www.pwc.dk

Trifork Security A/S

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 March 2024 to 31 December 2024 pursuant to the data processing agreement with customers

February 2025

Contents

1. Management's statement

Trifork Security A/S (Trifork Security) processes personal data on behalf of customers (data controllers) in accordance with data processing agreements.

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

Trifork Security uses Netic A/S as subprocessor for HR services. This report uses the inclusive method and comprises controls related to HR services that Netic A/S performs for Trifork Security.

Trifork Security uses Netic A/S as subprocessor for its hosting and backup services and CrowdStrike Inc. as subprocessor for its cybersecurity services. This report uses the carve-out method and does not comprise control objectives and related controls related to these services that Netic A/S and CrowdStrike Inc. perform for Trifork Security.

Some of the control objectives stated in our description in section 3 can only be achieved if the complementary controls at customers 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.

Trifork Security confirms that:

a) The accompanying description in section 3 fairly presents Trifork Security's Managed Security and Observability services that have processed personal data for data controllers subject to the data protection rules throughout the period from 1 March 2024 to 31 December 2024. The criteria used in making this statement were that the accompanying description:

   (i) Presents how Trifork Security's Managed Security and Observability services were designed and implemented, including:

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

- The procedures ensuring appropriate technical and organisational security measures in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

- Controls that we, in reference to the scope of Trifork Security's security and observability 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 the data processor's Managed Security and Observability services in the processing of personal data in the period from 1 March 2024 to 31 December 2024;

(iii) Does not omit or distort information relevant to the scope of Trifork Security's Managed Security and Observability 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 Trifork Security's Managed Security and Observability 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 2024 to 31 December 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 from 1 March 2024 to 31 December 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.

Aalborg, 24 February 2025
Trifork Security A/S

Mads Vigh
CEO

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 March 2024 to 31 December 2024 pursuant to the data processing agreement with customers

To: Trifork Security and Trifork Security's customers

Scope

We have been engaged to provide assurance about Trifork Security's and Netic A/S's description in section 3 of Trifork Security's Managed Security and Observability services in accordance with the data processing agreement with customers throughout he period from 1 March 2024 to 31 December 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 Trifork Security has designed and effectively operated suitable controls related to the control objectives stated in section 4. The report does not include an assessment of Trifork Security'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").

Trifork Security uses Netic A/S as subprocessor for HR services. This report uses the inclusive method and comprises controls related to HR services that Netic A/S performs for Trifork Security.

Trifork Security uses Netic A/S as subprocessor for its hosting and backup services and CrowdStrike Inc. as subprocessor for its cybersecurity services. This report uses the carve-out method and does not comprise control objectives and related controls related to these services that Netic A/S and CrowdStrike Inc. perform for Trifork Security.

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

We express reasonable assurance in our conclusion.

Trifork Security's responsibilities

Trifork Security 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 Trifork Security's description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

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

An assurance engagement to report on the description,design and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its Managed Security and Observability 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

Trifork Security's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of their Managed Security and Observability 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 Trifork Security's Managed Security and Observability services as designed and implemented throughout the period from 1 March 2024 to 31 December 2024; and

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 March 2024 to 31 December 2024

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 2024 to 31 December 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 Trifork Security's Managed Security and Observability services and who have a sufficient understanding to consider it, along with other information, including information about controls operated by the data controllers themselves, in assessing whether the requirements of the data protection rules have been complied with.

Aarhus, 24 February 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Rico Lundager
Senior Manager

3. Description of processing

Introduction

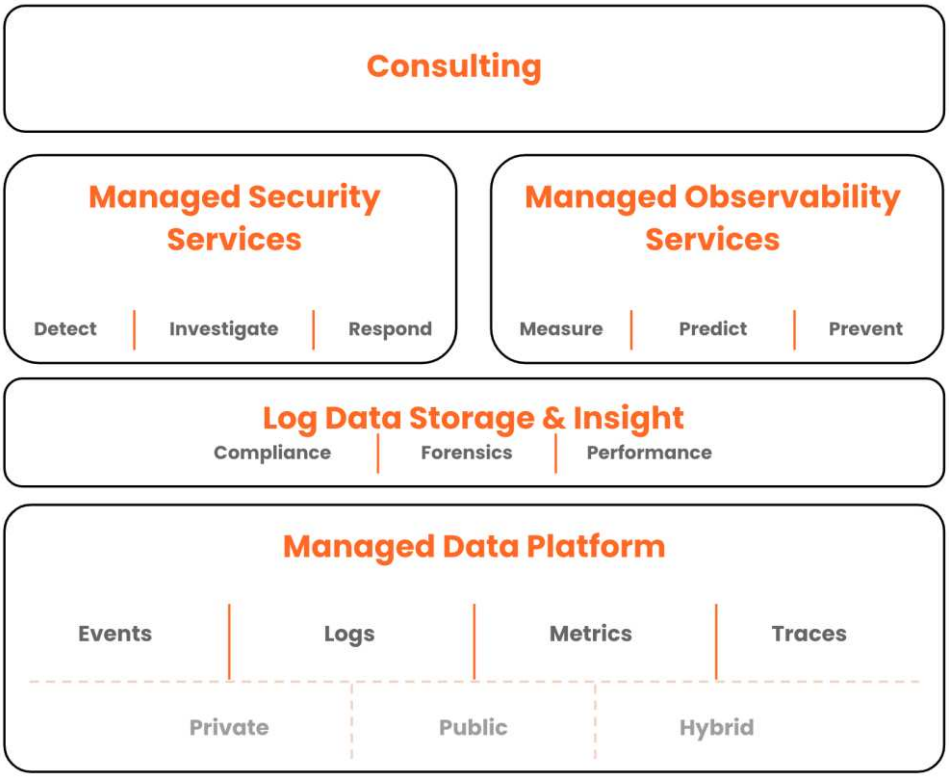
Trifork Security is a Danish company with more than 20 years of IT experience. Our goal is to solve the key challenges for public and private organisations focusing on cybersecurity, data management and observability, decreasing threats by doing our core services while increasing awareness on regulatory and compliance requirements.

In close collaboration with our originator Netic A/S, which consists of more than 150 IT operations specialists and which has extensive experience in secure and stable IT operations, we operate and secure some of the most critical infrastructure in Denmark.

Trifork Security has a diverse and dedicated team of around 50 consultants that provide managed and consulting services within operations, data observability and cybersecurity, all located in Denmark.

Description of services

Trifork Security is a supplier within managed services including managed EDR, 24/7 SOC and log management:



- Managed Security Services covering leading SIEM and EDR solutions is operated and monitored 24/7 by our Danish-based SOC and supported 24/7 by senior experts to handle major security incidents
- Managed Observability Services is mainly support and consulting covering implementation, operation and utilisation of business use cases
- Log Data Storage covers the discipline of ensuring the right data sources, data maintenance and retention times to support compliance, security use cases and observability data

- Managed Data Platform is the 24/7 operation of the actual platform optimising capacity and performance.

In addition to the managed services, we provide consultancy services, covering cybersecurity, observability, strategy, compliance, governance and assessments relating to the maturity of a customer.

This assurance report only covers these services: Managed Security Services and Managed Observability Services.

Nature of processing

The data processor's processing of personal data on behalf of the data controller primarily concerns collecting, analysing, monitoring, handling and storing operational and security logs.

Personal data

The processing will typically deal with data of a technical nature relating to operational monitoring or potential or confirmed security incidents. This can be logs from applications, operating systems, operational security tools and network equipment in which, for example, the following general personal data are processed:

- Name
- Address
- Gender
- Information about education and course certificates
- Nationality
- Login information
- Phone number
- IP address
- Mail address
- Job-related matters
- Active Directive Objectives
- All telemetry from endpoints.

The following special categories of personal data are also processed:

- Sensitive personal data: Race and ethnic origin, political beliefs, religious or philosophical beliefs, trade union affiliations, genetic data, biometric data for the purpose of unique identification, health information, sexual relationships or sexual orientation.

Other types of personal data are also processed:

- Social security number.

Categories of data subjects falling within the data processing agreement:

- Employees
- Employees' relations
- Former employees
- Customers
- Business or organisation partners and stakeholders
- Suppliers and other affiliates
- Users.

Control environment

Trifork Security is committed to maintaining a robust control environment that prioritises integrity, ethical values and a commitment to competence. This commitment is embedded in our company culture and is reinforced by a comprehensive framework of policies, procedures and practices. Our dedication to information security is demonstrated by our ISO 27001 certification, which ensures we have implemented internationally recognised best practices for managing and protecting sensitive information. Furthermore, we are dedicated to achieving and maintaining compliance with the NIS2 Directive, further solidifying our commitment to cybersecurity at all levels.

Management commitment:

- Our senior management team actively promotes a culture of ethical conduct, compliance with laws and regulations (including NIS2) and the importance of effective internal controls
- We have a code of conduct that clearly articulates our ethical principles and expectations for all employees
- Management and all employees receive regular communication and security training reinforcing the importance of these principles and providing guidance on ethical decision-making and compliance with relevant regulations
- Management is committed to attracting, developing and retaining competent individuals, and provides ongoing training and development to ensure the necessary skills and knowledge to perform their duties effectively.

Data processing compliance:

- We have implemented specific controls to ensure compliance with the data processing agreements
- This includes measures to ensure the confidentiality, integrity and availability of personal data, aligned with our ISO 27001 framework and NIS2 requirements
- We have established procedures for data subject requests, data breach notification and data retention.

Human resources practices:

- Our human resources practices are designed to support a strong control environment
- We conduct performance evaluations to assess employee performance and identify areas for improvement
- We have a whistleblower hotline that allows employees to report concerns confidentially without fear of retaliation.

Information security (ISO 27001 certified):

- We have implemented a comprehensive information security management system (ISMS) in accordance with ISO 27001 standards. This certification demonstrates our commitment to maintaining the confidentiality, integrity and availability of information.
- Our ISMS includes a wide range of controls, including:
    - Technical measures: Firewalls, intrusion detection systems, access controls, encryption and data loss prevention tools

  - Organisational measures: Data classification policies, data backup procedures, incident response plans, well-defined organisational structure with clear lines of authority and responsibility and regular security awareness training for all employees
  - Physical security measures: Access controls to our facilities and secure data centres.
- Our ISO 27001 framework serves as a strong foundation for meeting the technical and organisational security requirements of NIS2.

Monitoring and continuous improvement:

- We regularly monitor the effectiveness of our control environment through internal audits, management reviews and other monitoring activities, including regular reviews of our ISO 27001 compliance and progress towards NIS2 compliance
- We have a process for identifying and addressing non-conformities and opportunity for improvements and implementing corrective actions
- We are committed to continuous improvement and regularly review our control environment to ensure it remains effective and aligned with our business objectives and regulatory requirements.

Subprocessor organisations

Netic A/S supports and provides a range of services to Trifork Security.

Netic A/S provides the following services:

- HR and administration services to Trifork Security, HR advisory and handling of employee contracts, obtaining criminal records and verifying them
- Facility services like housing, physical security incl. access control, alarms and video surveillance
- Financial administration like bookkeeping, invoicing etc.
- Legal services like legal advisory in regard to current or new legislation and matters relating to customers, vendors, employees, etc.
- IT and hosting services like data centres, server housing, storage, backup and core and office network.

CrowdStrike is our endpoint security provider. Their Falcon platform provides us with advanced threat protection and helps us comply with applicable security standards. The platform is integrated into our existing IT infrastructure, and we have a DPA with CrowdStrike that ensures GDPR compliance.

Incorporation of subservice organisation

For the part of HR services that are outsourced to Netic A/S, we have tested the following related controls at Netic A/S: C.3, C.4 and C.6.

Risk management

Trifork Security has a systematic approach to risk management, where we have established a methodology and procedure regarding risk management. Multiple times a year, risk workshops are held, and in the assessments of the risks both senior management and employees with technical knowledge and experience are involved.

During the quarterly Information Security Board (ISB) meetings, where senior management and a representative from the Governance, Risk and Compliance (GRC) team participate, the biggest risks and their

possible treatments are discussed. This ensures that senior management is kept informed, while also discussing and agreeing on treatments of the risks.

Risk management is a focus area at Trifork Security. Therefore, one of the objectives in our ISMS is Risk Identification & Assessment, supporting our continuous focus and work with risk management.

Control objectives and control activities

As an ISO/IEC 27001:2022 certified company, Trifork Security has implemented an ISMS, which includes an information security policy and controls, which are continuously improved.

In the following, we will elaborate the areas and provide an overview of the primary implemented controls.

Information security policies

Based on ISO 27001, Trifork Security has developed an information security policy, framing our approach to information security, as well as relevant topic-specific policies.

Organisation of information security

The management team responsible for the day-to-day operation of Trifork Security consists of Mads Vigh, CEO; Karsten Thygesen, CTO; Stig Andersen, CPO; and Philip Lyngø, CISO and Manager.

Trifork Security has established an ISB. The ISB has board meetings every three months concerning risks, recommendations and news from stakeholders, events and incidents, as well as other relevant topics. The ISB consists of the management team and relevant employees such as representatives from the GRC team. The ISB is responsible for Trifork Security's information security.

Employee security

All employees (full-time and part-time included) sign an employment contract, including a confidentiality section. Interns sign a non-disclosure agreement. This confidentiality is maintained during and after employment.

Trifork Security requires all employees to have a clean criminal record, and criminal records are obtained annually.

As part of the onboarding process, all employees must participate in an "introduction to information security" meeting, where topics such as information security guidelines, GDPR, and incident reporting are reviewed by either the CISO or a GRC consultant. During onboarding, all employees read and accept all guidelines regarding information security, and these guidelines must be read and accepted annually.

Trifork Security does continuous awareness training, including social engineering simulations, quizzes and more.

Access management

Trifork Security's general policy on access to systems is that access is only allowed if it serves a legitimate purpose and on a need-to-know basis. This applies to physical as well as logical access. Where technically feasible, all access to systems must be logged with accurate information on time and identification of the user who accessed the system.

During onboarding, access is given to employees based on RBAC. If the need arises, access to systems can be given later in one's employment if this serves a legitimate purpose. This process is managed through our ITSM system.

All access rights are removed as part of the offboarding process.

Access rights are reviewed for systems every three months to ensure any errors or changes are corrected.

Customers only have access to their own systems.

Cryptography

All data connections transmitting confidential, personal or sensitive data must be encrypted with up-to-date technology.

Data extracts containing sensitive data transmitted between Trifork Security and our customers and/or business partners must be encrypted, e.g. by use of PGP, only allowing the intended party to open them.

Data extracts include all types of sensitive data on all types of media – for example CDs, USB sticks, emails and digital uploads.

Physical and environmental security

Customer data is stored and protected in our suppliers'/partners' data centres, depending on the services delivered.

Operations security

Operations security is an important part of Trifork Security's daily operations and we make an effort to document our operations procedure.

Trifork Security has set up log monitoring. Alarms are raised by e.g. specific log patterns and errors. Audit events are logged and used centrally in our log management platform.

All our endpoints are protected against malware, and continuous vulnerability scanning is being carried out. Patching takes place continuously and follows a determined patch management plan.

Backup of Trifork Security systems is done by our hosting partner.

All systems and services are monitored 24/7 by our SOC.

Authentication and authorisation are centrally handled, and different roles are given minimum privileges to systems and services internally at Trifork Security.

Trifork Security makes network segmentation via firewalls and microsegmentation.

Trifork Security regularly performs vulnerability scans.

All production systems are redundant, where possible.

All mobile devices and laptops are managed by MDM.

Change management

Trifork Security has a process for change management, covering standard, normal and emergency changes based on ITIL. The process includes adequately documenting e.g. the change risk, rollback plan and test plan. An approval phase and CAB phase as well as a verification phase are also part of the process. The changes are documented in our ITSM system, and this is done to ensure that any possible consequences can be linked back to the change.

Supplier relationships

Trifork Security has established a supplier and partner management process for both selection and evaluation of suppliers/partners. The selection process consists e.g. of classifying the supplier/partner and based on classification, there are information security requirements the supplier/partner must comply with.

Annually we evaluate the supplier/partner to ensure that they still comply with the requirements indicated in the partner management process.

Incident management

Trifork Security has implemented an information security incident management process. The processes consist of reporting, assessing, handling and learning from information security incidents. Reporting of information security incidents is communicated to the employees and is an easy procedure where employees send a specific template to an ISB mailbox.

Furthermore, Trifork Security has implemented an operational incident process that can be escalated to a major incident process, e.g. containing communication plans.

Information security aspects of business continuity management

An emergency response plan is implemented with clear roles and responsibilities, RPO and RTO, as well as action cards. The plan has been developed to ensure business continuity and to maintain a high level of information security.

The emergency response plan is tested annually and is continuously improved.

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

Changes to Trifork Security's system during the period

During the period from 1 March 2024 to 31 December 2024, Trifork Security has obtained an ISO 27001:2022 certification. The certificate demonstrates our great information security focus and dedication to strengthen our internal processes, ensuring a reliable and secure service to our customers. The certificate is valid during the period 18 October 2024 to 17 October 2027 with annual external audits.

No material changes to services or control activities were made during the period.

Complementary controls at the customers

As part of the delivery of services, the customers must implement certain controls that are important to achieve the control objectives specified in the description. This includes:

- Setting up and administering own users of the solution in the production environment (identity and access management)
- Setting up and administering users from Trifork Security who have access to the customer's environment (identity and access management)
- Ensuring that sensitive personal information is not included in support cases sent to Trifork Security via tickets etc.
- Complying with password policies based on the best practices set up by Trifork Security in software-as-a-service solutions.

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 operation that the processing is 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 agreement that the security measures agreed have been established.	No exceptions noted.
B.2	The data processor has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the security measures agreed with the data controller.	Checked by way of inspection that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data. Checked by way of inspection that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment. Checked by way of inspection that the data processor has implemented the security measures agreed with the data controller.	No exceptions noted.
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	Checked by way of inspection that antivirus software has been installed for the systems and databases used in the processing of personal data. Checked by way of inspection that antivirus software is up to date.	No exceptions noted.

Control objective B:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	Checked by way of inspection that external access to systems and databases used in the processing of personal data takes place only through a secured firewall. Checked by way of inspection that the firewall has been configured in accordance with the relevant internal policy.	No exceptions noted.
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	Inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. Inspected network diagrams and other network documentation to ensure appropriate segmentation.	No exceptions noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	Checked by way of inspection that formalised procedures are in place for restricting users' access to personal data. Checked by way of inspection that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need. Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data. Checked by way of inspection of a sample of user's access to systems and databases that such access is restricted to the employees' work-related need.	No exceptions noted.

Control objective B:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
B.7	System monitoring with an alarm feature has been established for the systems and databases used in the processing of personal data. This monitoring comprises: • Splunk ITSI.	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.
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.	No exceptions noted.

Control objective B:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests

B.9	Logging of the following matters has been established in systems, databases and networks:
	• Activities performed by system administrators and others holding special rights
	• Security incidents comprising:
	  ○ Changes in log set-ups, including disabling of logging
	  ○ Changes in users' system rights
	  ○ Failed attempts to log on to systems, databases or networks
	  ○ Log on to systems identified as crown jewels
	  ○ Changes in systems configuration on baseline servers.
	Log data are protected against manipulation and technical errors and are reviewed regularly.
		Checked by way of inspection that formalised procedures are in place for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs.
		Checked by way of inspection that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated.
		Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.
		Checked by way of inspection of a sample of day of logging that the content of log files is as expected compared to the set-up and that documentation confirms the follow-up performed and the response to any security incidents.
		Checked by way of inspection of a sample of day of logging that documentation confirms the follow-up performed on activities carried by system administrators and others holding special rights.
			No exceptions noted.

Control objective B:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	Checked by way of inspection that formalised procedures are in place for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. Checked by way of inspection of a sample of development or test database that personal data included therein are pseudonymised or anonymised. Checked by way of inspection of a sample of development or test database in which personal data are not pseudonymised or anonymised that this has taken place according to agreement with, and on behalf of, the data controller.	No exceptions noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	Checked by way of inspection that formalised procedures are in place for regularly testing technical measures, including for performing vulnerability scans and penetration tests. Checked by way of inspection of samples that documentation confirms regular testing of the technical measures established. Checked by way of inspection that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner and communicated to the data controllers as appropriate.	No exceptions noted.

Control objective B:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
B.12	Changes to systems, databases or networks are made consistently with established procedures that ensure maintenance using relevant updates and patches, including security patches.	Checked by way of inspection that formalised procedures are in place for handling changes to systems, databases or networks, including handling of relevant updates, patches and security patches. Checked by way of inspection of extracts from technical security parameters and set-ups that systems, databases or networks have been updated using agreed changes and relevant updates, patches and security patches.	No exceptions noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	Checked by way of inspection that formalised procedures exist for granting and removing users' access to systems and databases used for processing personal data. Checked by way of inspection of a sample of employee's access to systems and databases that the user accesses granted have been authorised and that a work-related need exists. Checked by way of inspection of a sample of resigned or dismissed employee that the employee's access to systems and databases was deactivated or removed in a timely manner. Checked by way of inspection that documentation states that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	No exceptions noted.

Control objective B:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	Checked by way of inspection that formalised procedures are in place to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects. Checked by way of inspection that users' access to processing personal data that involve a high risk for the data subjects may only take place by using two-factor authentication.	No exceptions noted.
B.15	Physical access security measures have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	Checked by way of inspection that formalised procedures are in place to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. Checked by way of inspection of documentation that only authorised persons have physical access to premises and data centres at which personal data are stored and processed.	No exceptions noted.

Control objective C:

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

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

Control objective C:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
C.3	The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant: • Certificates of criminal record • Verifying identity with MitID.	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 agreement that the requirements therein for screening employees are covered by the data processor's screening procedures. Checked by way of inspection of one employee appointed during the assurance period that documentation exists of the screening having comprised: • Certificates of criminal record • Verifying identity with MitID.	No exceptions noted.
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	Checked by way of inspection of one newly appointed employee that the employee has signed a confidentiality agreement. Checked by way of inspection of one newly appointed employee that the employee has been introduced to: • The information security policy • Procedures for processing data and other relevant information.	No exceptions noted.
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	Inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned. Checked by way of inspection of one employee resigned or dismissed that rights have been deactivated or terminated and that assets have been returned.	No exceptions noted.

Control objective C:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	Checked by way of inspection that formalised procedures are in place to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. Checked by way of inspection of one employee resigned or dismissed that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality.	No exceptions noted.
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	Checked by way of inspection that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data. Inspected documentation stating that all employees who have either access to or process personal data have completed the awareness training provided.	No exceptions noted.

Control objective D:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
D.1	Written procedures are in place which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. Checked by way of inspection that procedures are up to date.	No exceptions noted.
D.2	The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines: • Any agreed specific requirements for the data processor's storage periods and deletion routines in accordance with the concluded data processing agreements are followed.	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 session from the data processor's list of processing activities that documentation states that personal data are stored in accordance with the agreed storage periods. Checked by way of inspection of a sample of data processing session from the data processor's list of processing activities that documentation states that personal data are deleted in accordance with the agreed deletion routines.	No exceptions noted.
D.3	Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: • Returned to the data controller and/or • Deleted if this is not in conflict with other legislation.	Checked by way of inspection that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data. Checked by way of inspection of one terminated data processing session that documentation states that the agreed deletion or return of data has taken place.	No exceptions noted.

Control objective E:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
E.1	Written procedures are in place which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place for only storing and processing personal data in accordance with the data processing agreements. Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of data processing session from the data processor's list of processing activities that documentation states that data processing takes place in accordance with the data processing agreement.	No exceptions noted.
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	Checked by way of inspection that the data processor has a complete and updated list of processing activities stating localities, countries or regions. Checked by way of inspection of a sample of data processing session from the data processor's list of processing activities that documentation states that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller.	No exceptions noted.

Control objective F:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
F.1	Written procedures are in place which include requirements for the data processor when using subprocessors, including requirements for subprocessing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place for using subprocessors, including requirements for subprocessing agreements and instructions. Checked by way of inspection that procedures are up to date.	No exceptions noted.
F.2	The data processor only uses subprocessors to process personal data that have been specifically or generally approved by the data controller.	Checked by way of inspection that the data processor has a complete and updated list of subprocessors used. Checked by way of inspection of a sample of subprocessor from the data processor's list of subprocessors that documentation states that the processing of data by the subprocessor follows from the data processing agreement – or otherwise as approved by the data controller.	No exceptions noted.
F.3	When changing the generally approved subprocessors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved subprocessors used, this has been approved by the data controller.	Checked by way of inspection that formalised procedures are in place for informing the data controller when changing the subprocessors used. 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 agreement that it includes the same requirements and obligations as are stipulated in the data processing agreement between the data controller and the data processor.	No exceptions noted.
F.5	The data processor has a list of approved subprocessors disclosing: • Name • Company registration no. • Address • Description of the processing.	Checked by way of inspection that the data processor has a complete and updated list of subprocessors used and approved. Checked by way of inspection that, as a minimum, the list includes the required details about each subprocessor.	No exceptions noted.

Control objective F:

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

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

Control objective G:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
G.1	Written procedures are in place which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Checked by way of inspection that procedures are up to date.	No exceptions noted.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	Checked by way of inspection that the data processor has a complete and updated list of transfers of personal data to third countries or international organisations. Checked by way of inspection of a sample of data transfer from the data processor's list of transfers that documentation states that such transfers were arranged with the data controller in the data processing agreement or subsequently approved.	No exceptions noted.
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	Checked by way of inspection that formalised procedures are in place for ensuring a valid basis of transfer. Checked by way of inspection that procedures are up to date. Checked by way of inspection of a sample of data transfer from the data processor's list of transfers that documentation confirms a valid basis of transfer in the data processing agreement with the data controller and that transfers have only taken place insofar as this was arranged with the data controller.	No exceptions noted.

Control objective H:

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

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

Control objective I:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
I.1	Written procedures are in place which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Checked by way of inspection that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. Checked by way of inspection that procedures are up to date.	No exceptions noted.
I.2	The data processor has established the following controls to identify any personal data breaches: • Awareness of employees • Monitoring of network traffic • Follow-up on logging of access to personal data.	Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches. Checked by way of inspection of documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on. Checked by way of inspection of documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on in a timely manner.	No exceptions noted.

Control objective I:

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

No.	Data processor's control activity	Tests performed by PwC	Result of PwC's tests
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than 24 hours after having become aware of such personal data breach at the data processor or a subprocessor.	Checked by way of inspection that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach. 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 and no later than 24 hours after the data processor became aware of the personal data breach.	No exceptions noted.
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency. These procedures must contain instructions on descriptions of: • The nature of the personal data breach • Probable consequences of the personal data breach • Measures taken or proposed to be taken to respond to the personal data breach.	Checked by way of inspection that the procedures in place for informing the data controllers in the event of any personal data breach include detailed instructions for: • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach. Checked by way of inspection of documentation that the procedures available support that measures are taken to respond to the personal data breach.	No exceptions noted.

PENNEO

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

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

Mads Vigh
CEO
På vegne af: Trifork Security A/S
Serienummer: 9e48e84c-fcc8-4da7-9673-58e68ad0c0d7
IP: 83.151.xxx.xxx
2025-02-24 07:26:22 UTC

Mit ID

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
På vegne af: PricewaterhouseCoopers Statsautoriseret…
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2025-02-24 07:40:33 UTC

Mit ID

Rico Lundager
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Senior manager
På vegne af: PricewaterhouseCoopers Statsautoriseret…
Serienummer: 2e75390a-f48a-4123-b26c-3fd3e97823aa
IP: 208.127.xxx.xxx
2025-02-24 08:11:16 UTC

Mit ID