Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR no. 33 96 35 56
Weidekampsgade 6
2300 Copenhagen S

Phone: 36102030
www.deloitte.dk

team.blue Denmark A/S

Independent auditor's ISAE 3000 type 1 assurance report on controls for data protection and processing of personal data on behalf of customers subject to the general Data Protection Regulation (GDPR) as of 8 November 2022

Table of contents

1. Independent auditor's report

Independent auditor's ISAE 3000 assurance report on controls for data protection and processing of personal data on behalf of customers subject to the General Data Protection Regulation (GDPR)

Scope

We have been engaged to provide assurance about team.blue Denmark A/S' (hereinafter "team.blue Denmark") description in section 3 of the described services in accordance with the data processing agreements with clients as of 8 November 2022 (hereinafter "the description"), and about the design and implementation of controls related to the control objectives stated in the description.

This report does not include controls performed by sub-data processors. team.blue Denmark uses the following sub-data processors:

- Fuzion A/S:
  - Housing
  - Physical and environmental security of production environment
- GlobalConnect A/S:
  - Housing
  - Physical and environmental security of production environment
- Cibicom A/S:
  - Housing
  - Physical and environmental security of production environment
  - Storage of backup.

Additionally, team.blue Denmark uses the sub-service provider, SentinelOne, for cloud storage and reporting logic for a subset of logging and monitoring on critical platforms.

The description provided by team.blue Denmark in section 3 of this report does not include control objectives and supporting controls at the sub-data processors of team.blue Denmark.

Some of the control objectives presented in the description provided by team.blue Denmark can only be achieved if complementary controls at the clients are implemented and are working effectively. This report does not include the design, implementation and operating effectiveness of such complementary controls.

team.blue Denmark's responsibilities

team.blue Denmark is responsible for preparing the description and the accompanying assertion in section 2, including the completeness, accuracy and method of presentation of the description and the assertion; providing the services covered by the description; stating the control objectives; and designing and implementing controls to achieve the stated control objectives.

Auditor's independence and quality control

We have complied with the requirements for independence of the IESBA's Code of Ethics for Professional Accountants, which is based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct.

We are subject to the International Standard on Quality Control (ISQC 1) and accordingly use and maintain a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on team.blue Denmark's description and on the design and implementation of controls related to the control objectives stated in that description, based on our procedures.

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

An assurance engagement to report on the description, design and implementation of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its services, and the design and implementation 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 implemented. Our procedures included testing the design and implementation of controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved as per the audit date.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein and the appropriateness of the criteria specified by the data processor and described in section 2.

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

Limitations of controls at team.blue Denmark

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 control that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the controls 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 section 2 in this report. In our opinion, in all material respects:

(a) The description fairly presents the services provided as designed and implemented as of 8 November 2022;
(b) The controls related to the control objectives stated in the description were suitably designed and implemented as of 8 November 2022.

Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed in section 4 of this report.

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 services 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 EU Regulation on the protection of

natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with.

Copenhagen, 21 February 2023

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR No. 33 96 35 56

Thomas Kühn
Partner, State-Authorised Public Accountant

Michael Bagger
Partner, CISA

2. Management assertion

The accompanying description has been prepared for the customers who have used the services described in this report, 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 Regulation have been complied with.

team.blue Denmark confirms that:

a) The accompanying description in section 3 fairly presents the system for processing personal data for data controllers covered by the General Data Protection Regulation as of 8 November 2022. The criteria used in making this statement were that the accompanying description:

(i) Presents how the services delivered were designed and implemented, including:

- The types of services provided, including the type of personal data processed;
- The processes in both IT and manual systems that are used for initiating, registering, processing and, if necessary, correcting, deleting and restricting processing of personal data;
- The processes used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller;
- The processes ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
- The processes which, on termination of data processing, ensure that, according to the data controller's choice, all personal data can be deleted or returned, unless law or regulation prescribes retention of personal data;
- The processes which, in the event of a personal data breach, support the data controller in reporting to the supervisory authority and notifying the data subjects of the breach;
- The processes which ensure appropriate technical and organisational security measures for the processing of personal data, taking into account the risks involved in processing, in particular, by accidental or illegal destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed;
- Controls which we, referring to the system, assumed would be designed and implemented by the data controller and which, if necessary to achieve the control objectives set forth in the description, are identified in the description;
- Other aspects of our control environment, risk assessment process, information system (including related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data.

(ii) Contains relevant information about changes in the data processor's services in the processing of personal data made as of 8 November 2022.

(iii) Does not omit or distort information relevant to the scope of the system described for the processing of personal data, taking into consideration that the description was prepared to meet the general needs of a wide range of data controllers and therefore cannot include any aspect of the system that the individual data controller might consider important according to their particular circumstances.

b) The controls associated with the control objectives listed in the accompanying description were appropriately designed and implemented as of 8 November 2022. The criteria used in making this statement were that:

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

(ii) The controls identified would, if carried out as described, provide a high level of assurance that the risks involved did not prevent the achievement of the control objectives stated.

c) Appropriate technical and organisational measures have been established and maintained to fulfil the agreements with the data controller, good data processing practices and relevant data processing requirements under the General Data Protection Regulation.

Copenhagen, 21 February 2023

On behalf of team.blue Denmark A/S

Lotte Bendstrup
MD

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.
- Sub-processors are only being used based on a general approval from the data controller and upon prior notification of the use of a new sub-processor.
- 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 CPR number	Racial or ethnic origin Political, religious or philosophical beliefs Trade union membership Data concerning health Information revealing sex life or sexual orientation 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, 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 ISO27001, 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 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 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 sub-processors
- 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 sub-processors
- Information security aspects of business continuity management

- Annual cycle of periodic controls related to organisational and technical measures.

3.8 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
- That instructions are appropriate with respect to this data processing agreement and the principal service
- To ensure deletion routines.

4 team blue Denmark's control objectives, controls, test and results

Introduction

This report is intended to provide the data controllers with information about the controls at team.blue Denmark that may affect the processing of personal data, and to provide the data controllers with information about the design and implementation of the controls that were tested.

This report, when combined with an understanding and assessment of the controls at the data controllers, is intended to assist the data controllers in assessing the risks related to the processing of personal data that may be affected by the controls at team.blue Denmark.

Our testing of team.blue Denmark's controls was limited to the control objectives and related controls listed in the matrices in this section of the report and did not include all controls described in the system description, nor controls that may be in place at the data controllers. It is the responsibility of the data controllers to evaluate this information in relation to the controls in place at each data controller. If certain complementary controls are not in place at the data controller, team.blue Denmark's controls may not compensate for such weaknesses.

team.blue Denmark's system description does not include control objectives and associated controls at the sub-service organisation. team.blue Denmark uses the following sub-suppliers to deliver physical and environmental security of production environments and storage of backup.

- Fuzion A/S:
  - Housing
  - Physical and environmental security of production environment
- GlobalConnect A/S:
  - Housing
  - Physical and environmental security of production environment
- Cibicom A/S:
  - Housing
  - Physical and environmental security of production environment
  - Storage of backup.

Additionally, team.blue Denmark uses the sub-service provider, SentinelOne, for cloud storage and reporting logic for a subset of logging and monitoring on critical platforms.

The data controller should assess whether obtaining audit report's from sub-data processors is relevant to be able to make an overall assessment of whether all necessary controls are in place in relation to the overall control environment.

Test of controls

The test of controls performed involves one or more of the following methods:

Method	Description
Interview	Interviews with selected personnel at team.blue Denmark.
Observation	Observation of the execution of controls.
Inspection	Review and evaluation of policies, procedures and documentation of the performance of the control. This includes reading and evaluating reports and other documentation to assess whether specific controls are designed and implemented. Furthermore, it is assessed whether controls are monitored and supervised adequately and at appropriate intervals.
Re-performance	Repetition of the relevant control to verify that the control functions as intended.

Control objectives, controls and test results

The following matrices state the control objectives and controls tested and present the audit procedures performed and the results thereof. If we identified material control weaknesses, we have described them as well.

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.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
A.1	team.blue Denmarks standard processing agreement is applicable to customers storing personal data on team.blue Denmark's servers by using services provided by team.blue Denmark. Written procedures and the standard data processing agreement require that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis as to whether the data processing agreement should be updated.	Deloitte has checked by way of inspection that formalised procedures exist to ensure that personal data is only processed according to instructions. Deloitte has 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. Deloitte has 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.	Deloitte has checked by way of inspection that Management ensures that personal data is only processed according to instructions. Deloitte has inspected a sample of one data processing agreement and checked that processing of personal data takes place in accordance with instructions.	No exceptions noted.
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.	Deloitte has checked by way of inspection that formalised procedures exist ensuring verification that personal data is not processed against the Regulation or other legislation. Deloitte has 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 in breach of legislation.	No exceptions noted.

Control objective B

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

No.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
B.1	Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Deloitte has checked by way of inspection that formalised procedures are in place to ensure establishment of the agreed safeguards. Deloitte has checked by way of inspection that procedures are up to date. Deloitte has checked by way of inspection that the agreed safeguards have been established for a sample of one data processing agreement.	No exceptions noted.
B.2	team.blue Denmark 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.	Deloitte has 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. Deloitte has checked by way of inspection that the risk assessment performed is up to date and comprises the current processing of personal data. Deloitte has checked by way of inspection that the data processor has implemented technical measures ensuring an appropriate level of security consistent with the risk assessment. Deloitte has checked by way of inspection that the data processor has implemented the safeguards 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.	Deloitte has checked by way of inspection that, for the systems and databases used in the processing of personal data, anti-virus software has been installed. Deloitte has checked by way of inspection that anti-virus software is up to date.	No exceptions noted.

No.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	Deloitte has 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. Deloitte has 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.	Deloitte has inquired whether internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data. Deloitte has checked by way of inspection whether internal networks are segmented to ensure limited access to systems and databases processing personal data.	No exceptions noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	Deloitte has checked by way of inspection that formalised procedures are in place for restricting users' access to personal data. Deloitte has 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 needs. Deloitte has checked by way of inspection that the technical measures agreed support retaining the restriction in users' work-related access to personal data. Deloitte has inspected documentation of performed reviews of user access performed in the period.	No exceptions noted.

No.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
B.7	All servers are automatically monitored for availability via the central monitoring tool. Alerts are pushed to the monitoring screens placed in the operations department.	Deloitte has checked by way of inspection that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. Deloitte has checked by way of inspection that, in a sample of one alarm, follow-up action had been taken and that the data controllers were informed thereof as appropriate.	No exceptions noted.
B.8	Effective encryption is applied when team.blue Denmark is transmitting confidential and sensitive personal data through the internet or by email internally. Data encryption on the service is the responsibility of the customers.	Deloitte has 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. Deloitte has checked by way of inspection that technological encryption solutions have been available and active throughout the assurance period. Deloitte has checked by way of inspection that encryption is applied when transmitting confidential and sensitive personal data through the internet.	No exceptions noted.
B.9	**Event logging** Event logging is configured for team.blue Denmark's critical, central systems. **Protection of log information** team.blue Denmark's central critical logs are stored at an external party and cannot be altered. **Administrator and operator logs** System administrator and system operator activities shall be logged in the Operations Management System.	Deloitte has checked by way of inspection that logging has been activated as described. Deloitte has checked by way of inspection that user activity data collected in logs is protected against manipulation or deletion.	No exceptions noted.

No.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
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.	Deloitte has checked by way of inspection that formalised procedures exist for granting and removing users' access to systems and databases used for processing personal data. Deloitte has inspected a sample of one user provision to systems and databases and checked that the user access granted had been authorised, and that a work-related need exists. Deloitte has inspected a sample of one resigned employee and checked that the access to systems and databases was deactivated or removed timely. Deloitte has checked by way of inspection that documentation exists that user access granted is evaluated and authorised on a regular basis.	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.	Deloitte has checked by way of inspection that formalised procedures exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. Deloitte has 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 ensure relevant security of processing.

No.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
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. Assessments are made on a regular basis as to whether the IT security policy should be updated.	Deloitte has checked by way of inspection that an information security policy exists which the management has considered and approved within the past year. Deloitte inspected documentation that the information security policy has been communicated to relevant stakeholders, including team.blue Denmark'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.	Deloitte inspected documentation showing Management of team.blue Denmark 's assessment of the information security policy, and that the policy generally meets the requirements for safeguarding data in relation to the data processing agreements entered into. Deloitte inspected a sample of one data processing agreement and checked that the requirements are covered by the requirements in the information security policy for safeguards 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: • References from former employers; • Certificates of criminal record;	Deloitte has 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. Deloitte has checked by way of inspection a sample of one employee appointed during the assurance period that documentation exists of the screening, comprising: • Certificates of criminal record	No exceptions noted.
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.	Deloitte inspected a sample of one employee recruitment in the period and checked that a confidentiality agreement was signed. Deloitte inspected a sample of one new employee and checked that the employee had been introduced to:	No exceptions noted.

No.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
		• The information security policy; • Procedures for processing data and other relevant information.	
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.	Deloitte inspected procedures ensuring that user access rights of terminated employees are deactivated upon resignation or dismissal, and that assets, such as access cards, computers, mobile phones, etc., are returned. Deloitte inspected a sample of one resigned employee and checked 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.	Deloitte inspected a sample of one resigned employee and observed that they have been notified of the continued validity of the confidentiality agreement and the general duty of confidentiality.	No exceptions noted.
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.	Deloitte has checked by way of inspection that team.blue Denmark provides awareness training to the employees covering general IT security and security of processing related to personal data.	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.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on an annual basis as to whether the procedures should be updated.	Deloitte has 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. Deloitte has checked by way of inspection that the 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 their data, it will be deleted on the platform as well.	Deloitte has checked by way of inspection that procedures for storage and deletion exist. Deloitte inspected a sample of data processing sessions from the data processor's list of processing activities and checked that documentation exists and that personal data is stored in accordance with the agreed storage periods. Deloitte inspected a sample of data processing sessions from the data processor's list of processing activities and checked that documentation exists and that personal data is 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 in accordance with the deletion procedures for the given service.	Deloitte has 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. Deloitte inquired about the latest terminated data processing sessions and checked by way of inspection that the deletion of data was performed as stated in the data processing agreement.	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.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
E.1	Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	Deloitte has checked by way of inspection that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. Deloitte has checked by way of inspection that the procedures are up to date. Deloitte inspected a sample of one data processing session from the data processor's list of processing activities and checked that documentation exists 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.	Deloitte has checked by way of inspection that team.blue Denmark has a complete and up-to-date list of processing activities stating localities, countries or regions. Deloitte inspected a sample of one data processing session from team.blue Denmark's list of processing activities and checked that documentation exists that the processing of data, including the storage of personal data, only takes place 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 sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

No.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
F.1	Written procedures for supplier management exist which include requirements for the data processor when using sub-processors, including requirements for sub-processing agreements and instructions. Assessments are made on a regular basis as to whether the procedures should be updated.	Deloitte has checked by way of inspection that formalised procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions. Deloitte has 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.	Deloitte has checked by way of inspection that the data processor has a complete and up-to-date list of sub-data processors used. Deloitte has checked by way of inspection of a sample of one sub-data processor from the data processor's list of sub-data processors that documentation exists that the processing of data by the sub-data processor is stated in the data processing agreements – or otherwise as approved by the data controller.	No exceptions noted.
F.3	When changing the generally approved sub- processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw data from their services When changing the specially approved sub-data processors used, this has been approved by the data controller.	Deloitte has checked by way of inspection that formalised procedures are in place for informing the data controller when changing the sub-data processors used. Inspected documentation that the data controller was informed when changing the sub-data processors used throughout the assurance period.	No exceptions noted.
F.4	team.blue Denmark has subjected the sub-processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	Deloitte has checked, by way of inspection, for existence of signed sub-data processing agreements with sub-data processors used which are stated on the data processor's list. Deloitte has checked by way of inspection of a sample of one sub-data processing agreement that it includes the same requirements and obligations as those stipulated in	No exceptions noted.

No.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
		the data processing agreements between the data controllers and the data processor.	
F.5	team.blue Denmark has a list of approved sub-data processors disclosing: • Name; • Business Registration No.; • Address; • Description of the processing.	Deloitte has checked by way of inspection that the data processor has a complete and up-to-date list of sub-data processors used and approved. Deloitte has checked by way of inspection that, as a minimum, the list includes the required details about each sub-data processor.	No exceptions noted.
F.6	team.blue Denmark's supplier management programme include regularly following up on sub-processors through meetings, inspections, reviews of auditor's reports or similar activity.	Deloitte has checked by way of inspection that formalised procedures are in place for following up on processing activities at sub-data processors and compliance with the sub-data processing agreements. Deloitte has checked by way of inspection of documentation that each sub-data processor and the current processing activity at such processor are subjected to risk assessment. Deloitte has checked by way of inspection of documentation that technical and organisational measures and security of processing at the sub-data processors used are appropriately followed up on. Deloitte has checked by way of inspection of documentation that information on the follow-up at sub-data processors 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.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
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. Assessments are made on a regular basis as to whether the procedures should be updated.	Deloitte has 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. Deloitte has checked by way of inspection that the procedures are up to date and assessments are planned on an annual basis.	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: • 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 that requests by the data controller for assistance in handing out, correcting, deleting or providing information about the processing of personal data to data subjects, or restricting the processing of personal data, have been documented in a correct and 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.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
I.1	Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis as to whether the procedures should be updated.	Deloitte has 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. Deloitte has checked by way of inspection that procedures are updated on an annual basis.	No exceptions noted.
I.2	team.blue Denmark has established the following controls to identify any personal data breaches: • Awareness of employees; • Monitoring of systems, network traffic and malicious behaviour; • 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. 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 a timely basis.	No exceptions noted.
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 sub-processor.	Deloitte has checked by way of inspection that guidelines for informing the data controllers in case of a breach exist. We have inquired about breach of personal data security in the audit period.	No exceptions noted.

No.	team.blue Denmark's control activity	Test performed by Deloitte	Results of Deloitte's test
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: • 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.	Deloitte has checked by way of inspection that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for: • Describing the nature of the personal data breach; • Describing the probable consequences of the personal data breach; • Describing the measures taken or proposed to be taken to respond to the personal data breach. Deloitte has 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.

LIJA/ABP
T:\Afd1180\team.blue\2023\team.blue 3000 – Independent Auditor's Report – FINAL 210223