www.pwc.dk

TwentyThree

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 January 2023 to 31 January 2024 pursuant to the data processing agreement with data controllers

March 2024

Contents

1. Management's statement

TwentyThree processes personal data on behalf of data controllers in accordance with data processing agreements.

The accompanying description has been prepared for data controllers who have used TwentyThree's online marketing platform 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.

TwentyThree uses Amazon AWS, Fastly, Twilio, Sentry, Stripe, Segment, HubSpot, Amplitude, Planhat and Amberscript as subprocessors. This report uses the carve-out method and does not comprise control objectives and related controls that the subprocessors perform for TwentyThree.

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

TwentyThree confirms that:

a) The accompanying description in section 3 fairly presents TwentyThree's online marketing platform that has processed personal data for data controllers subject to the data protection rules throughout the period from 1 January 2023 to 31 January 2024. The criteria used in making this statement were that the accompanying description:

   (i) Presents how TwentyThree's online marketing platform was designed and implemented, including:

   - The types of services provided, including types 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 contracts, instructions and agreements 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 TwentyThree's online marketing platform 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 online marketing platform in the processing of personal data in the period from 1 January 2023 to 31 January 2024.

(iii) Does not omit or distort information relevant to the scope of TwentyThree's online marketing platform 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 TwentyThree's online marketing platform 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 January 2023 to 31 January 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 individuals who have the appropriate competence and authority, throughout the period from 1 January 2023 to 31 January 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.

Copenhagen, 15 March 2024
TwentyThree

Thomas Madsen-Mygdal Chief Executive Officer	Steffen Fagerström Christensen Chief Technology Officer

2. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on information security and measures for the period from 1 January 2023 to 31 January 2024 pursuant to the data processing agreement with data controllers

To: TwentyThree and TwentyThree's customers

Scope

We have been engaged to provide assurance about TwentyThree's description in section 3 of TwentyThree's online marketing platform in accordance with the data processing agreement with data controllers throughout the period from 1 January 2023 to 31 January 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 TwentyThree has designed and effectively operated suitable controls related to the control objectives stated in section 4. The report does not include an assessment of TwentyThree'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").

TwentyThree uses Amazon AWS, Fastly, Twilio, Sentry, Stripe, Segment, HubSpot, Amplitude, Planhat and Amberscript as subprocessors. This report uses the carve-out method and does not comprise control objectives and related controls that the subprocessors perform for TwentyThree.

Some of the control objectives stated in Twenty Three's description in section 3 can only be achieved if the complementary controls at the data controllers are suitably designed and operating effectively with Twenty Three's 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.

TwentyThree's responsibilities

TwentyThree 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 TwentyThree'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 online marketing platform 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

TwentyThree's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of TwentyThree's online marketing platform 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 TwentyThree's online marketing platform as designed and implemented throughout the period from 1 January 2023 to 31 January 2024;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January 2023 to 31 January 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 January 2023 to 31 January 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 TwentyThree's online marketing platform 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, 15 March 2024
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Iraj Bastar
Director

3. Description of processing

The purpose of the data processor's processing of personal data on behalf of the data controller is for TwentyThree to be able to perform the "master agreement" with consideration of the "data processing agreement" which describes the services being provided to each data controller, namely providing video marketing technology designed for companies and organisations. The TwentyThree product platform allows the data processors to produce, manage, deliver and track their videos and webinar content across channels. In keeping with previous annual audits and to align with internal year processes, the audit period covers the 13 calendar months.

Nature of processing

The data processor's processing of personal data on behalf of the data controller primarily concerns TwentyThree's provision of the following services:

TwentyThree, The Video Marketing Platform allows customers to deliver video content to a central origin which will prepare and distribute the video globally through the TwentyThree infrastructure. Players and streams are optimised to work across all browsers and mobile devices. The platform is set up to allow customers to deliver a single video signal after which TwentyThree will adapt the signal for adaptive playback, meaning that devices will receive a version of the video optimised for its screen and bandwidth. The platform allows at-scale delivery of video content from redundant core origins through a global content delivery network (CDN).

TwentyThree Webinars allows the customers to run live webinars directly in-browser without the need of large downloads by speakers or the audience. The online software is fully integrated into the customers' marketing tech stack, providing full report on visits, conversions, attendees and leads. The recordings are ready moments after the live webinar is finished and can be hosted in the customers' on-demand webinars in a branded website hub.

TwentyThree Personal is a more creative and collaborative way to create videos. In a world of disinterested and inauthentic communications, Personal from TwentyThree is a better way to record, edit, send and track your personal videos. With Personal, organisations can start producing dynamic personal videos and simultaneously record with the user's screen and webcam directly in-browser, with the ability to edit what shows on screen afterwards. The product lets users set up flows to assign tasks to others to add a personal recording to a video that has already been produced, whether that is a message from the CEO or another viewpoint on a problem.

Enterprise provides dedicated tools for thousands of Enterprise marketers around the world to succeed with video. With single sign-on, unlimited video storage and traffic, advanced security, multiple backends and governance filters, TwentyThree enables enterprises to take their video marketing and processes to the next level. Delivering results from video starts with the tools and processes that accompany them. Our enterprise solution offers the ability to run global and localised accounts that streamline video management, distribution and analysis.

Organisation in Security and GDPR

System owner: Chief technology officer
Security officer: Chief technology officer
Data protection responsible: Chief technology officer and general counsel
Data protection advisor: Chief technology officer and general counsel
Responsible for internal IT security: System operations team

Personal data

The types of personal data processed include, but are not limited to, full name, username, email address, phone number, location, employer, IP address, profile photograph, third-party login, social media accounts and cookies along with video viewing activity and comment history.

The data controllers are aware that the service is not intended or designed for the processing of sensitive information such as the special categories of personal data covered by articles 8, 9 and 10 of the GDPR, and agree not to host any sensitive information through the service without prior agreement with the data processor.

Categories of data subjects falling within the data processing agreement: Our services may be used to process personal data for system users and for video viewers.

Risk assessment

TwentyThree performs risk management in several areas and at several levels. Once a year, we conduct a risk assessment to carefully review the security of our systems and the protection of data processed in our platforms. This assessment includes the review of existing records of processing activities, evaluation of the risks inherent to cloud computing and the delivery of a Software-as-a-Service product along with the safety of our internal systems and the requirements set out by applicable data protection legislations. Based on this risk assessment, we update our security practices, policies and training.

The data protection team is responsible for reviewing the risk analysis in order to update or establish new procedures and technical and organisational measures. The risk assessment report is approved by Management. No critical risks have been identified, and the currently adopted security practices have been evaluated as satisfactory.

Control measures

Control objective A: Data controller instructions for processing data

Written data processing agreements are entered into with both customers and subcontractors. The agreements with customers is based on TwentyThree's standard data processing agreement, which again is based on guidelines from the Danish Data Protection Agency's standard.

Yearly review of procedures

Once a year or in the event of major changes, TwentyThree reviews the applicable standard and concluded data processing agreements, policies and procedures.

Control objective B: Technical measures to safeguard data processing

TwentyThree's platform

The TwentyThree platform is designed around the principle of least privilege. All access control settings, file system access privileges, network port access et cetera are off by default and enabled only for operational purposes with the minimum subset of resources necessary. Such privileges are idempotently managed by a central configuration management process.

By design, any component of the platform not designed from a security perspective to persist its state in accordance with the security guidelines set forth in this document is considered stateless. As such, any non-stateful component holds no customer data at rest.

The access of platform components to and from the public internet is delegated to several reverse proxying servers so that no application instances or infrastructure components are directly reachable from the public internet.

Unauthenticated contexts such as the public web page are isolated from the authenticated context at the network level. Additionally, infrastructure layer contexts are isolated at the network level to strictly isolate the potential reach of a given breach. As such, no infrastructure configuration is accessible from the application context and vice versa.

The TwentyThree platform employs a strict paradigm of strongly separated network layers to provide a base level of security. System management of physical infrastructure components are separated from the production networking layers by being a physically separate network accessible through an independent access point. In addition to our extensive internal security measures, TwentyThree employs a third-party service provider to perform scans across the TwentyThree platform centred around the OWASP 2013 and 2017 security guidelines.

System logging

All requests to and in-band access of the TwentyThree platform are collected in a centralised logging system. System logging is covered by control activity B9. Logs include, but are not limited to, HTTP/HTTPS requests, platform events, system events, security events from access or attempts to access individual servers. Collected logs are kept in a searchable index accessible to only personnel with the highest level of system access for a duration of time necessary to identify and investigate incidents. Logs are kept for at least 30 days.

In the case of a severe security event, a report will be forwarded to impacted customers at the discretion of TwentyThree and in accordance with our security breach notification policy.

Monitoring

All services that make up TwentyThree are monitored internally, and we compute metrics both for availability and performance. In addition, access to external-facing services is monitored using Pingdom. For both of these monitoring regimes, all incidents are assigned to the on-duty systems operations team for resolution.

TwentyThree is a cloud-hosted platform with TwentyThree assuming full responsibility for the maintenance and systems administration of the platform. For this reason, we routinely:

- make status reports and event information publicly available through the dedicated TwentyThree status page at https://status.twentythree.com
- make uptime and availability monitoring available at http://uptime.twentythree.com.

Configuration management

By design, all services underpinning the TwentyThree platform apply the described security architecture idempotently by being fully defined in, and controlled by, a configuration management system. The source of truth for the configuration management is providing a full history of changes in system configuration.

Configuration of network and storage equipment is manually managed with all details of the configuration fully documented in a version-controlled source repository, providing full history and audit trail of the configuration of the equipment.

Access management

Access to the TwentyThree platform is restricted to an explicit need-to-know and need-to-access basis and utilises the principle of least privilege when granted. The system administrative team frequently monitors this access to non-application-level components, which is idempotently enforced for all non-application-level components using the configuration management regime described in this document.

We log when employees have been granted or revoked access to personal data, including the justification for the access. Access lists are reviewed at least quarterly. Access to all TwentyThree systems and services that process data on behalf of customers must be protected with 2-factor authentication. In most cases, this is implemented by using the TwentyThree single sign-on gateway.

Passwords

Our authentication and password management includes 2-factor authentication when accessing any system containing customer data, and we enforce requirements on complex, secure passwords to such systems as well.

Our products support single sign-on (SSO), and customers can enforce their own password requirements to access their platform.

Data encryption

Data stored on the TwentyThree platform is encrypted at rest whenever possible. Personal data such as real names, username and email addresses is securely encrypted by the database systems, and the classification and categorisation of personal data is detailed in our data processing agreements with customers. For performance reasons, we do not encrypt raw video and thumbnail image data at rest.

External data transit of sensitive data is, unless elected by the customer, always handled over HTTPS/TLS following industry recommendations for high-compatibility environments or using other similar or stronger means of encryption depending on the protocol in question. Equally, all databases containing sensitive customer data are encrypted using 256-bit AES encryption at rest and require manual operation by a system administrator to be decrypted for use. This practice extends to all backups and other derivatives of the database.

The IT contingency plan

Contingency planning is done based on the ongoing risk analysis of the company's operations environment. The risk analysis reveals the individual units' dependence on the various systems and services. By means of contingency planning, we can thereby meet the required need for availability in the best possible way.

System administrative personnel actively monitors security bulletins for software used across the platform, including but not limited to relevant mailing lists and the Common Vulnerabilities and Exposures database. High-risk vulnerabilities are sought mitigated as soon as the personnel becomes aware of them, while low-risk vulnerabilities are mitigated as soon as it can be proven that such a patch does not impact the stability of the platform. Non-security-related software updates are applied in a continuous, rolling fashion to avoid any one update causing platform-wide interruptions.

Additionally, system administrative personnel maintains runbooks for recovery of system-critical infrastructure which are audited and tested monthly to ensure recovery is functional.

Incident management and handling of security breaches

All TwentyThree services are covered by automated monitoring which alerts relevant personnel to any operational issues. Case management for high-level issues is handled through a third-party system that automatically notifies the on-call rotation of technical operational staff of incidents. Assigned staff follows any available runbook for resolution of incident. The third-party system is used as the source-of-truth for resolution of operational incidents through the automated monitoring system.

Severe non-operational issues are reported to technical staff, and communication regarding the resolution of the issue is handled through auditable channels with individual staff members reporting and, when necessary, receiving acknowledgement and approval of remediation steps performed.

All issues of user impact as well as their remediation are reported through official technical communication channels. Customers experiencing severe impact will be contacted directly when necessary, and TwentyThree prepares an overview of preventive actions taken to avoid similar situations from occurring.

Technical emergency operations rely on established runbooks for recovery of services in an established priority order. Should full failure of primary operations occur, secondary operations are established by the system-administrative staff in the same priority order.

Control objective C: Organisational measures to safeguard data processing

Security policy

TwentyThree's security policy establishes procedures and controls for our internal systems and includes all services offered to our customers. Continued work to adapt and improve security measures is carried out in collaboration with highly qualified specialists. Based on this framework, control areas and control activities

have been implemented in accordance with best practice in order to minimise the risk of services offered by TwentyThree.

Overall, the following areas are included in TwentyThree's security policy:

- Infrastructure and system operations
- Development, deployment and monitoring
- Security awareness, redundancy and continuity.

Employee awareness training in relation to GDPR and IT Security

TwentyThree's way of working is GDPR-driven. A central group has been set up to oversee the regulation across the company. All employees must be familiar with current and relevant policies, guidelines and procedures.

The company maintains a set of security awareness guidelines and training materials which are used to ensure all employees are aware of responsibilities and expectations. These materials cover GDPR topics and other security practices. New employees joining the company receive training as part of the onboarding, and the entire team undergoes mandatory, annual training. The guidelines themselves are reviewed and revised annually by Management.

Control objective D: Deleting and returning data

TwentyThree is established the procedure to govern the secure deletion and/or return of data when it is no longer required for its intended purpose. Requesting personal data to be returned or deleted within thirty days of termination or cancellation of the agreement.

Control objective E: Data storage

Categories of personal data collected, processed and stored

TwentyThree, as a data processor for the data controller (customer), only collects, processes and stores personal data at the data controller's request and agreement.

Control objective F: Approval and inspection of sub-processors

Written data processing agreements are entered with customers and subprocessors. TwentyThree's data processing agreement is pre-signed and publicly available at TwentyThree's website. Once a year or in case of major regulatory changes, the data processing agreement is reviewed and updated.

Subprocessors

TwentyThree relies on third-party services for the delivery of our service. A subset of these services handle and processes personal data on behalf of us and our customers and are characterized as a Data Subprocessor and subject to our Data Processing Agreement. A list of all subprocessors is publicly available at https://www.twentythree.com/subprocessors. Using the same page and in accordance with our Data Processing Agreement, customer can request to notified of subprocessor changes.

Control objective G: Transfer of personal data to third countries

TwentyThree uses different subprocessors, including subprocessors located outside the EEA. For subprocessors located in third countries, we verify the transfer tool by making sure that there is an adequacy decision in place or up to date and compliant standard contractual clauses. All subprocessors are listed at https://www.twentythree.com/subprocessors. We have obtained general written consent to the use of such subprocessors, and any update to the list is previously informed to the customers who have the right to reasonably refuse any update.

Control objective H: Data subject rights

TwentyThree is responsible for assisting the customers to fulfil their data subjects' requests. The customers are able to download a report of all personal data processed in TwentyThree's platform in relation to a specific data subject through the privacy dashboard. Other requests can be sent to privacy@twentythree.com and are replied within 24 hours or fulfilled as soon as possible. Once the GDPR request is processed, a copy of the log activity is sent to the customer by mail. The GDPR request is stored in our internal control systems.

Control objective I: Data breaches

Personal data breach management

TwentyThree adopts a personal data breach policy establishing that we must notify the affected customer of any personal data breach without undue delay and, where feasible, no later than 72 hours after we become aware of the breach. The information to be provided to the customer in case of a personal data breach follows the requirements established by the GDPR.

Complementary controls at the data controllers

The data controllers are responsible for determining the purpose and the means of the processing of personal data. The primary responsibilities of the data controller, in its use of TwentyThree's platforms, include:

- processing personal data in accordance with the requirements of all relevant data protection laws and regulations and all its instructions for the processing of personal data shall comply with data protection laws and regulations
- ensuring accuracy, quality and legality of personal data and the means by which the data controller acquired personal data, including transparent information provided to the data subjects
- ensuring compliance with principles of data minimisation, purpose and storage limitation
- ensuring that the data subjects have received all information required to ensure transparency under the data protection legislation
- ensuring compliance with any request from data subjects to exercise their rights under the data protection legislation, which can be achieved through the privacy dashboard or by sending an email to privacy@twentythree.com
- ensuring that no sensitive data is collected, stored or anyhow processed in TwentyThree's platforms
- enforcing its own password management systems
- requesting personal data to be returned or deleted within thirty days of termination or cancellation of the agreement
- notifying TwentyThree of any change in the instructions to the processing of personal data.

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.

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 users' 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: • Access to databases with personal data • Monitoring of security bulletins • Service availability.	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.
	Logon data are protected against manipulation and technical errors and are reviewed regularly.
		Checked by way of inspection that formalised procedures are in place for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data, including review of and follow-up on logs.
		Checked by way of inspection that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated.
		Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.
		Checked by way of inspection of a sample of 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.

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 a test database that personal data included therein are pseudonymised or anonymised.	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.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.
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.

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.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.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.

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.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, throughout the assurance period, only authorised persons have had physical access to premises.	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 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.
C.3	The employees of the data processor are screened as part of the employment process. Such screening comprises, as relevant: • Contact to two former employers.	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: • Contact to two former employers.	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.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.
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.

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.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: • Storage in data centres in the EU • Backup kept up to 30 days • Notification of customer before deletion of data • Deletion of data 30 days after terminated DPA.	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.	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 sessions 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 sessions 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 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.	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 accepted standard 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. • 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 processing agreements 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 transfers 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 72 hours after having become aware of such personal data breach at the data processor or a subprocessor.	Checked by way of inspection that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach. Made inquiries 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 72 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.

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

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

Thomas Madsen-Mygdal
Kunde
Serienummer: 6ba81ffa-3d6b-41c1-952e-5a959a957e7d
IP: 62.198.xxx.xxx
2024-03-15 12:02:39 UTC

Steffen Fagerström Christensen
Kunde
Serienummer: 5b96f226-8720-4ae0-8814-3fc1c1eee645
IP: 87.52.xxx.xxx
2024-03-15 14:20:59 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 83.136.xxx.xxx
2024-03-15 14:28:19 UTC

Iraj Bastar
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
PwC-medunderskriver
På vegne af: PwC
Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96
IP: 208.127.xxx.xxx
2024-03-15 14:31:36 UTC