www.pwc.dk

The following is a translation of a Danish original document. Please note that the English translation is provided for convenience only. In case of any discrepancy, the Danish version shall prevail.

Tier 1 Asset A/S

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 March 2023 to 29 February 2024 pursuant to the data processing agreement and standard service level agreement with customers regarding the data erasure services.

June 2024

pwc

Contents

1. Management's statement

Tier1 Asset A/S (hereafter T1A) processes personal data on behalf of data controllers (customers) in accordance with the data processing agreement and standard service level agreement with customers.

The accompanying description has been prepared for data controllers (customers) who has used T1A's data erasure services and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU regulation on the "Protection of natural persons with regard to the processing of personal data and on the free movement of such data" and "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (subsequently "the data protection rules") have been complied with.

Depending on the agreement with customers, T1A either uses its own freight trucks or external haulers as sub-suppliers for transporting equipment from data controllers to T1A's address. This report uses the carve-out method and does not comprise control objectives and related controls that external haulers perform for T1A.

Some of the control objectives stated in our description in section 3 can only be achieved if the complementary controls at data controller are suitably designed and operating effectively with our controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

T1A confirms that:

a) The accompanying description in section 3 fairly presents information security and measures in relation to T1A's data erasure services that has processed personal data for data controllers subject to the data protection rules throughout the period from 1 March 2023 to 29 February 2024. The criteria used in making this statement were that the accompanying description:

   (i) Presents how information security and measures in relation to T1A's data erasure services was designed and implemented, including:

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

- Controls that we, in reference to the scope of scope of T1A's data erasure services, have assumed would be implemented by the data controllers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description;

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

(ii) Includes relevant information about changes in T1A's data erasure services in the the erasure services in the processing of personal data in the period from 1 Marts 2023 to 29 February 2024;

(iii) Does not omit or distort information relevant to the scope of T1A's data erasure 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 of T1A's data erasure services that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 March 2023 to 29 February 2024. The criteria used in making this statement were that:

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

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

(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 from1 March 2023 to 29 February 2024.

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

Allerød, 20 June 2024
Tier 1 Asset A/S

Peter Hemicke
CEO

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 March 2023 to 29 February 2024 pursuant to the data processing agreement and standard service level agreement with customers regarding data erasure services.

To: T1A and data controllers that have used T1A's data erasure services

Scope

We have been engaged to provide assurance about T1A's description in section 3 of T1A's data erasure services in accordance with the data processing agreement and standard service level agreement with customers throughout the period from 1 March 2023 to 29 February 2024 (the description) and about the design and operating effectiveness of controls related to the control objectives stated in the description.

Our report covers whether T1A has designed and effectively operated suitable controls related to the control objectives stated in section 4. The report does not include an assessment of T1A'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").

Depending on the agreement with clients, T1A either uses its own freight trucks or external haulers as subsuppliers for transporting equipment from data controllers to T1A's address. This report uses the carve-out method and does not comprise control objectives and related controls that external haulers perform for T1A.

Some of the control objectives stated in T1A's description in section 3 can only be achieved if the complementary controls at data controller are suitably designed and operating effectively. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

We express reasonable assurance in our conclusion.

T1A's responsibilities

T1A is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing and effectively operating controls to achieve the stated control objectives.

Auditor's independence and quality control

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

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

Auditor's responsibilities

Our responsibility is to express an opinion on T1A's description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3000 (revised), "Assurance engagements other than audits or reviews of historical financial information", and additional requirements applicable in Denmark to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of T1A's data erasure services and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified by the data processor and described in the Management's statement section.

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

Limitations of controls at a data processor

T1A's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of T1A's data erasure 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. 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 information security and measures in relation to T1A 's data erasure services as designed and implemented throughout the period from 1 March 2023 to 29 February 2024.

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 March 2023 to 29 February 2024; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 March 2023 to 29 February 2024.

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 T1A's data erasure services and who have a sufficient understanding to consider it, along with other information, including information about controls operated by the data controllers themselves, in assessing whether the requirements of the data protection rules have been complied with.

Copenhagen, 20 June 2024
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Michael Clement
State-Authorised Public Accountant
mne23410

3. Description of processing

The purpose of the data processor's processing of personal data on behalf of the data controller is as follows:

- T1A will comply with every legal demand. We will also respect and comply with any further specific demands and conditions that could be contained in e.g. client agreements and contracts.
- The company's strategies and guidelines must support this obligation to leadership regarding quality conditions, environmental conditions and information security.
- All employees and contractors at T1A must follow this policy and report conditions regarding processes, products and services that could negatively affect quality, environment, health, safety and information security to the management of T1A. Corrective action must be taken immediately.
- The management will provide the necessary resources to achieve the objectives for this company policy.

Nature of processing

The data processor's processing of personal data on behalf of the data controller primarily concerns company data that needs to be erased.

Personal data

Data processing primarily includes erasure of data from the data controller's IT units. It may contain the following data:

- Confidential company data
- Personal data on devices related to employees at data controller
- Emails sent from data controllers personnel to other companies
- Various documents saved by data controllers personnel

Categories of data subjects falling within the data processing agreement:

- Clients

Practical measures

T1A has implemented the R2v3 as well as ISO 27001 standard and complies with the principles along with the control elements of a series of organisational and technical safety measures. These will help ensure that T1A complies with the GDPR regulation and the Danish Data Protection Act.

As data processor T1A ensures that the data erasure complies with the most up-to-date standard, at least NIST 800-88, equivalent or higher, unless other method is requested and instructed by the data controller.

Risk assessment

T1A must carefully identify and assess the extent of all types of risks and opportunities applicable to the organisation.

To uncover risks and opportunities, the following forms are used:

- B 612.1.1 Identification of environmental risk

- B 612.1.2 Identification of information security risks
- B 612.1.3 Identification of occupatonial health and safety risks
- B 612.1.4 Identification of quality risks.
- B 612.1.5 Identification of bribery risks.
- B 613.1.1 SOA – Statement of Applicability (ISO 27001)

Updating of the risk assessments is done continuously and at least annually reassessed as part ofthe company's Committee meetings. The company has four functioning committees:

- IT and information security committee
- R2v3 committee
- Compliance committee
- Occupational Health and Safety committee

All the company's committees support the Management's review and oversight of the effectiveness of the management system.

The company's risks are identified, understood, prioritised and handled as describedthe above-mentioned forms.

When the forms are filled in:

The coverage, scope and applicability of risks and opportunities in the management system for the company and its stakeholders is outlined in P 410 Context and stakeholders of the organisation as well as P 430 Determining the scope of the management system.

Risks are identified, analysed, evaluated and assessed and prioritised incl. the company's risk response

Control measures

T1A will strive to continuously improve our IT and information security as well as our information security management system certified against the requirements of the ISO 27001:2013 standard "Information technology - Security techniques – Information security management systems - Requirements" and Responsible Recycling Version 3 (R2v3).

T1A establishes the objectives for the information security. The objectives are fulfilled by the monitoring of the management system in place with oversight of the committees and the management team.

The effectiveness of the management system and the management's oversight hereof is verified through extensive internal and external audits.

The management system also covers maintenance of a legal compliance plan, where changes in legal requirements and special risks are managed.

T1A will:

- Ensure confidential processing, transmission and storage of data
- Ensure that data and information are only used by individuals with a legal right to do so
- Ensure efficient access management so that unauthorised individuals cannot directly access data and systems to the detriment of T1A, our customers, employees and partners
- Ensure that attempts at infringement or breach of security measures are detected as far as possible and that the activity can be traced back to the individual(s) involved
- Ensure that the information security is continuously adapted and improved to the change in context and environment

T1A has its own freight trucks with attached boxes, own drivers and GPS tracking. There is 24-hour surveillance of T1A's own freight trucks. In addition, T1A uses external haulers for shipping IT units from clients to T1A 's address for further processing. Haulers are not considered as subprocessors, but T1A has entered into common business to business agreements with these regarding safe transport of the IT units.

There have not been any material changes in the period.

Reference is also made to section 4, where the specific control objectives and control activities are described.

Control activities in relation to the standard template from FSR-Danske Revisorer and the Danish Data Protection Agency that are not included in section 4 of the declaration

All data transport from the data controller to T1A takes place physically which is why B.8 of the declaration regarding encryption is absent. The client is responsible for ensuring that the data on the received IT units etc. are encrypted. Furthermore, there is no personal data in development and test which is why B.10 is also absent. Likewise, we have assessed that B.11 regarding vulnerability scans and penetration tests, and B.14 regarding use of two-factor authentication, area E regarding storage of data and area G regarding transfer of data to third countries are not relevant to the service provided by T1A. Finally, we are not responsible for providing, correcting and deleting data for data subjects. Area H is consequently not included in the report

No.	Data processor's control activity
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.
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.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration 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.
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.

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
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.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller
G.3	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller
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
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.

Complementary controls at the data controllers

T1A has implemented a series of safety precautions through our quality management system and is using all the standards of ISO 27001 and R2v3 to ensure and maintain the high level of data security.

The data controllers have the following obligations:

- To ensure that the instructions are appropriate with respect to this data processing agreement and the main service.
- To ensure that data on IT units are encrypted before T1A receives the IT units.

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 in accordance 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 personal data processing operations that these are conducted consistently with instructions.	No exceptions noted.

Control objective A:

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

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

Control objective B:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
B.1	Written procedures are in place which include a requirement that security measures agreed are established for the processing of personal data in accordance with the agreement with the data controller. 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 data processing agreements that the security measures agreed have been established.	No exceptions noted.
B.2	The data processor has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the security measures agreed with the data controller.	Checked by way of inspection that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. 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.
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.	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
		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. 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 users' access to systems and databases that such access is restricted to the employees' work-related need.	No exceptions noted.
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: • Use of key chip for production areas with ongoing random control of physical access logs to production and the office.	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. Checked by way of inspection that, in a sample of alarms, these were followed up on and that the data controllers were informed thereof as appropriate.	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

	• Processing of received IT equipment, including:
	  ○ Scanning and evaluation of received IT equipment
	  ○ Implementation of data deletion		

B.9	Logging of the following matters has been established in production areas:
	• Use of key chip for production areas
	• Processing of received IT equipment, including:
	  ○ Scanning and evaluation of received IT equipment
	  ○ Implementation of data deletion
	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 production areas 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 days of logging that the content of log files is as expected compared to the set-up and that documentation confirms the follow-up performed and the response to any security incidents.
		Checked by way of inspection of a sample of days of logging that documentation confirms the follow-up performed on activities carried out 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.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.	We have been informed that there have been no changes to systems, databases or networks in the reporting period, which is why it has not been possible to test the effectiveness of the control. 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 are in place for granting and removing users' access to systems and databases used for processing personal data. Checked by way of inspection of a sample of employees' access to systems and databases that the user accesses granted have been authorised and that a work-related need exists. Checked by way of inspection of a sample of resigned or dismissed employees that their 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.
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.	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
		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	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 data processing agreements that the requirements in these agreements are covered by the requirements of the information security policy for security measures and security of processing.	No exceptions noted.

Control objective C:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
C.3	The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant: • Where relevant references from previous employment • Certificates of criminal record	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 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 employees appointed during the assurance period that documentation states that the screening has comprised: • Where relevant references from previous employment • Certificates of criminal record	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 employees appointed during the assurance period that the relevant employees have signed a confidentiality agreement. Checked by way of inspection of employees appointed during the assurance period that the relevant employees have been introduced to: • The information security policy • Procedures for processing data and other relevant information.	No exceptions noted.

Control objective C:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	Inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned. Checked by way of inspection of employees resigned or dismissed during the assurance period that rights have been deactivated or terminated and that assets have been returned.	No exceptions noted.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	Checked by way of inspection that formalised procedures are in place to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. Checked by way of inspection of employees resigned or dismissed during the assurance period that documentation confirms the continued validity of the confidentiality agreement and the general duty of confidentiality.	No exceptions noted.
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	Checked by way of inspection that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data. 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: • Received data-bearing IT equipment is stored at T1A's locations during processing. • Received data-bearing IT equipment is deleted after receipt.	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 data processing sessions from the data processor's list of processing activities that documentation states that personal data are stored in accordance with the agreed storage periods. Checked by way of inspection of a sample of data processing sessions from the data processor's list of processing activities that documentation states that personal data are deleted in accordance with the agreed deletion routines.	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 terminated data processing sessions during the assurance period that documentation states that the agreed deletion or return of data has taken place.	We have observed that no data processing agreements have terminated during the reporting period, which is why we have not been able to test the effectiveness of the procedure. 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.4	Data sanitization (erasure) of data storage media is done, at least in accordance with NIST Guidelines for Media Sanitization: Special Publication 800-88, equivalent or higher, unless other method is requested and instructed by the data controller. A data erasure certificate will be generated containing the following information: • Serial # of the device, where data is erased • Date and time for erasure • Applied data erasure method (e.g. NIST 800-88) • Name on technician who performed the data erasure • Verification that all data is erased in accordance with applied data erasure method	Checked by way of inspection of samples of data erasure certificates, that data sanitization (erasure) is done in accordance with instructions from the data controller. If not otherwise specified, at least in accordance with NIST Guidelines for Media Sanitization: Special Publication 800-88, equivalent or higher.	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 subprocessors from the data processor's list of subprocessors that documentation states that the processing of data by the subprocessor follows from the data processing agreements – or otherwise as approved by the data controller.	We have been informed that T1A does not use subprocessors for processing of personal data 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. Inspected documentation stating that the data controller was informed when changing the subprocessors used throughout the assurance period.	No exceptions noted.

Control objective F:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
F.4	The data processor has subjected the subprocessor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	Checked by way of inspection for existence of signed subprocessing agreements with subprocessors used, which are stated on the data processor's list. Checked by way of inspection of a sample of subprocessing agreements that they include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.	No exceptions noted.
F.5	The data processor has a list of approved subprocessors disclosing: • Name • Company registration no.	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.
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 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 • Logging of physical access to production areas • Registration and tracking of received IT equipment during processing	Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches. Inspected documentation that only authorized persons have physical access to premises and production areas in which personal data is stored and processed. Inspected that there is registration and tracking of received IT equipment during its processing and possibly data deletion	No exceptions noted.

Control objective I:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay have 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 of the subprocessors 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 subprocessors 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 subprocessors have been communicated to the data controllers concerned without undue delay after the data processor became aware of the personal data breach.	We have not been able to test the effectiveness of the procedure, as there have been no recorded security incidents involving personal data breaches during the reporting period No exceptions noted.
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency. These procedures must contain instructions on descriptions of: • 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.	We have not been able to test the effectiveness of the procedure, as there have been no recorded security incidents involving personal data breaches during the reporting period No exceptions noted.