www.pwc.dk

# *team.blue Denmark A/S*

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

*March 2025*

# Contents

1. Management's statement ..... 3
2. Independent auditor's report ..... 5
3. Description of processing ..... 8
4. Control objectives, control activity, tests and test results ..... 13

# 1. Management's statement

team.blue Denmark A/S (team.blue Denmark) processes personal data on behalf of customers (data controllers) in accordance with the data processing agreements.

The accompanying description has been prepared for customers who have used team.blue Denmark's hosting services to customers 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.

team.blue Denmark uses the following subprocessors:

- T1A Enterprise A/S for erasure of data and decommissioning of hardware
- B4Restore A/S for IBM Spectrum (TSM) backup services
- inMobile ApS for SMS gateway for multi factor authentication.

This report uses the carve-out method and does not comprise control objectives and related controls that the subprocessors perform for team.blue Denmark.

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.

team.blue Denmark confirms that:

a) The accompanying description in section 3 fairly presents team.blue Denmark's hosting services to customers that have processed personal data for data controllers subject to the data protection rules throughout the period from 1 January 2024 to 31 December 2024. The criteria used in making this statement were that the accompanying description:

   (i) Presents how team.blue Denmark's hosting services to customers 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 team.blue Denmark's hosting services to customers, 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 team.blue Denmark's hosting services to customers in the processing of personal data in the period from 1 January 2024 to 31 December 2024;

(iii) Does not omit or distort information relevant to the scope of team.blue Denmark's hosting services to customers 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 team.blue Denmark's hosting services to customers 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 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 January 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.

Skanderborg, 5 March 2025
**team.blue Denmark A/S**

Lotte Bendstrup
MD

# 2. Independent auditor's report

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

To: team.blue Denmark A/S (team.blue Denmark) and customers (data controllers)

**Scope**

We have been engaged to provide assurance about team.blue Denmark's description in section 3 of team.blue Denmark's hosting services to customers in accordance with the data processing agreement with customers throughout the period from 1 January 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 team.blue Denmark has designed and effectively operated suitable controls related to the control objectives stated in section 4. The report does not include an assessment of team.blue Denmark'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").

team.blue Denmark uses the following subprocessors:

- T1A Enterprise A/S for erasure of data and decommissioning of hardware
- B4Restore A/S for IBM Spectrum (TSM) backup services
- inMobile ApS for SMS gateway for multi factor authentication.

This report uses the carve-out method and does not comprise control objectives and related controls that the subprocessors perform for team.blue Denmark.

Some of the control objectives stated in team.blue Denmark's description in section 3 can only be achieved if the complementary controls at customers are suitably designed and operating effectively with team.blue Denmark'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.

**team.blue Denmark's responsibilities**

team.blue Denmark 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 team.blue Denmark'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 hosting services to customers 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**

team.blue Denmark's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of its hosting services to customers 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 team.blue Denmark's hosting services to customers as designed and implemented throughout the period from 1 January 2024 to 31 December 2024;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January 2024 to 31 December 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 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 team.blue Denmark's hosting services to customers 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, 5 March 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

## 3.1. Introduction

As part of the services provided to the data controller and during the term of the concluded data processing agreement, the data processor will process personal data on behalf of the data controller for the purpose of storing the personal data.

As a hosting company, team.blue Denmark hosts many customers' technical platforms (services) as agreed in hosting agreements and concluded terms and conditions. The services are hosted on team.blue Denmark's servers, which are located at physical data centres. team.blue Denmark offers its customers technical platforms that enable customers to store their data. team.blue Denmark operates the servers on which the data is stored, which includes provision of technical assistance and carrying out maintenance work.

## 3.2. Nature of processing

The data processor's processing of personal data on behalf of the data controller primarily concerns storing of personal data. As a natural part of providing the services, team.blue Denmark will also carry out deletion of data in accordance with instructions from the data controller and the data processing agreement.

team.blue Denmark is in no way dependent on the customer to provide or store personal data on their services in order to provide the services.

When carrying out our data processing activities we comply with the following:

- Personal data is processed based on instructions from the data controller.
- The data controller is informed if an instruction, in our opinion, infringes the regulation or other European Union or member state data protection provisions.
- Organisational measures are implemented to safeguard the security of processing, such as management reviews and approvals, screenings procedures, employee confidentiality requirements, awareness training and access controls.
- Personal data is stored and deleted in accordance with the data processing agreement with the data controller.
- The data controller is informed of the locations at which the data processing is taking place.
- No current transfer of personal data to third countries is taking place. Such transfers can only be carried out according to instructions from the data controller.
- Subprocessors are only being used based on a general approval from the data controller and upon prior notification of the use of a new subprocessor.
- Assistance is provided to the data controller to comply with data subject's rights.
- If any personal data breach occurs, we will inform the data controller of it without undue delay and provide relevant information about the incident.

## 3.3. Personal data

team.blue Denmark makes its services available to the controller, and the data controller is thus able to store personal data using the services. As team.blue Denmark has no control or knowledge of the types of personal data stored by the data controller, the responsibility to define and specify the personal data and data subjects will lie with the data controller.

To provide the data controller with a starting point, the data processing agreement will include the following listings in Appendix A:

| REGULAR PERSONAL INFORMATION | PERSONAL DATA SPECIFICALLY REGULATED IN DATABESKYTTELSESLOVEN | SPECIAL CATEGORIES OF PERSONAL INFORMATION |
|---|---|---|
| Any other kind of personal information that is not special categories of personal information | Information about criminal offences<br><br>CPR number | Racial or ethnic origin<br><br>Political, religious or philosophical beliefs<br><br>Trade union membership<br><br>Data concerning health<br><br>Information revealing sex life or sexual orientation<br><br>Genetic and biometric data |

To provide the data controller with a starting point, categories of data subjects falling within the data processing agreement are set out to be:

Classifications of data subjects whom the personal information pertains to may, for example, be users, employees, applicants, candidates, customers, consumers, patients or similar individuals.

## 3.4. Practical measures

The established information security management systems we follow are essential for the processing of personal data controls in the ISMS, as well as other security measures, and will be covered by our ISAE 3402 auditor's report and ISO 27001 audits.

These measures are implemented and based on a risk assessment, recognised standards, including ISO 27001, and general guidelines of the data protection regulation. All employees have been made aware of team.blue Denmark's policies and guidelines, including information security and data security policies, and they are continuously trained throughout their employment.

## 3.5. Security of processing

### Organisation of security

We have established an industry-leading information security programme (ISMS) that gives our customers the best protection and highest degree of confidence. The programme follows the ISO 27001 security standard, which we have been certified for since 2015.

### Policies, procedures and standards

We have defined a set of policies, procedures and standards for how we operate in the company and take the best care of your data. The documents are regularly updated in line with changes to our risk assessment. In this way we ensure that we always prioritise our efforts where they are needed the most.

## Employee security

All employees and consultants with access to systems and facilities are subject to our security policies. Everyone undergoes security awareness training where they are presented with all relevant and current privacy and security topics. This occurs both upon commencement and continuously throughout their employment. The purpose is to equip employees so they can cope with actual threats against company and customer data.

To boost the overall level of the industry and to maintain own competences, our employees participate actively in communities and exchange of experience groups. We encourage our employees to constantly stay abreast of the latest developments and to acquire the highest certifications within security, networks, etc.

## Dedicated security and personal data competences

Our security manager is responsible for implementing and maintaining our information security programme. Our internal auditor regularly reviews our security setup and reports directly to Management. Finally, we have internal, legal competences within personal data, ensuring that personal data is processed according to the applicable rules both within the company and on behalf of our customers.

## Operational security

Our security environment is divided into several layers:

- Physical security – Our data centres are state of the art, and our data centre provider is responsible for the physical environment, such as power, cooling, fire suppression and access control, and we carry out stringent checks to ensure that our sub-contractors always comply with the applicable security regulations for this field.

- Network – Our network is segmented, so customers are protected from each other and from threats that move across the network. Firewalls restrict attacks on customers' environments, and DDoS protection limits the impact a potential attack might have on the servers. Advanced network inspection detects patterns and attack attempts from known malicious IP addresses and alerts our operations department, if necessary.

- Logical access – We only assign rights to employees who need them, and we evaluate them regularly. Only specially privileged employees have authority to manage the internal systems.

- Monitoring – We monitor our infrastructure and relevant services around the clock. All deviations are registered in our incident management system. In addition to monitoring, we have assigned a 24/7 on-call service.

- Logging – We log all access to management and customer environments. In this way, we ensure integrity and traceability and can correlate incidents. Our central log platform ensures that we can correlate logs from many sources.

- Backup – We perform backup based on the individual agreement with the customer or the agreed SLA. Backup data is always stored on another site than the production data, so a copy is always available in case of a critical failure.

- Anti-virus – Next-generation anti-virus software has been deployed on internal workstations. The next-gen anti-virus is designed to detect threats by detecting and preventing malicious behaviour. As a customer it is your responsibility to deploy anti-virus software in your own environment, which is key to protecting you from malicious behaviour.

- Business continuity and disaster recovery – Business continuity is about being prepared for incidents that may have a critical or disastrous impact on operations. Therefore, we have contingency plans which determine our procedures, routines and roles in the event of a disaster. Employees are trained for such an emergency several times a year.

In case of a security incident, an incident management plan and contingency plan have been prepared. All stakeholders and teams involved have been informed of their role if an incident that requires activation of the contingency plan should occur. The contingency plan is approved by the Security Board on an annual basis, and annual tests of the contingency plan are carried out.

## 3.6. Risk assessment

The entire operation of team.blue Denmark is at all levels governed and driven by necessary risk assessments, which are carried out on a smaller scale on a daily basis and also materialise in important overall assessments and positions on our level of security. Our risk assessment procedure consists of:

- Identification and mapping of all of the risks involved in the processing and a classification of such risks
- Assessment of what constitutes appropriate technical and organisational measures to ensure compliance with the Regulation and the documentability thereof.

Risk management is implemented in team.blue Denmark as an integral part of team.blue Denmark's processes. A risk register is continuously maintained throughout the year, containing the most significant risks to team.blue Denmark's operation of services. Risk treatment plans are defined and tracked for risks that fall outside our risk acceptance criteria. The risk register is reviewed at least annually and approved by the Security Board.

Based on the risk assessment, information security and data security policies and measures are prepared and implemented.

## 3.7. Control measures

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

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

- Data processing agreements and instructions
- Information security policies
- Organisational measures
- Data storage and deletion
- System and application access control
- Supplier service delivery management and use of subprocessors
- Incident management in case of a personal data breach.

The following have been prepared:

- Risk assessments of processing activities
- Information security and data security policies
- Awareness training of employees in protection of personal data and IT security
- Supplier management and use of subprocessors
- Information security aspects of business continuity management
- Annual cycle of periodic controls related to organisational and technical measures.

Section 4 includes the controls that are relevant to the services, which is why the following controls have been omitted: B.10, B.11, B.12, B.14, G.1, G.2 and G.3

## 3.8. Subprocessors

team.blue Denmark uses the following subprocessors:

- T1A Enterprise A/S for erasure of data and decommissioning of hardware
- B4Restore A/S for IBM Spectrum (TSM) backup services
- inMobile ApS for SMS gateway for multi-factor authentication.

## 3.9. Changes to team.blue Denmark's system during the period

During the reporting period, there were no changes to the design or operation of our system that would materially affect the suitability of the design and operating effectiveness of the controls in place to meet the stated control objectives.

## 3.10. Complementary controls at the data controllers

The data controllers have the following obligations:

- To define, establish and inform the data processor of the types of personal data and categories of personal data being processed on behalf of the controller
- To ensure the legality of instructions under the regulations in force at any time under privacy law
- To ensure that instructions are appropriate with respect to this data processing agreement and the principal service
- To ensure deletion routines.

# 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 | team.blue Denmark's standard processing agreement is applicable to customers storing personal data on team.blue Denmark's servers by using services provided by team.blue Denmark.<br>Written procedures and the standard data processing agreement require that personal data must only be processed when instructions to this effect are available.<br>Assessments are made on a regular basis as to whether the data processing agreement 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.<br>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.<br>Checked by way of inspection that procedures are up to date. | No exceptions noted. |
| A.2 | The standard data processing agreement applicable to customers and team.blue Denmark states that personal data shall only be processed on the basis of instructions from the data controller. | Checked by way of inspection that Management ensures that personal data are only processed according to instructions.<br>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 | team.blue Denmark 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.<br>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.<br>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 exist which include a requirement that agreed safeguards are established for the processing of personal data in accordance with the agreement with the data controller.<br>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.<br>Checked by way of inspection that procedures are up to date.<br>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 | team.blue has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller. | Checked by way of inspection that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security.<br>Checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data.<br>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.<br>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 clients used in the processing of personal data, anti-virus 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.<br>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.<br>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.<br>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.<br>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.<br>Checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data.<br>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 | All servers are automatically monitored for availability via the central monitoring tool.<br>Alerts are pushed to the monitoring screens placed in the operations department. | 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.<br>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 team.blue Denmark transmits confidential and sensitive personal data through the internet or by email internally. Data encryption on the service is the responsibility of the customers. | 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.<br>Checked by way of inspection that technological encryption solutions have been available and active throughout the assurance period.<br>Checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.<br>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 | **Event logging**<br>Event logging is configured for team.blue Denmark's critical, central systems.<br>**Protection of log information**<br>team.blue Denmark's central critical logs are stored at an external party and cannot be altered.<br>**Administrator and operator logs**<br>System administrator and system operator activities shall be logged in the Operations Management System. | 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.<br>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.<br>Checked by way of inspection that user activity data collected in logs are protected against manipulation or deletion.<br>Checked by way of inspection of a sample 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.<br>Checked by way of inspection of a sample of logging that documentation confirms the follow-up performed on activities carried out by system administrators and others holding special rights. | No exceptions noted. |

**Control objective B:**

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

| No. | Data processor's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.13 | A formalised procedure is in place for granting and removing privileged users' access to personal data. Privileged 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.<br>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.<br>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.<br>Checked by way of inspection that documentation states that user accesses granted are evaluated and authorised on a regular basis – and at least once a year. | No exceptions noted. |
| B.15 | Physical access safeguards have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data is 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.<br>Checked by way of inspection of documentation that, throughout the assurance period, only authorised persons have had physical access to premises and data centres at which personal data are stored and processed. | 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 team.blue Denmark has approved a written information security policy that has been communicated to all relevant stakeholders, including team.blue Denmark's employees. The IT security policy is based on the risk assessment performed.<br>Assessments are made on a regular basis as to whether the IT security policy should be updated. | Checked by way of inspection that an information security policy exists that Management has considered and approved within the past year.<br>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 team.blue Denmark has checked that the information security policy does not conflict with the applicable data processing agreement. | 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.<br>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 team.blue Denmark are screened as part of the employment process. Such screening comprises, as relevant:<br>• References from former employers<br>• Certificates of criminal record. | Checked by way of inspection that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process.<br>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.<br>Checked by way of inspection of employees appointed during the assurance period that documentation states that the screening has comprised, as relevant:<br>• References from former employers<br>• Certificates of criminal record. | 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 included in the employment contract. 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.<br>Checked by way of inspection of employees appointed during the assurance period that the relevant employees have been introduced to:<br>• The information security policy<br>• Procedures for processing data and other relevant information. | No exceptions noted. |
| C.5 | For resignations or dismissals, team.blue Denmark 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.<br>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.<br>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 team.blue Denmark'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.<br>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 exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.<br>Assessments are made on an annual basis 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.<br>Checked by way of inspection that procedures are up to date. | No exceptions noted. |
| D.2 | Enforcement of storage periods and deletion routines is solely the responsibility of the data controller. When the data controller deletes its data, it will be deleted on the platform as well. | 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.<br>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.<br>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:<br>• Returned to the data controller; and/or<br>• Deleted in accordance with the deletion procedures for the given service. | 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.<br>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 exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller.<br>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.<br>Checked by way of inspection that procedures are up to date.<br>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 | team.blue Denmark will inform the data controller of the localities, countries or regions in which the processing and storage by team.blue Denmark takes place. | Checked by way of inspection that the data processor has a complete and updated list of processing activities stating localities, countries or regions.<br>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 for supplier management exist which include requirements for the data processor when using subprocessors, including requirements for subprocessing agreements and instructions.<br>Assessments are made on a regular basis 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.<br>Checked by way of inspection that procedures are up to date. | No exceptions noted. |
| F.2 | The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller. | Checked by way of inspection that the data processor has a complete and updated list of subprocessors used.<br>Checked by way of inspection of a sample of subprocessors from the data processor's list of subprocessors that documentation states that the processing of data by the subprocessor follows from the data processing agreements – or otherwise as approved by the data controller. | 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 data from its services When changing the specially approved sub-data processors 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.<br>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 | team.blue Denmark 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.<br>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 | team.blue Denmark has a list of approved sub-data processors disclosing:<br>• Name<br>• Business registration no.<br>• Address<br>• Description of the processing. | Checked by way of inspection that the data processor has a complete and updated list of subprocessors used and approved.<br>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 | team.blue Denmark's supplier management programme includes regularly following up on subprocessors through meetings, inspections, reviews of auditor's reports or similar activities. | 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.<br>Checked by way of inspection of documentation that each subprocessor and the current processing activity at such processor are subjected to risk assessment.<br>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.<br>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 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 | The standard data processing agreement includes a requirement that the data processor must assist the data controller in relation to the rights of data subjects.<br><br>Assessments are made on a regular basis 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.<br><br>Checked by way of inspection that procedures are up to date. | No exceptions noted. |
| H.2 | team.blue Denmark has established procedures, in so far as this was agreed, that enable timely assistance to the data controller in handing out, correcting, deleting or providing information about the processing of personal data to data subjects, or restricting the processing of personal data. | Checked by way of inspection that the procedures in place for assisting the data controller include detailed procedures for:<br>• Handing out data<br>• Correcting data<br>• Deleting data<br>• Restricting the processing of personal data<br>• Providing information about the processing of personal data to data subjects.<br>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 exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches.<br>Assessments are made on a regular basis 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.<br>Checked by way of inspection that procedures are up to date. | No exceptions noted. |
| I.2 | team.blue Denmark has established the following controls to identify any personal data breaches:<br>• Awareness of employees<br>• Monitoring of systems, network traffic and malicious behaviour<br>• Logging access to systems which enable us to correlate logs in the event of an incident. | Checked by way of inspection that the data processor provides awareness training to the employees in identifying any personal data breaches.<br>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.<br>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 occurs team.blue Denmark will inform the data controller without undue delay 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.<br>Made inquiries of the subprocessors as to whether they have identified any personal data breaches throughout the assurance period.<br>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.<br>Checked by way of inspection that all personal data breaches recorded at the data processor or the subprocessors have been communicated to the data controllers concerned without undue delay after the data processor became aware of the personal data breach. | No exceptions noted. |
| I.4 | In accordance with the data processing agreement team.blue Denmark will to the extent possible assist the data controller in filing reports with the Danish Data Protection Agency:<br>• Nature of the personal data breach<br>• Probable consequences of the personal data breach<br>• 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:<br>• Describing the nature of the personal data breach<br>• Describing the probable consequences of the personal data breach<br>• Describing measures taken or proposed to be taken to respond to the personal data breach.<br>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 registreret, og informationerne er listet herunder.*

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

**Lotte Bendstrup**
**MD**
På vegne af: team.blue Denmark A/S
*Serienummer: lotte.bendstrup@team.blue*
*IP: 185.25.xxx.xxx*
*2025-03-05 14:53:05 UTC*

**Rico Lundager**
**PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231**
**Senior manager**
På vegne af: PricewaterhouseCoopers Statsautoriseret…
*Serienummer: 2e75390a-f48a-4123-b26c-3fd3e97823aa*
*IP: 80.208.xxx.xxx*
*2025-03-05 15:11:07 UTC*

**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*
*2025-03-05 15:15:40 UTC*

*Penneo dokumentnøgle: PHK16-0DQYJ-8ZS0Z-7UHUC-UYB7V-KY81V*