as of 30 of November 2024;

b) The controls related to the control objectives stated in the Description were suitably designed as of 30 of November 2024, if relevant controls at subservice organisations are suitably designed, and data controllers applied the complementary user entity controls assumed in the design of Unik System Design's controls as at 30 of November 2024.

Description of tests of controls

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

Intended users and purpose

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

Copenhagen, 13. december 2024
EY Godkendt Revisionspartnerselskab
CVR no.: 30 70 02 28

Jesper D. Sørensen
Partner

Nils B. Christiansen
State Authorized Public Accountant
mne34106

3 Description of processing

Unik System Design A/S (hereafter Unik) is a Danish-owned company developing and operating various IT solutions for the property management industry and for the legal sector. Unik's headquarter is located in Vejle, with additional locations in Aalborg and Copenhagen. Furthermore, Unik has a team of Polish developers in Warsaw.

Unik processes personal data on behalf of our customers, where Unik acts as the data processor and the customer acts as the data controller. Therefore, a data processing agreement has been established between Unik and the data controller for the solutions described below.

3.1 Nature of processing

Unik provides the following IT-solutions:

On-prem client-server-solutions:

- Unik Bolig
- Unik Advosys
- Unik Hosting

Cloud-enabled versions:

- Unik Bolig CE
- Unik Advosys CE

SaaS solutions:

- HabiCen
- JustiCase
- JustiBusiness
- i-produkter
- uHabi

Unik Bolig and Unik Advosys are provided as on-prem client-server-solutions. These solutions can be hosted by Unik, by the customer themselves, or by a third party.

The remaining solutions are SaaS solutions. Over time, Unik Bolig and Unik Advosys will be replaced by HabiCen and JustiCase and JustiBusiness. Unik Bolig CE and Unik Advosys CE are cloud-enabled versions for our upcoming SaaS solutions for efficient synchronization of data from existing on-prem client-server-solutions to our forthcoming SaaS solutions.

There may be cases where the customer sends databases to Unik for support, debugging or similar reasons. In such cases, an addendum to the data processing agreement will be prepared to provide formal instructions for the processing of personal data contained in the customer-sent databases.

The data controllers must ensure that access is only given to the customer solution to which the support inquiry relates as well as using the FTP server established by Unik when they send data to Unik.

3.2 Personal data

Unik's solutions are designed to process ordinary personal data under Article 6 of the General Data Protection Regulation. The solutions are also designed to process Personal Identification Numbers (CPR numbers), which should be considered as confidential personal data under Danish data protection law.

Additionally, there may be sensitive personal data under Article 9 and criminal data under Article 10 of the General Data Protection Regulation, as Unik provides solutions to the legal sector in the form of case management systems. Unik cannot control the amount and categorization of personal data, as this will vary depending on the activities and size of the data controller.

- For Unik Bolig, Unik Bolig CE, HabiCen, uHabi, and i-products: the data subjects covered by the data processing agreement will include employees, tenants, creditors and debtors, suppliers, and business partners of the data controller.
- For Unik Advosys, Unik Advosys CE, JustiCase, and JustiBusiness: the data subjects covered by the data processing agreement will include employees, clients, parties in cases, opposing parties, witnesses, creditors and debtors, suppliers, and business partners of the data controller.

3.3 Practical measures

Unik has prepared requirements for establishing, implementing, maintaining, and improving a management system for the security of personal data, which ensure compliance with the concluded agreements with the data controllers, good data processor practice, and relevant requirements for Data Processors in accordance with the General Data Protection Regulation and the Data Protection Act.

3.4 Risk assessment

For each processing activity, IT system/information activity, and data recipient, an assessment of the likelihood of loss of confidentiality, integrity, or availability has been conducted. This assessment is based on known potential threats and the measures implemented to protect the confidentiality, integrity, and availability of the information. An assessment of the potential consequences for the data subjects in the event of loss of confidentiality, integrity, or availability has also been conducted. The assessment is based on whether the information is general, confidential, or sensitive and the potential indirect consequences regarding the type of personal data.

Based on the assessment of the likelihood and consequences of the processing activity, a risk rating has been calculated. These assessments are conducted by those responsible for the processing activities in collaboration with the Compliance team. Based on the assessments, an impact assessment analysis and an action plan will be initiated if the risk for the specific processing is deemed too high.

3.5 Control measures

Unik has formulated and implemented measures for secure processing of personal data. These measures have been prepared on the basis of the requirements of the Data Processing Agreement.

See also section 4 for a description of the specific control activities.

3.5.1 Control Objective A: Compliance with instructions

Unik only processes personal data according to instructions from the data controller. Such instructions are provided through a data processing agreement or an addendum to the data processing agreement. A policy for processing the data controller's personal data has been implemented, which includes guidelines for processing under instructions. All employees at Unik have been instructed to follow these guidelines.

3.5.2 Control Objective B: Technical measures

Based on the risk assessments, Unik has implemented technical measures, which are as follows:

- Antivirus for Unik's own servers and clients
- Firewall for Unik's own servers
- User access controls to personal data
- Encryption of sensitive personal data via internet and emails
- Logging
- Vulnerability scanning
- Patching

- Based on a risk assessment, physical security access controls to locations and server rooms have been implemented

In addition, Unik has outsourced some of the responsibilities for implementing technical measures to subcontractor Sentia, which supplies and operates the physical infrastructure for the virtual hosting environment where Unik Bolig and Unik Advosys are implemented, including servers, networks, storage system, firewall, internet connection, power supplies, firefighting equipment and refrigeration. Sentia also provides data backup.

Unik has developed a new hosting platform at Global Connect and Unit IT. This means that Sentia will continuously cease to be a sub-data processor, and the platform will be phased out as customers are moved. Going forward GlobalConnect will supply data center services such as floor space, internet connection, power supplies, fire extinguishing equipment and cooling for Unik Bolig, Unik Bolig CE, Unik Advosys and Unik Advosys CE. Unit IT will deliver off-site immutable backup instead of Global Connect, which is relevant for all customers who have entered into a new agreement for Unik Bolig, Unik Bolig CE, Unik Advosys or Unik Advosys CE.

3.5.3 Control Objective C: Organizational measures

Unik has implemented an IT security policy that includes instructions for Unik's employees. The IT security policy has been approved by Unik's top management and is reviewed at least annually.

All employees are subject to confidentiality agreements as part of their employment contract or associated non-disclosure agreements (NDAs).

Unik has implemented mandatory awareness training for all employees.

3.5.4 Control Objective D: Deletion and return of personal data to data controller

Unik deletes and/or returns the data controller's data upon termination of the agreement, as described in the data processing agreement or upon specific request from the data controller.

3.5.5 Control Objective E: Records of processing

Unik processes the data controller's data as described in the data processing agreement. The data processing agreement includes a list of approved sub-processors.

Data processing locations are within the EU.

3.5.6 Control Objective F: Sub-processors

Unik only uses sub-processors listed in the data processing agreement. Unik maintains a register of sub-processors and performs a minimum of one annual review of sub-processors regarding their handling of personal data. Unik ensures that sub-processors meet at least the same requirements as those specified in the data processing agreement between Unik and the data controller. Unik notifies the data controller of changes to sub-processors within the notice periods established in the data processing agreement.

Unik transfers only personal data to third party countries if the data controller instructs Unik to do so. In the event of transferring personal data to a third country, Unik ensures that there is a valid basis for transfer.

There are no situations where Unik transfers personal data to third parties.

3.5.7 Control Objective H: Right of the registered persons

In the event of requests from data subjects, the data controller will be contacted. Unik supports the data controller in addressing requests from data subjects.

3.5.8 Control Objective I: Personal data breach management

Unik has implemented processes for handling data breaches. In the event of a data breach, Unik ensures that the data controller is promptly notified. Unik supports the data controller in reporting the data breach to the Danish data protection authority, Datatilsynet.

3.6 Complementary controls at the data controllers

In addition to Unik's control measures, it is the data controller's own responsibility to:

- ensure that personal data in the systems is kept up to date.
- assess which personal data the system must contain.
- ensure the content of the free text fields is within the framework of the data processing agreement.
- have identified a purpose and a valid authority for the processing of data.
- ensure that instructions given are legal in relation to the personal data legislation applicable at any time.
- ensure that the instructions to Unik are appropriate in relation to the data processor agreement and the main service.
- Implementation of technical as well as organizational controls to systems where Unik is not hosting.

4 Control objectives, control activity, tests and test results

4.1 Purpose and scope

Our work was performed in accordance with ISAE 3000, Assurance Engagements other than audits or reviews of historical financial information.

Our test of the controls' design and implementation comprised the control objective and related controls, which have been selected by Management and which are stated below. Any other control objectives, related controls and controls at Data Controllers are not covered by our tests.

The tests performed in connection with the determination of design and operating effectiveness of controls are outlined below.

4.2 Tests performed

Below, we have summarised the tests performed by EY in order to assess controls relevant to Unik System Design's information security and measures pursuant to the data processing agreement:

Inspection	Reading of documents and reports which contain disclosure on the performance of the control. This work includes i.a. the reading of and position-taking to reports and other documentation to assess whether specific controls have been designed in a way that allow them to be effective, if implemented. Furthermore, we assess whether controls are adequately monitored at suitable intervals. As to the technical platforms, databases and network components, we tested the specific system set-up to ensure that controls were implemented as of 30 of November 2024. Our tests comprised i.a. an assessment of the patching level, services allowed, segmenting, password complexity, etc.
Inquiries	Inquiries of suitable staff with Unik System Design. Inquiries comprised i.a. the performance of controls.
Observation	We observed the performance of controls.

4.3 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.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
A.1	Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures exist to ensure that personal data are only processed according to instructions. Inspected 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. Inspected that procedures are up to date.	No deviations noted.
A.2	Unik only processes personal data stated in the instructions from the data controller.	Inspected that Unik ensures that personal data are only processed according to instructions. Inspected a sample of one data processor agreement, that instructions have been agreed upon herein.	No deviations noted.
A.3	Unik 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.	Inspected that formalised procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation. Inspected that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation.	We have been informed by Unik, that they have not detected any cases close to the assurance date, where the processing of personal data was evaluated to be against legislation. No deviation 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.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
		Inquired whether Unik has registered any cases where the processing of personal data was evaluated to be against legislation.	

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.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
B.1	Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures exist to ensure establishment of the safeguards agreed. Inspected that procedures are up to date. Inspected a sample of one data processing agreement that safeguards have been agreed upon herein.	No deviations noted.
B.2	Unik has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller.	Inspected that formalised procedures are in place to ensure that Unik performs a risk assessment to achieve an appropriate level of security. Inspected that the risk assessment performed is up to date and comprises the current processing of personal data. Inspected that Unik has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment.	No deviations noted.
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.	Inspected that, for the systems and databases used in the processing of personal data, antivirus software has been installed. Inspected that antivirus software is up to date.	No deviations noted.
B.4	External access to systems and databases to SaaS solutions used in the processing of personal data takes place through a secured firewall.	Inspected that external access to systems and databases to SaaS solutions used in the processing of personal data takes place only through a secured firewall.	No deviations 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.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
		Inspected that the firewall to SaaS solutions has been configured in accordance with the relevant internal policy.	
B.6	Access to personal data is isolated to users with a work-related need for such access.	Inspected that formalised procedures are in place for restricting users' access to personal data. Inspected that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need. Inspected that the technical measures agreed support retaining the restriction in users' work-related access to personal data. Inspected a sample of one users' access to systems and databases that such access is restricted to the employees' work-related need.	No deviations noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	Inspected that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet or by email are protected by encryption. Inspected that technological encryption solutions have been available and active around the assurance date.	No deviations 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.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
		Inspected that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	
B.9	Logging of the following matters has been established: ► Unik users access to customer data in Unik Advosys, Unik Advosys CE, Unik Bolig and Unik Bolig CE, where data controllers have these solutions hosted by Unik. ► Unik users' access to customer data in i-produkter. If requested by the Data Controller, Unik will review logs.	Inspected that logging of user access to systems, databases that are used to process or transmit personal data for Unik Advosys, Unik Advosys CE, Unik Bolig and Unik Bolig CE and i-products has been configured and activated close to the assurance date. Inspected of a sample of logging configurations that the content of log files is as expected compared to the setup. Inquired whether Unik has received requests from data controllers regarding the review of logs.	No deviations noted.
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form.	Inspected that formalised procedures exist for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. Inspected a sample of one development or test environment that personal data included therein are pseudonymised or anonymised.	No deviations noted.
B.11	The technical measures established are tested on a weekly basis through vulnerability scans.	Inspected that formalised procedures exist for performing vulnerability scans.	No deviations 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.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
		Inspected for one sample that documentation exists regarding regular testing of the technical measures established. Inspected that any deviations or weaknesses in the technical measures have been responded to in a timely manner.	
B.12	Procedures are established to ensure maintenance using relevant updates and patches, including security patches.	Inspected that formalised procedures exist for handling relevant updates and patches, including security patches. Inspected extracts from technical security parameters and setups that systems, databases or networks have been updated using agreed relevant updates, patches and security patches.	No deviations noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reviewed once a year, including the continued justification of rights by a work-related need.	Inspected that formalised procedures exist for granting and removing users' access to systems and databases used to process personal data. Inspected a sample of one employees' access to systems that the user accesses granted have been authorised and that a work-related need exists. Inspected a sample of one resigned or dismissed employees that their access to systems and databases was deactivated or removed on a timely basis.	No deviations 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.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
		Inspected that documentation exists that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	
B.15	Based on a risk assessment, physical access safeguards have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	Inspected that formalised procedures exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. Inspected documentation close to the assurance date, that only authorised persons have had physical access to premises and data centres at which personal data are stored and processed, based on a risk assessment.	No deviation 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.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
C.1	Management of Unik has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	Inspected that an information security policy exists which Management has considered and approved within the past year. Inspected documentation that the information security policy has been communicated to Unik's employees.	No deviations noted.
C.2	Management of Unik has checked that the information security policy does not conflict with data processing agreements entered into.	Inspected Management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered into. Inspected a sample of one data processing agreement that the requirements in this agreement are covered by the requirements of the information security policy for safeguards and security of processing.	No deviations 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.	Inspected a sample of one employee appointed close to the assurance date that the relevant employee has signed a confidentiality agreement. Inspected a sample of one employee appointed close to the assurance date that the relevant employee has been introduced to procedures for processing data and other relevant information.	No deviations 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.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
C.5	For resignations or dismissals, Unik 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. Inspected a sample of one employee resigned or dismissed close to the assurance date, that rights have been deactivated or terminated and that assets have been returned.	No deviations 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 Unik for the data controllers.	Inspected a sample of one employee resigned or dismissed close to the assurance date that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality.	No deviations noted.
C.7	Awareness training is provided to Unik's employees on a regular basis with respect to general IT security and security of processing related to personal data.	Inspected procedure for awareness training. Inspected a sample of one, that the offered training contains topics within GDPR and information security. Inspected a sample of one, that quarterly follow-up is carried out to ensure that the employees have carried out the planned training.	No deviations 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.	*Uniks control activity*	*Test performed by EY*	*Result of EY's test*
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. Inspected that the procedures are up to date.	No deviations noted.
D.2	The following specific requirements have been agreed with respect to Unik's storage periods and deletion routines: ► Upon termination of customer agreement, Unik will delete the data within 90 days and confirm to the data controller that this has taken place.	Inspected that the existing procedures for storage and deletion include specific requirements for Unik's storage periods and deletion routines. Inspected a sample of one, that documentation exists that personal data can be deleted in accordance with the procedures.	No deviations 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: ► Returned to the data controller; and/or ► Deleted if this is not in conflict with other legislation.	Inspected that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data. Inspected one terminated data processing session close to the assurance date regarding Unik Bolig and Unik Advosy that documentation exists that the agreed deletion or return of data has taken place. Inquired a sample of one terminated data processing session regarding SaaS solutions, that documentation exists that the agreed delegation of data has taken place.	We have been informed by Unik, that there has not been any termination of the processing of personal data for the data controller regarding all SaaS solutions close to the assurance date. No deviation 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.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
E.1	Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. Inspected that the procedures are up to date.	No deviations noted.
E.2	Data processing and storage by Unik must only take place in the localities, countries or regions approved by the data controller.	Inspected a sample of one data processing agreement that documentation exists that the processing of data, including the storage of personal data, takes place in the localities stated in the data processing agreement.	No deviations noted.

Control objective F Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.			
No.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
F.1	Written procedures exist which include requirements for Unik when using sub-data processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions. Inspected that procedures are up to date.	No deviations noted.
F.2	Unik only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.	Inspected that Unik has a complete and updated list of sub-data processors used. Inspected a sample of one sub-processor from the list of sub-processors that documentation exists that the processing of data by the sub-processor is stated in the data processing agreements – or otherwise approved by the data controller.	No deviations noted.
F.3	When changing the generally approved sub-data processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from Unik. When changing the specially approved sub-data processors used, this has been approved by the data controller.	Inspected that formalised procedures are in place for informing the data controller when changing the sub-data processors used. Inspected documentation that the data controller was informed when changing the sub-data processors used throughout the assurance period.	No deviations noted.

Control objective F Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.			
No.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
F.4	Unik has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	Inspected existence of signed sub-data processing agreements with sub-data processors used, which are stated on the data processor's list. Inspected a sample of one sub-data processing agreements that they include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.	No deviations noted.
F.5	Unik has a list of approved sub-data processors disclosing: ► Name ► Service-type ► Criticality	Inspected that Unik has a complete and updated list of sub-data processors used and approved. Inspected that, as a minimum, the list includes the required details about each sub-data processor.	No deviations noted.
F.6	Based on an updated risk assessment of each sub-data processor and the activity taking place at such processor, Unik regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity.	Inspected that formalised procedures are in place for following up on processing activities at sub-data processors and compliance with the sub-data processing agreements. Inspected a sample of one sub-processor that documentation exists that the sub-processor and the current processing activity at such processor are subjected to risk assessment. Inspected a sample of one sub-processor that documentation exists that technical and organisational measures, security of processing	No deviations noted.

Control objective F Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.			
No.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
		at the sub-data processors used, third countries' bases of transfer and similar matters are appropriately followed up on.	

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.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
H.1	Written procedures exist which include a requirement that Unik must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place for Unik's assistance to the data controller in relation to the rights of data subjects. Inspected that procedures are up to date.	No deviations noted.
H.2	Unik has established procedures in so far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects.	Inspected that the procedures in place for assisting the data controller include detailed procedures for: ► Handing out data; ► Correcting data; ► Deleting data; ► Restricting the processing of personal data; ► Providing information about the processing of personal data to data subjects. Inspected a sample of one, that requests by the data controller for assistance in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects have been documented in a correct and timely manner.	No deviations 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.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
I.1	Written procedures exist which include a requirement that Unik must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Inspected that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. Inspected that procedures are up to date.	No deviations noted.
I.2	Unik has established the following controls to identify any personal data breaches: ► Awareness of employees; ► Performing vulnerability scans	Inspected that Unik provides awareness training to the employees in identifying any personal data breaches. Inspected for one sample that documentation exists regarding regular testing of the technical measures established.	No deviations noted.
I.3	If any personal data breach occurred, Unik will inform the data controller without undue delay and no later than 48 hours after having become aware of such personal data breach at Unik or a sub-data processor.	Inspected that Unik has a list of security incidents disclosing whether the individual incidents involved a personal data breach. Inquired whether sub-data processors have identified any personal data breaches throughout the assurance period. Inspected that Unik has included any personal data breaches at sub-data processors in the list of security incidents.	We have been informed by Unik, that no personal data breach occurred close to the assurance date. No deviation noted.
I.4	Unik has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency:	Inspected that the procedures in place for informing the data controllers in the event of	We have been informed by Unik, that they have not assisted the data controllers in filing reports with the Danish Data

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.	*Unik's control activity*	*Test performed by EY*	*Result of EY's test*
	▶ Nature of the personal data breach; ▶ Probable consequences of the personal data breach; ▶ Measures taken or proposed to be taken to respond to the personal data breach.	any personal data breach include detailed procedures for: ▶ Describing the nature of the personal data breach; ▶ Describing the probable consequences of the personal data breach; ▶ Describing measures taken or proposed to be taken to respond to the personal data breach. Inspected documentation that the procedures available support that measures are taken to respond to the personal data breach.	Protection Agency close to the assurance date. No deviation noted.

PENNEO

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

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

Jens Jensen Find
CEO
På vegne af: Unik System Design A/S
Serienummer: d91ee1b4-c5d4-4873-ac07-b3d53dcce46e
IP: 194.192.xxx.xxx
2024-12-13 10:52:48 UTC

Mit ID

Nils Bonde Christiansen
EY Godkendt Revisionspartnerselskab CVR: 30700228
Statsaut. revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: a4c7bea3-5a9f-4f35-bb2c-9ca1124e41f1
IP: 165.225.xxx.xxx
2024-12-13 13:54:37 UTC

Mit ID

Jesper Due Sørensen
EY Godkendt Revisionspartnerselskab CVR: 30700228
Partner
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: a6d834d7-442d-428e-ade9-c250dca23ab3
IP: 37.96.xxx.xxx
2024-12-13 14:05:12 UTC

Mit ID