DANSKE REVISORER FSR

FSR – Danish Auditors publishes auditor's assurance report on personal data in English

An English version of the newly published auditor's assurance report on personal data, which FSR – Danish Auditors prepared in collaboration with the Danish Data Protection Agency, is now available.

On 5 February 2019 FSR – Danish Auditors published a new auditor's assurance report on personal data. The assurance report was prepared in collaboration with the Danish Data Protection Agency. The purpose of the assurance report is to provide assurance that data processors comply with the requirements of GDPR, and the agreed terms in the data processing agreements.

FSR – Danish Auditors is now publishing an English version of the assurance report. The English version is a direct translation of the Danish version. As a result, the two versions have similar background, purpose, focus, and structure.

You can read more about the newly published auditor's assurance report on personal data in this link:
https://www.fsr.dk/Faglige_informationer/Om_revisor/Persondataforordningen/FSR%20lancerer%20paa%20baggrund%20af%20samarbejde%20med%20Datatilsynet%20ny%20erklaering%20om%20persondata

The English version of the assurance report aims to help companies with international business partners and customers, and where the primary communication in general is in English. The English version can also be used by companies that have international data processors and where communication between the parties is in English.

Similar to the Danish version, the English assurance report on personal data is not an expression of minimum requirements. The assurance report includes a variety of examples on control objectives and audit procedures. These are for inspiration only and should always be adjusted to meet the specific risk assessment, the arrangements, which have been agreed upon between the parties, and in consideration of the auditor's professional assessments.

We refer to next page for the auditor's assurance report

Contact details:
Thomas Krath Jørgensen
Chief Consultant, State Authorised Public Accountant
Email: tkj@fsr.dk
Phone: +45 4193 3148

[Data processor]

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with [Data controller]

Note: This assurance report template comprises a number of examples of control activities and audit procedures. These are for inspiration only and should always be adapted to the specific risk assessment, the measures as might otherwise have been arranged by the parties, and considering the auditor's professional judgement.

1 February 2019

Table of contents

1. Management's statement

[Data Processor] processes personal data for [Data Controller] in accordance with the data processing agreement [to be specified by date, version or similar information – e.g. data processing agreement for staff administration, version 2.3].

The accompanying description has been prepared for [Data Controller], who has used [identification of processing – e.g. staff administration in HC-System], and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with. [Data Processor] confirms that:

a) The accompanying description, pages [bb-cc], fairly presents [identification of processing – e.g. staff administration in HC-System], which has processed personal data for data controllers subject to the Regulation throughout the period from [date] to [date]. The criteria used in making this statement were that the accompanying description:

   (i) Presents how [identification of processing – e.g. staff administration in HC-System] 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;
   - Controls that we, in reference to the scope of [identification of processing – e.g. staff administration in HC-System], have assumed would be implemented by the data controllers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description;

- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data;

(ii) Includes relevant information about changes in the Data Processor's [identification of processing – e.g. staff administration in HC-System] in the processing of personal data in the period from [date] to [date];

(iii) Does not omit or distort information relevant to the scope of [identification of processing – e.g. staff administration in HC-System] 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 [identification of processing – e.g. staff administration in HC-System] that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from [date] to [date]. The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from [date] to [date].

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.

[Signature of Data Processor]

[Date of Data Processor's statement]

[Address of Data Processor]

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with [Data Controller]

To: [Data Processor] and [Data Controller]

Scope

We were engaged to provide assurance about [Data Processor]'s description on pages [bb-cc] of [identification of processing – e.g. staff administration in HC-System] in accordance with the data processing agreement with [Data Controller] throughout the period from [date] to [date] ("the Description") and about the design and operating effectiveness of controls related to the control objectives stated in the Description. We express reasonable assurance in our conclusion.

[Data Processor]'s responsibilities

[Data Processor] is responsible for: preparing the Description and the accompanying statement on page [aa], including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's independence and quality control

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

[Data Processor's auditor] 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 [Data Processor]'s Description and on the design and operating effectiveness of controls related to the control objectives stated in that Description, based on our procedures.

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

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

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

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

Opinion

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

(a) The Description fairly presents [identification of processing – e.g. staff administration in HC-System] as designed and implemented throughout the period from [date] to [date];

(b) The controls related to the control objectives stated in the Description were appropriately designed throughout the period from [date] to [date]; and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from [date] to [date].

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed on pages [yy-zz].

Intended users and purpose

This report and the description of tests of controls on pages [yy-zz] are intended only for data controllers who have used [Data Processor]'s [name of the system/service], who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with.

[Signature of Data Processor's auditor]

[Date of assurance report of Data Processor's auditor]

[Address of Data Processor's auditor]

3. Description of processing

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is: [Insert here a brief description of the underlying contract(s) between the parties which is the reason for the need to have a data processing agreement, preferably with references to "the master agreement", the data processing agreement and other relevant arrangements and the purpose and nature of such processing].

Nature of processing

The Data Processor's processing of personal data on behalf of the Data Controller primarily concerns [describe the nature of such processing].

Personal data

- Describe the type of personal data being processed [describe the specific data being processed under the data processing agreement]:
- General personal data, including identification data such as name and address or data on finances, taxes, debts, significant social problems, other private matters, sick days, job-related matters, family circumstances, housing, motor vehicle, degrees, applications, CV, date of employment and position, field of work and business phone.
- Special categories of personal data, including race and ethnic origin, political opinion, religion or beliefs, trade union membership, genetic data, biometric data for the unique identification of a natural person, data concerning health or sex life, or sexual orientation.
- Other personal data, including data on criminal offences and personal identification numbers.

Categories of data subjects falling within the data processing agreement:

- [E.g. employees]
- [E.g. clients]
- [E.g. customers]
- [E.g. children]

Practical measures

A description of the practical measures, including technical as well as organisational measures, that the data processor has implemented to ensure compliance with its obligations under the data processing agreement. The description may include a presentation of management systems established and implemented for information security and for processing personal data as well as a description of other measures initiated.

Risk assessment

A description of how the data processor has mapped the risk to the rights of data subjects, including a balancing of such risk against the precautions (e.g. control measures, see below) being taken to protect such rights.

The actual risk assessment consists of two parts, both of which should be described:

- Mapping of all of the risks involved in the processing and a classification of such risks (scoring, probability and severity);
- Assessing what constitute appropriate technical and organisational measures to ensure compliance with the Regulation and the documentability thereof.

In those special cases where a high risk entails that the data controller needs to perform an impact analysis regarding data protection, it must also be described how the data processor may have assisted in this respect.

Control measures

A description of the control measures initiated and implemented by the data processor to measure and test the effectiveness of the management system established for information security and for processing personal data as well as performance measurement thereof.

Also refer to section 4 for a description of the specific control activities.

Complementary controls at the data controllers

[Insert here a description of the controls that are assumed to have been implemented at the data controllers and that are material in achieving the control objectives stated in the description.]

The data controllers have the following obligations:

- [E.g.: To ensure that the personal data are up to date]
- [E.g.: To ensure the legality of instructions under the regulations in force at any time under privacy law]
- [E.g.: That instructions are appropriate with respect to this data processing agreement and the principal service]
- [E.g.: To ensure that the data controller's users are up to date]
- xx

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*	*Test performed by auditor*	*Result of auditor'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.	Checked by way of inspection that formalised procedures exist 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.	
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 XX personal data processing operations that these are conducted consistently with instructions.	

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*	*Test performed by auditor*	*Result of auditor's test*
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 exist ensuring verification that personal data are not processed against the 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 evaluated to be against legislation. Checked by way of inspection that the data controller was informed in cases where the processing of personal data was evaluated to be against legislation.	

Control objective B **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*	*Test performed by auditor*	*Result of auditor'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.	Checked by way of inspection that formalised procedures exist to ensure establishment of the safeguards agreed. Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of XX data processing agreements that the safeguards agreed have been established.	
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 safeguards 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.	

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*	*Test performed by auditor*	*Result of auditor's test*
		Checked by way of inspection that the data processor has implemented the safeguards agreed with the data controller.	
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, for the systems and databases used in the processing of personal data, antivirus software has been installed. Checked by way of inspection that antivirus software is up to date.	
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	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.	
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.	

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*	*Test performed by auditor*	*Result of auditor's test*
		Inspected network diagrams and other network documentation to ensure appropriate segmentation.	
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 XX users' access to systems and databases that such access is restricted to the employees' work-related need.	
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. This monitoring comprises: • XX	Checked by way of inspection that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	

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*	*Test performed by auditor*	*Result of auditor's test*
	• XX • XX	Checked by way of inspection that, in a sample of XX alarms, these were followed up on and that the data controllers were informed thereof as appropriate.	
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 have been available and active throughout the assurance period. Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email. Inquired whether any unencrypted transmission of sensitive and confidential personal data has taken place during the assurance period and whether the data controllers have been appropriately informed thereof.	

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*	*Test performed by auditor*	*Result of auditor's test*

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 setups, including disabling of logging;
	  ○ Changes in users' system rights;
	  ○ Failed attempts to log on to systems, databases or networks;
	  ○ XX.
	
	Logon data are protected against manipulation and technical errors and are reviewed regularly.
		Checked by way of inspection that formalised procedures exist for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs.
		
		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 XX days of logging that the content of log files is as expected compared to the setup and that documentation exists regarding the follow-up performed and the response to any security incidents.
		
		Checked by way of inspection of a sample of XX days of logging that documentation exists regarding the follow-up performed for activities carried by system administrators and others holding special rights.	

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*	*Test performed by auditor*	*Result of auditor's test*
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 exist 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 XX development or test databases that personal data included therein are pseudonymised or anonymised. Checked by way of inspection of a sample of XX development or test databases 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.	
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 exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests. Checked by way of inspection of samples that documentation exists regarding regular testing of the technical measures established. Checked by way of inspection that any deviations or weaknesses in the technical measures have	

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*	*Test performed by auditor*	*Result of auditor's test*
		been responded to in a timely and satisfactory manner and communicated to the data controllers as appropriate.	
B.12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	Checked by way of inspection that formalised procedures exist 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 setups that systems, databases or networks have been updated using agreed changes and relevant updates, patches and security patches.	
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 using to process personal data. Checked by way of inspection of a sample of XX employees' access to systems and databases that the user accesses granted have been authorised and that a work-related need exists.	

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*	*Test performed by auditor*	*Result of auditor's test*
		Checked by way of inspection of a sample of XX resigned or dismissed employees that their access to systems and databases was deactivated or removed on a timely basis. Checked by way of inspection that documentation exists that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	Checked by way of inspection that formalised procedures exist to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects. 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.	
B.15	Physical access safeguards have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	Checked by way of inspection that formalised procedures exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed.	

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*	*Test performed by auditor*	*Result of auditor's test*
		Checked by way of inspection of documentation that, throughout the assurance period, only authorised persons have had physical access to premises and data centres at which personal data are stored and processed.	

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*	*Test performed by auditor*	*Result of auditor's test*
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 IT 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 IT security policy should be updated.	Checked by way of inspection that an information security policy exists that Management has considered and approved within the past year. Checked by way of inspection of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	
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 safeguards and the security of processing in the data processing agreements entered into. Checked by way of inspection of a sample of XX data processing agreements that the requirements in these agreements are covered by the requirements of the information security policy for safeguards and security of processing.	
C.3	The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant:	Checked by way of inspection that formalised procedures are in place to ensure screening of	

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*	*Test performed by auditor*	*Result of auditor's test*
	• References from former employers; • Certificates of criminal record; • Diplomas; • Xx.	the data processor's employees as part of the employment process. Checked by way of inspection of a sample of XX data processing agreements that the requirements therein for screening employees are covered by the data processor's screening procedures. Checked by way of inspection of XX employees appointed during the assurance period that documentation exists of the screening having comprised: • References from former employers; • Certificates of criminal record; • Diplomas; • Xx.	
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 XX employees appointed during the assurance period that the relevant employees have signed a confidentiality agreement.	

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*	*Test performed by auditor*	*Result of auditor's test*
		Checked by way of inspection of XX employees appointed during the assurance period that the relevant employees have been introduced to: • Information security policy; • Procedures for processing data and other relevant information.	
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 XX employees resigned or dismissed during the assurance period that rights have been deactivated or terminated and that assets have been returned.	
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 exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality.	

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*	*Test performed by auditor*	*Result of auditor's test*
		Checked by way of inspection of XX employees resigned or dismissed during the assurance period that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality.	
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 that all employees who have either access to or process personal data have completed the awareness training provided.	

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*	*Test performed by auditor*	*Result of auditor'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.	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 the procedures are up to date.	
D.2	The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines: • [Insert description of specific requirements]	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 XX data processing sessions from the data processor's list of processing activities that documentation exists that personal data are stored in accordance with the agreed storage periods. Checked by way of inspection of a sample of XX data processing sessions from the data processor's list of processing activities that documentation exists that personal data are deleted in accordance with the agreed deletion routines.	

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*	*Test performed by auditor*	*Result of auditor's test*
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 XX terminated data processing sessions during the assurance period that documentation exists that the agreed deletion or return of data has taken place.	

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*	*Test performed by auditor*	*Result of auditor'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.	Checked by way of inspection that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. Checked by way of inspection that the procedures are up to date. Checked by way of inspection of a sample of XX data processing sessions from the data processor's list of processing activities that documentation exists that data processing takes place in accordance with the data processing agreement.	
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 XX data processing sessions from the data processor's list of processing activities that documentation exists that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller.	

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.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
F.1	Written procedures exist which include requirements for the data processor 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.	Checked by way of inspection that formalised procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions. Checked by way of inspection that procedures are up to date.	
F.2	The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.	Checked by way of inspection that the data processor has a complete and updated list of sub-data processors used. Checked by way of inspection of a sample of XX sub-data processors from the data processor's list of sub-data processors that documentation exists that the processing of data by the sub-data processor is stated in the data processing agreements – or otherwise as approved by the data controller.	
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	Checked by way of inspection that formalised procedures are in place for informing the data	

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.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
	from the data processor. When changing the specially approved sub-data processors used, this has been approved by the data controller.	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.	
F.4	The data processor has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	Checked by way of inspection for existence of signed sub-data processing agreements with sub-data processors used, which are stated on the data processor's list. Checked by way of inspection of a sample of XX 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.	
F.5	The data processor has a list of approved sub-data processors disclosing: • Name; • Business Registration No.; • Address; • Description of the processing.	Checked by way of inspection that the data processor has a complete and updated list of sub-data processors used and approved.	

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.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
		Checked by way of inspection that, as a minimum, the list includes the required details about each sub-data processor.	
F.6	Based on an updated risk assessment of each sub-data processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-data processor.	Checked by way of inspection that formalised procedures are in place for following up on processing activities at sub-data processors and compliance with the sub-data processing agreements. Checked by way of inspection of documentation that each sub-data processor and the current processing activity at such processor are subjected to risk assessment. Checked by way of inspection of documentation that technical and organisational measures, security of processing at the sub-data processors used, third countries' bases of transfer and similar matters are appropriately followed up on. Checked by way of inspection of documentation that information on the follow-up at sub-data	

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.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
		processors is communicated to the data controller so that such controller may plan an inspection.	

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*	*Test performed by auditor*	*Result of auditor's test*
G.1	Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. 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 exist 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.	
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 XX data transfers from the data processor's list of transfers that documentation exists that such transfers were arranged with the data controller in the data processing agreement or subsequently approved.	
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.	

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*	*Test performed by auditor*	*Result of auditor's test*
		Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of XX data transfers from the data processor's list of transfers that documentation exists of a valid basis of transfer in the data processing agreement with the data controller and that transfers have only taken place in so far as this was arranged with the data controller.	

Control objective H **Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting or restricting information on the processing of personal data to the data subject.**			
No.	*Data processor's control activity*	*Test performed by auditor*	*Result of auditor's test*
H.1	Written procedures exist 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.	
H.2	The data processor has established procedures in so far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects.	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. *OR IF ASSISTANCE HAS BEEN PROVIDED DURING THE PERIOD*	

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*	*Test performed by auditor*	*Result of auditor's test*
		Checked by way of inspection 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.	

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*	*Test performed by auditor*	*Result of auditor's test*
I.1	Written procedures exist 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.	
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; • Xx.	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 on a timely basis. Checked by way of inspection of documentation that xx	

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*	*Test performed by auditor*	*Result of auditor's test*
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than XX hours after having become aware of such personal data breach at the data processor or a sub-data processor.	Checked by way of inspection that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach. Made inquiries of the sub-data processors as to whether they have identified any personal data breaches throughout the assurance period. Checked by way of inspection that the data processor has included any personal data breaches at sub-data processors in the data processor's list of security incidents. Checked by way of inspection that all personal data breaches recorded at the data processor or the sub-data processors have been communicated to the data controllers concerned without undue delay and no later than XX hours after the data processor became aware of the personal data breach.	
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency: • Nature of the personal data breach;	Checked by way of inspection that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for:	

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*	*Test performed by auditor*	*Result of auditor's test*
	• Probable consequences of the personal data breach; • Measures taken or proposed to be taken to respond to the personal data breach.	• 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. *OR IF BREACHES OCCURRED DURING THE PERIOD* Checked by way of inspection of documentation that, when a personal data breach occurred, measures were taken to respond to such breach.	