www.pwc.dk

IT Relation A/S

Independent auditor's ISAE 3000 assurance report on information security and measures as at 31 March 2021 pursuant to the data processing agreement with data controllers

May 2021

pwc

Contents

1. Management's statement

IT Relation A/S processes personal data on behalf of data controllers in accordance with the data processing agreement.

The accompanying description has been prepared for data controllers who have used the hosting services and who have 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.

IT Relation A/S uses Eniig and InterXion as subprocessors for housing services. This report uses the carve-out method and does not comprise controls that Eniig and InterXion perform for IT Relation A/S.

IT Relation A/S uses B4Restore and Front-Safe as subprocessors for backup services. This report uses the carve-out method and does not comprise controls that B4Restore and Front-Safe perform for IT Relation A/S.

IT Relation A/S confirms that:

a) The accompanying description in section 3 fairly presents the hosting services that have processed personal data for data controllers subject to the data protection rules as at 31 March 2021. The criteria used in making this statement were that the accompanying description:

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

   - The types of services provided, including the type of personal data processed;
   - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete and restrict processing of personal data;
   - The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller;
   - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
   - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation;
   - The procedures supporting, in the event of breach of personal data security, that the data controller may report this to the supervisory authority and inform the data subjects;
   - The procedures ensuring appropriate technical and organisational 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 hosting 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 the hosting 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 the hosting 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 at 31 March 2021. 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; and

(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.

c) Appropriate technical and organisational measures were established 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.

Herning, 25 May 2021

Frank Bech Jensen

IT Relation A/S
Dalgas Plads 7B, 1 Floor
DK-7400 Herning

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures as at 31 March 2021 pursuant to the data processing agreement with data controllers

To: IT Relation A/S and IT Relation A/S' customers

Scope

We have been engaged to provide assurance about IT Relation A/S' description in section 3 of the hosting services in accordance with the data processing agreement with data controllers as at 31 March 2021 (the description) and about the design related to the control objectives stated in the description.

Our report covers whether IT Relation A/S has designed appropriate controls related to the control objectives stated in section 4. The report does not include an assessment of IT Relation A/S' 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").

IT Relation A/S uses Eniig and InterXion as subprocessors for housing services. This report uses the carve-out method and does not comprise controls that Eniig and InterXion perform for IT Relation A/S.

IT Relation A/S uses B4Restore and Front-Safe as subprocessors for backup services. This report uses the carve-out method and does not comprise controls that B4Restore and Front-Safe perform for IT Relation A/S.

We have not performed procedures regarding the operating effectiveness of the controls included in section 4, and therefore we do not express any opinion thereon.

We express reasonable assurance in our conclusion.

IT Relation A/S' responsibilities

IT Relation A/S 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 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 IT Relation A/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 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.

An assurance engagement to report on the description and the design of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its hosting services and about the design 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. 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.

As mentioned above, we have not performed procedures regarding the operating effectiveness of the controls included in section 4, and therefore we do not express any 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 processor

IT Relation A/S' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the hosting 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 the Management's statement section. In our opinion, in all material respects:

a) The description fairly presents the hosting services as designed and implemented as at 31 March 2021; and

b) The controls related to the control objectives stated in the description were suitably designed as at 31 March 2021.

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 IT Relation A/S' hosting 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.

Aarhus, 25 Maj 2021
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab

Jesper Parsberg Madsen
State-Authorised Public Accountant

Iraj Bastar
Director

3. Description of processing

The purpose of the data processor's processing of personal data on behalf of the data controller is to provide the services agreed between the data responsible and the data processor. Services are further defined in the individual customer's contract (s) and are within the areas Hosting and operations, Service desk, Application services and Consultancy services. The data controller's instructions on data processing are defined in the data processor agreement between the partners.

Nature of processing

The data processor's processing of personal data on behalf of the data controller primarily concerns:

Hosting and operation

The data processor will provide hosting and operation of the data controller's IT systems and application services. Thus, the primary purpose of processing of personal data is hosting, including storage of the data controller's personal data, and day-to-day operation, including monitoring, backup and maintenance of the data controller's IT systems containing personal data.

In specific situations, processing may include organisation, structuring, facilitation, temporary storage, filtration, trouble-shooting, adaptation or alteration, retrieval, consultation, use, alignment, combination, restriction or erasure of personal data when so required in connection with the data processor's supply of services to the data controller, or if so required in order to comply with a specific request from the data controller.

The data processor will provide IT support to the data processor's employees etc. Any work undertaken by the data processor as part of this support, and which includes processing of personal data on behalf of the data controller, will be based on a specific request of the data controller.

Service desk

The data processor will provide support to the data controller as regards the data controller's day-to-day operation of the data controller's IT systems. At the request of the data controller, the data processor may take over the data controller's management of the data controller's IT system in the workplace or servers via TeamViewer or Remote Desktop for a specific task. In addition, the data processor may access systems for the purpose of troubleshooting and operational tasks.

In case of software failures or failures in the data controller's IT system in general, the data processor may obtain the database from the data controller for the purpose of troubleshooting, making corrections, etc. This is always subject to prior agreement.

In specific situations, processing may include organisation, structuring, facilitation, temporary storage, filtration, trouble-shooting, adaptation or alteration, retrieval, consultation, use, alignment, combination, restriction or erasure of personal data when so required in connection with the supply of the agreed services, or if so required in order to comply with a request from the data controller.

Application services

Support, operation, backup and application maintenance. The following applications are two of most important applications:

Sepo – Secure Mail

The service specifically includes:

- Encryption/decryption/signing/forwarding of emails (and possibly digital mail (Digital Post)/electronic postbox notices (e-Boks)) to and from the data controller
- Storage of the data controller's cryptographic key(s).

TK2 EPJ

The data processor provides maintenance and support of the TK2 EPJ IT system to the data controller. Any work undertaken by the data processor, and which includes processing of personal data on behalf of the data controller, will be based on a specific request of the data controller.

The data processor will provide support to the data controller in Team Viewer. At the request of the data controller, the data processor may take over the data controller's management of the system via Team Viewer for a specific task.

In case of product failures, the data processor may obtain the TK2 SQL database from the data controller for the purpose of troubleshooting, making corrections, etc.

In specific situations, processing may include organisation, structuring, facilitation, temporary storage, filtration, trouble-shooting, adaptation or alteration, retrieval, consultation, use, alignment, combination, restriction or erasure of personal data when so required in connection with the supply of the agreed services, or if so required in order to comply with a request from the data controller.

Consultancy services

The data processor will carry out specific and limited tasks. Consultancy tasks are carried out in the data controller's systems and with the data controller's data, and the processing will be defined for each specific task.

Tasks are requested and defined by the data controller, and the data processor will assist to the extent required in order to ensure a proper definition of tasks.

Personal data

The personal data that IT Relation processes on behalf of the data controller varies from customer to customer.

When entering into a data processor agreement, the data controller must ensure that the correct types of personal data and categories of data subjects have been defined in the data processing agreement.

Practical measures

The level of security shall reflect a generally high level of security reflecting the types of data being processed. Technical and organisational measures are implemented pursuant to the ISO 27001 standard security framework. All controls from ISO 27002 are implemented and complied with.

In addition, the level of security must reflect the specifically agreed services in the parties' agreement regarding the data processor's provision of services to the data controller.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the agreed level of data security.

At the time of commencement of the agreement, the obligation for the data processor to carry out security measures involves to implement and maintain the security level described in the documents "Organisational and Technical Measures" and "Physical and Logical Security". The documents are available in the data processor's customer portal and at www.itrelation.dk/gdpr-dokumenter. These security requirements represent the data controller's total requirements in terms of security matters with the data processor based on the data controller's own risk assessment.

Risk assessment

As part of the ISO 27001 security framework, IT Relation works in a structured manner with risk management. This is done through risk assessments of the implemented controls, data processing and suppliers (sub-processors).

Risk assessments are made on the basis of a probability / consequence model, and relevant and probable threats are used in the assessment. Based on the assessment, there will be threats that receive a score that is above IT Relations' maximum risk acceptance, and these threats will subsequently be treated in a risk plan, with the aim of minimising or eliminating risk.

For suppliers, another angle is applied in the risk assessment. IT Relation's experience of the supplier's security is included in the assessment. This includes a review of security breaches at the supplier, as well as obtaining and reviewing the supplier's audit report. If the supplier does not provide a standard audit report, or if there have been serious observations in the statement, follow-up with supervision is based on a control assessment form.

Risk assessments are updated regularly and at least once a year.

Control measures

IT Relation has implemented the following control measures:

Data processor agreements

Written data processor agreements are entered into with both customers and subcontractors. The agreement with customers is based on IT Relation's standard data processor agreement, which again is based on the Danish Data Protection Agency's standard template.

When entering a data processor agreement with a customer, this agreement is archived in IT Relation's data processor agreement system. Here, any deviations to the standard of the agreement are also registered, and implementation of the agreement is ensured. New customers must enter a data processor agreement before IT Relation can begin processing of the customer's data.

Yearly review of procedures

Once a year or in the event of major changes, IT Relation reviews the applicable standard and concluded data processor agreements to see if there are changes in e.g. guidelines and procedures. In this work, IT Relation involves their legal partner.

Once a year, suppliers are inspected, reviewed and risk assessed. In this work, audit statements are obtained from the subcontractors, which must be based on current standards. For suppliers who do not have an audit statement, extended supervision is performed.

When IT Relation receives a GDPR inquiry, it is processed based on a fixed procedure. Effective feedback is ensured to the data controller or data subject, and inquiries are processed within 30 days. The GDPR inquiry is stored in the ITSM system.

All employees must have knowledge of current and relevant policies, guidelines and procedures. This is done through awareness and training of employees.

It is ensured that general policies, guidelines, procedures and security framework are generally updated when needed and at least once a year.

Compliance, roles and responsibilities

The responsibility for IT Security and Compliance is placed with top management. Top management has delegated the work of leading implementation, control and continuous improvement to the Compliance and Security department.

Compliance and Security updates employees on current relevant security threats and provides good advice on better IT security. The individual employee is responsible for complying with applicable policies and guidelines, seeking out and following applicable procedures and, in general, proactively relating to safety. Once a year or in the event of major changes, samples are taken by the security manager, who must show whether there is awareness of IT security.

Monitoring
Only authorised users have access to personal information, and the assigned user accesses are in accordance with work-related needs.

At least once a year, standard user accounts are reviewed, and for privileged users, quarterly audits are performed in User Management.

IT Relation's access to customer systems is logged. The log contains information about time, user, privileges and to which system connection has been made. The information is stored for a minimum of six months and is then deleted.

The following must be logged in connection with access to personal data:

- Login to the administration platform for access to customer systems
- Login to customer servers
- Login to selected systems and services that IT Relation provides.

Compliance and security runs audits on accesses based on samples. This is done at least twice a year.

Complementary controls at the data controllers

The data controllers have the following obligations:

- Ensure that the personal data are up to date
- Ensure the legality of instructions under the regulations in force at any time under privacy law
- Ensure that instructions in the data processing agreement is correct and contact IT Relation if changes are needed
- Ensure that the personal data types and categories of data subjects are correct in the data processing agreement
- Ensure that the data controller’s users are reviewed and have the correct access profile
- Perform risk analysis on the controllers’ data subjects
- Perform audit of their data processors (e.g. IT Relation)
- On an ongoing basis, review agreed safety measures and configurations for the customer's environment and ensure they are adequate.

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. 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. 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. 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. Checked by way of inspection of a sample of one personal data processing operation that the processing is conducted consistently with instructions.	No exceptions noted.
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	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. 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.	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. 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. Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of one data processing agreement 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. Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data. 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. Checked by way of inspection that the data processor has implemented the security measures agreed with the data controller.	No exceptions 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.	Checked by way of inspection that antivirus software has been installed for the systems and databases used in the processing of personal data. Checked by way of inspection that antivirus software is up to date.	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.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. Checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy.	No exceptions noted.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. Inspected network diagrams and other network documentation to ensure appropriate segmentation.	No exceptions noted.
B.6	Access to personal data is 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. 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. Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data. Checked by way of inspection of a sample of one user's access to systems and databases that such access is restricted to the employees' work-related need.	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.7	System monitoring with an alarm feature has been established for the systems and databases used in the processing of personal data. This monitoring comprises: • User logins • Critical settings of systems and databasses	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.	No exceptions noted.
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. Checked by way of inspection that technological encryption solutions are available and active. Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	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:
	• Activities performed by system administrators and others holding special rights
	• Security incidents comprising:
	  ○ Changes in log set-ups, including disabling of logging
	  ○ Changes in users' system rights
	  ○ Failed attempts to log on to systems, databases or networks
	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.
		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.
		Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.
		Checked by way of inspection of a sample of one day 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.
		Checked by way of inspection of a sample of one day of logging that documentation confirms the follow-up performed on activities carried by system administrators and others holding special rights.
			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.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. Checked by way of inspection of a sample of one development or test database that personal data included therein are pseudonymised or anonymised. Checked by way of inspection of a sample of one development or test database in which personal data are not pseudonymised or anonymised that this has taken place according to agreement with, and on behalf of, the data controller.	During our audit of procedures for deployment we have observed some type of data in test and deployment environment have not been anonymized. Phone numbers and e-mails are not being anpnymized when these data are moved from production environment to test and deploymet environment. We are aware of the fact that the test (deployment environment has the same high level of security as production environment. No further 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. Checked by way of inspection of one sample that documentation confirms regular testing of the technical measures established.	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.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. 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.	No exceptions noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	Checked by way of inspection that formalised procedures exist for granting and removing users' access to systems and databases used for processing personal data. Checked by way of inspection of a sample of one employee's access to systems and databases that the user accesses granted have been authorised and that a work-related need exists. Checked by way of inspection of a sample of one resigned or dismissed employee that the employee's access to systems and databases was deactivated or removed in a timely manner. Checked by way of inspection that documentation states that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	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.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. 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.
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. Checked by way of inspection of documentation that only authorised persons have 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. 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. 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. Checked by way of inspection of a sample of one data processing agreement that the requirements therein 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: • References from former employers • Certificates of criminal record • Diplomas.	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. Checked by way of inspection of a sample of one data processing agreement that the requirements therein for screening employees are covered by the data processor's screening procedures. Checked by way of inspection of one employee appointed during the assurance period that documentation exists of the screening having comprised: • References from former employers • Certificates of criminal record • Diplomas.	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 of one newly appointed employee that the employee has signed a confidentiality agreement. Checked by way of inspection of one newly appointed employee that the employee has been introduced to: • The information security policy • Procedures for processing data and other relevant information.	No exceptions noted.
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. Checked by way of inspection of one employee resigned or dismissed that rights have been deactivated or terminated and that assets have been returned.	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.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. Checked by way of inspection of one employee resigned or dismissed that documentation exists of 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. 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. 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. 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: • Data in the customer's systems and configurations in firewalls etc. will be deleted no earlier than 1 month after and no later than 3 months after the termination of the agreement. • Data about the customer in IT Relations' systems and where IT Relation is data responsible, will be deleted based on the current deletion deadline for the individual system.	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. Checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities that documentation states that personal data are stored in accordance with the agreed storage periods. Checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities that documentation states that personal data are deleted in accordance with the agreed deletion routines.	No exceptions noted.
D.3	Upon termination of the processing of personal data for the data controller, data 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.	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. Checked by way of inspection of one terminated data processing session that documentation states that the agreed deletion or return of data has taken place.	No exceptions noted.

Control objective E:

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

No.	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. 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. Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities 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. Checked by way of inspection of a sample of one data processing session from the data processor's list of processing activities 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. 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. 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. Checked by way of inspection of a sample of one subprocessor from the data processor's list of subprocessors that documentation states that the processing of data by the subprocessor follows from the data processing agreement – or otherwise as approved by the data controller.	No 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.	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. Checked by way of inspection of a sample of one subprocessing agreement that it includes the same requirements and obligations as are stipulated in the data processing agreement between the data controller and the data processor.	No exceptions noted.
F.5	The data processor has a list of approved subprocessors disclosing: • Name • Company registration no. • Address • Description of the processing.	Checked by way of inspection that the data processor has a complete and updated list of subprocessors used and approved. Checked by way of inspection that, as a minimum, the list includes the required details about each subprocessor.	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.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. Checked by way of inspection of documentation that each subprocessor and the current processing activity at such processor are subjected to risk assessment. 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. 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. 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. 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. Checked by way of inspection of a sample of one data transfer from the data processor's list of 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. Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of one data transfer from the data processor's list of 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. 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. 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: • Handing out data • Correcting data • Deleting data • Restricting the processing of personal data • Providing information about the processing of personal data to data subjects. 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. 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. 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: • Awareness of employees • Monitoring of network traffic • 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. 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. 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.
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than 72 hours after having become aware of such personal data breach at the data processor or a 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. Made inquiries as to whether personal data breaches have been identified at subprocessors and checked by way of inspection that these breaches are included in the list of security incidents.	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.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: • The 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.	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: • 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. 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.