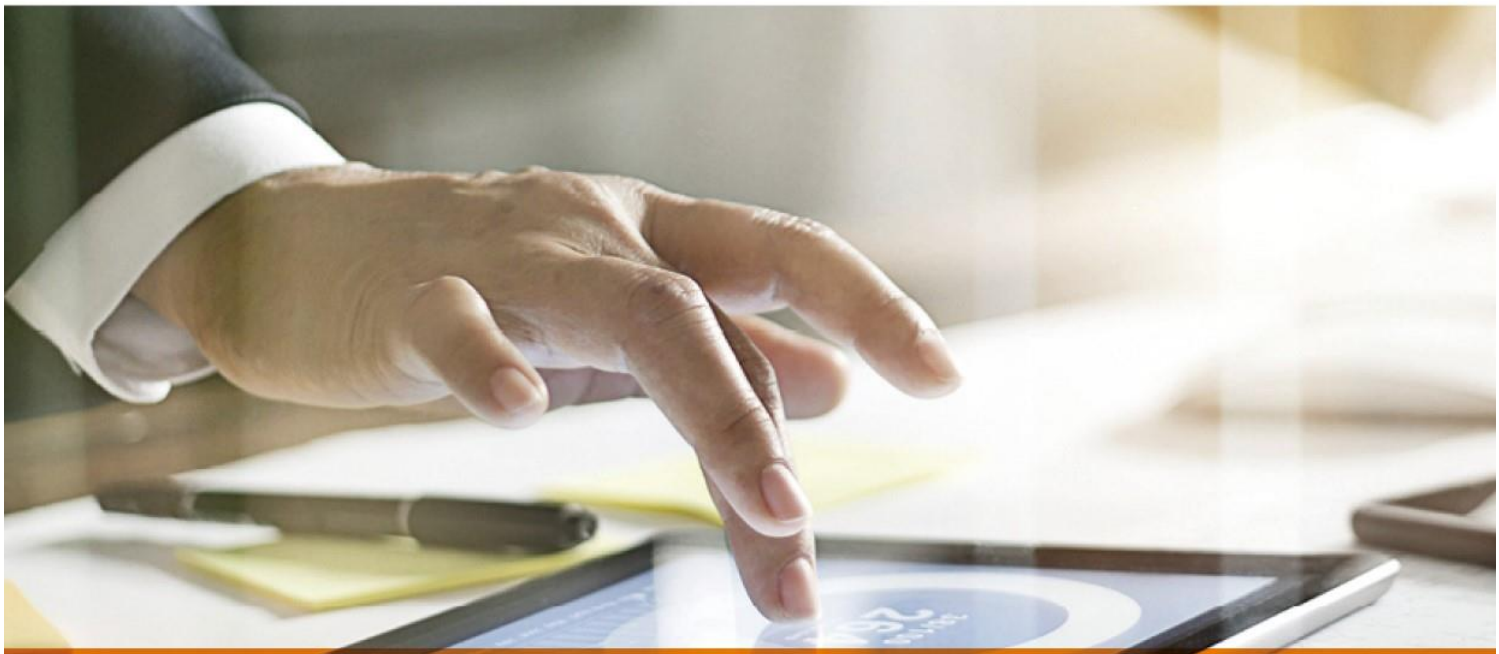
BEIERHOLM
VI SKABER BALANCE



JANUARY 2024

GLOBALCONNECT OUTSOURCING SERVICES OF GLOBALCONNECT A/S

ISAE 3000 TYPE 2 ASSURANCE REPORT

Independent Auditor's ISAE 3000 Report on information security and data protection measures in relation to Data Processor Agreement with Data Controllers.

Beierholm
State Authorized Public Accountants
Copenhagen
Knud Højgaards Vej 9
DK-2860 Søborg
Denmark
CVR no. DK 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

Structure of the Assurance Report

Chapter 1:
Letter of Representation.

Chapter 2:
Independent Auditor's Assurance Report.

Chapter 3:
Description of the control environment for the operation of GlobalConnect Outsourcing Solutions.

Chapter 4:
Auditor’s description of control objectives, security measures, tests, and findings.

Chapter 5:
Supplementary information provided by GlobalConnect.

CHAPTER 1:

Letter of Representation

GlobalConnect A/S processes personal data in relation to GlobalConnect Outsourcing Services to our Customers, who are controllers according to the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions (the Danish Data Protection Act).

The accompanying description has been prepared for the use of customers and their auditors, who have used the GlobalConnect Outsourcing Services from GlobalConnect, and who have sufficient understanding to consider the description along with other information, including information about controls operated by the customers i.e. the Data Controllers themselves, when assessing, whether the demands to the control environment as well as requirements laid down in the General Data Protection Regulation are complied with.

GlobalConnect A/S uses a sub-processor for backup. This sub-processor's relevant control objectives and related technical and organisational measures and other controls are not included in the accompanying description (partial method).

Furthermore, the Data Center department at GlobalConnect A/S is service sub-organisation in relation to the physical security in the data centers from which GlobalConnect Outsourcing Services are operated. The description does not include control objectives and controls managed by the Data Center department and thus includes solely control objectives and controls relating to processes and procedures managed by GlobalConnect Outsourcing Services (partial method).

GlobalConnect A/S hereby confirms that

(A) The accompanying description, Chapter 3, gives a true and fair description of GlobalConnect A/S control environment in relation to GlobalConnect Outsourcing Services, which has processed personal data covered by the General Data Protection Regulation as of 1 January to 31 December 2023. The criteria for this assertion are that the following description:

(i) Gives an account of how the controls were designed and implemented, including:

- The types of services delivered, including the type of personal data processed
- The processes in both IT and manual systems that are used to initiate, record, process and, if necessary, correct, erase and limit the processing of personal data
- The processes utilized to secure that the performed data processing was conducted according to contract, directions, or agreements with the customer i.e., the Data Controller
- The processes securing that the persons authorized to process personal data have pledged themselves to secrecy or are subject to relevant statutory confidentiality
- The processes securing that - at the Data Controller's discretion - all personal data are erased or returned to the Data Controller, when the data processing is finished, unless personal data must be stored according to law or regulation
- The processes supporting the Data Controller's ability to report to the Supervisory Authority as well as inform the Data Subjects in the event of personal data security breaches

- The processes ensuring appropriate technical and organizational security measures for processing personal data taking into consideration the risks connected to processing, in particular accidental or illegal actions causing destruction, loss, change, unauthorized forwarding of or access to personal data that is transmitted, stored or in other ways processed
- Control procedures, which we assume – with reference to the limitations of the GlobalConnect Outsourcing Services – have been implemented by the Data Controllers and which, if necessary, to fulfil the control objectives mentioned in the description, have been identified in the description
- Other aspects of our control environment, risk assessment process, information system (including the accompanying work routines) and communication, control activities and monitoring controls relevant for processing of personal data

(ii) Includes relevant information about changes in GlobalConnect Outsourcing Services in relation to processing of personal data performed as of 1. January to 31 December 2023

(iii) Does not omit or misrepresent information relevant for the scope of the controls described, taking into consideration that the description has been prepared to meet the common needs of a broad range of customers and their auditors, and may not, therefore, include every aspect of the control system that each individual customer may consider important in their own particular environment.

(B) The controls related to the control objectives stated in the accompanying description were suitably designed as of 1 January to 31 December 2023. The criteria for this assertion are that:

(i) The risks threatening the fulfilment of the control objectives mentioned in the description were identified

(ii) The identified controls would, if used as described, provide reasonable assurance that the risks in question would not prevent the fulfilment of the said control objectives

(C) Appropriate technical and organizational security measures are established in order to honour the agreements with the Data Controllers, compliance with generally accepted data processor standards and relevant demands to Data Processors according to the General Data Processing Regulation.

Copenhagen, 30 January 2024

GlobalConnect A/S

Monika Juul Henriksen

Head of B2B DK and CEO DK

CHAPTER 2:

Independent auditor's ISAE 3000 assurance report on information security and data protection measures in relation to Data Processor Agreement with GlobalConnect A/S customers

For GlobalConnect A/S and relevant data controllers

Scope

We were engaged to report on GlobalConnect A/S' (Processor) description in chapter 3 of GlobalConnect Outsourcing Services and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the Regulation of the European Parliament and of the Council on protection of natural persons with regard to processing of personal data and on the free movement of such data (EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions to the Regulation (Danish Data Protection Act), and on the design and operating effectiveness of the technical and organisational measures and other controls relating to the control objectives stated in the description, throughout the period from 1 January to 31 December 2023.

We express our opinion with reasonable assurance.

The report is based on a partial approach, which means that the present report does not include the IT security controls and control activities related to the use of external business partners. The report does not include control or supervision of subcontractors in relation to Outsourcing Service activities. GlobalConnect A/S' subcontractors are listed in the Data Processing Agreements with the customers.

The scope of our report does not cover customer-specific conditions, and the report does not include the complementary controls and control activities conducted by the user company; see the description of the company in Chapter 3.

GlobalConnect's responsibility

GlobalConnect is responsible for the preparation of the description and accompanying assertion in Chapter 3, including the completeness, accuracy and method of presentation of the description and assertion; for providing the services covered by the description; for stating the control objectives; and for designing and implementing controls to achieve the stated control objectives.

Beierholm's independence and quality management

We have complied with the requirements of independence and other ethical requirements laid down in FSR's Ethical Rules based on fundamental principles of integrity, objectivity, professional competence and requisite care, confidentiality, and professional conduct.

We apply ISQM 1 and thus sustain a comprehensive system of quality management, including documented policies and procedures for compliance with ethical rules, professional standards as well as requirements in force under existing laws and additional regulation.

Auditor's responsibility

Our responsibility is to express an opinion, based on our procedures, on GlobalConnect's description and on the design and implementation of controls related to the control objectives stated in the said description. We have conducted our engagement in accordance with ISAE 3000, Other assurance reports than audit or review of historical financial statements and additional requirements according to Danish audit regulation. The standard requires that we comply with ethical requirements and that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and whether the controls in all material aspects are appropriately designed.

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 their system, and about the design of controls. The procedures selected depend on the judgement of the data processor's auditor, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or implemented.

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 and described by GlobalConnect in Chapter 3. We have not performed procedures regarding the operating effectiveness of controls included in the description and express no opinion thereof.

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

Limitations of controls at GlobalConnect

GlobalConnect's description is prepared to meet the common needs of a broad range of customers and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment. Moreover, because of their nature, controls at GlobalConnect may not prevent or detect all breaches of personal data security.

Opinion

Our opinion is based on the matters outlined in this report. The criteria on which our opinion is based are those described in Chapter 1 under Letter of Representation. In our opinion,

a) The description presents fairly GlobalConnect Outsourcing Services and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act, as designed and implemented, throughout the period from 1 January to 31 December 2023.
b) The technical and organisational measures and other controls, relating to the control objectives stated in the description were appropriately designed throughout the period from 1 January to 31 December 2023.
c) The technical and organisational measures and other 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 to 31 December 2023.

Description of tests of controls

The specific controls tested, and the nature, timing and findings of those tests are listed in Chapter 4.

Intended users and purpose

This report and the description of the test of controls in Chapter 4 are solely intended for GlobalConnect's customers and their auditors, who have sufficient understanding to consider them along with other information, including information about the customers' own control measures, which the Data Controllers themselves have performed, when assessing whether the control environment is appropriate and there is compliance with the requirements of General Data Protection Regulations.

Søborg, 30 January 2024

Beierholm
State Authorized Public Accountants
CVR 32 89 54 68

Kim Larsen
State-authorized Public Accountant

Peter Nicolai Riis
IT-auditor

CHAPTER 3

GLOBALCONNECT A/S' DESCRIPTION

GENERAL DESCRIPTION OF GLOBALCONNECT

GlobalConnect A/S (GlobalConnect), part of Nordic Connectivity AB, is a provider of Dark Fiber solutions, Transmission solutions, Outsourcing Services, including Cloud services, and Data Center solutions in Denmark to several national and international private and public companies.

This description is prepared with the purpose of reporting on the general controls which GlobalConnect Outsourcing Services (GCOS) applies to support and safeguard IT, Outsourcing and Cloud Services to its customers. The description focuses on business-related control objectives and processes implemented.

The Data Center department at GlobalConnect A/S is service sub-organisation in relation to the physical security in the data centers from which GCOS is operated. This description does not include control objectives and controls managed by the Data Center department.

DESCRIPTION OF GLOBALCONNECT OUTSOURCING SERVICES

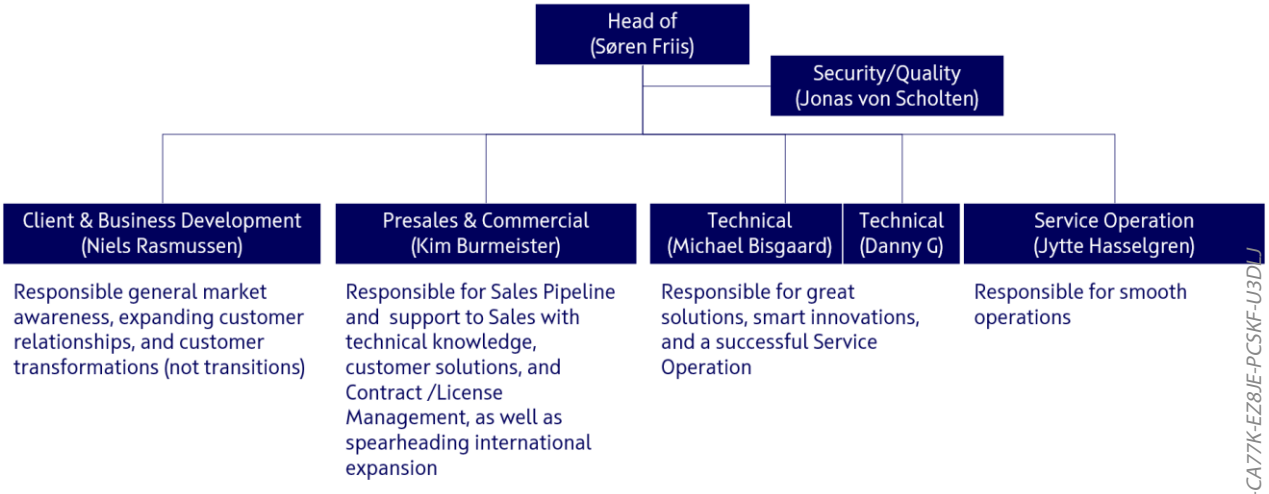
GlobalConnect Outsourcing Services (GCOS) has since 2001 specialised in providing IT outsourcing and IT services to a wide range of public and private businesses in the Danish market. As a medium-sized provider, servicing both small, medium, and large companies, GCOS has been able to maintain a unique focus on supporting our customers' ability to operate an effective business in a public or private context, with a focus on stability, cost efficiency, scalability, and operational reliability. GCOS has throughout the years had a unique focus on customer satisfaction by means of quality assurance.

GCOS has implemented a quality management system based on the requirements in ISO 9001:2015, which aims at continuously enhancement of the quality of all deliveries. This means that all parts of the delivery process are subject to quality assurance; from appointment of suppliers, over internal policies for i.e., staff, compliance with all relevant public authority and regulatory requirements, to the quite central ITIL-based operating processes.

As a specialised outsourcing/cloud-partner GCOS' principal duty is to provide stable and secure 24/7 operations and maintenance practice, this means that GCOS delivers at the agreed service levels, and that the business relationship with GCOS contributes actively to value creation and technological development for GCOS' customers. GCOS' customers will have access to "critical mass" in the form of expert technological operations, expert knowledge, processes, and security. GCOS' customers may thus focus their resources on their core business.

GENERAL DESCRIPTION OF GLOBALCONNECT OUTSOURCING SERVICES' ORGANISATION

GCOS has several high tier partnerships with several significant technology vendors. Some of these are Microsoft CSP Gold Partner, VMware VCPP (VMware Cloud Provider Program) and Dell Platinum Partnership. GCOS' staff have relevant certifications within ITIL, and the technologies provided to GCOS customers. Following organisational chart shows GCOS' formal organisation of functions:



RISK MANAGEMENT OF GLOBALCONNECT OUTSOURCING SERVICES

A risk assessment is carried out periodically, or at least once every year, and input for this assessment is obtained from all levels in the organisation and by regulatory and public authority requirements. The process is facilitated by a quality and security committee consisting of executive staff from relevant departments. The assessment is presented to the company's senior management for approval. A contingency plan is also prepared annually which reflects the existing threat scenario.

Risks are assessed and managed at tactical and operational level. In practice, risk assessments are an explicit element of several of our ITIL-based operating processes and we record potential security-related incidents caused by both external and internal conditions in our Servicedesk system for the purpose of a subsequent analysis.

Risk assessments are based on the implementation guidelines in the international standard ISO 27005.

The likelihood and consequence of the threats are (re)assessed based on the information existing at the time of the assessment. This reflects, in combination, the threat level. When the threat level has been determined, it is assessed to which extent the security environment considers the relevant threat level and, from where, it can be assessed, what the level of residual risk is.

GCOS has a formal process for management of risks which result in specific action plans. The action plans are allocated and addressed according to the adopted risk treatment procedure.

The day-to-day Management of GCOS decides based on the risk assessment whether an identified risk can be accepted, is to be mitigated or whether insurance is required based on selected risks.

When using external service providers in the processing of personal data, risk assessment for the services provided by the service provider is performed as part of the vendor selection and evaluation process, to support the overall risk assessment and the accompanying mitigating factors.

This report only includes controls and control objectives for processes and controls that are managed by GCOS, it does not include controls or control objectives that are managed by sub-organizations or parts of shared processes, regarding those parts that are managed outside GCOS.

MANAGEMENT OF PERSONAL DATA SECURITY

GCOS is certified according to the international standard ISO 27001 and has implemented an Information Security Management System (ISMS) in accordance with the requirements of the standard.

GCOS has set up requirements for an ISMS, so that this is managing the processing of personal data. This is supported by data processing agreements with the data controllers in which relevant requirements for processing personal data according to the General Data Protection Regulation and the Danish Data Protection Act are described.

The technical and organisational measures and other controls for protection of personal data are designed according to risk assessments and are implemented to ensure confidentiality, integrity, and accessibility as well as compliance with applicable data protection legislation. Security measures and controls are, to the extent possible, automated, and technically supported by IT systems.

The management of the personal data security and technical and organisational measures and other controls are organised in the following main areas for which control objectives and control activities have been defined:

ISO 27001	Control activities	GDPR article
Risk assessment	• Risk assessment	• Art. 28(3)(c)
A.5: Information security policies	• Information Security Policy • Personal Data Policy • Review of policies	• Art. 28(1)
A.6: Organisation of information security	• Roles and responsibilities • Remote workplaces and mobile equipment • Authentications of external connections	• Art. 28(1) • Art. 28(3)(c)
A.7: Human resource security	• Before employment • During employment • GDPR awareness • Non-disclosure and confidentiality agreements • End or change of employment	• Art. 28(1) • Art. 28(3)(b)

ISO 27001	Control activities	GDPR article
A.8: Asset management	• Record of assets • Record of categories of processing activities • Ownership of assets • Classification of assets • Classification of information	• Art. 30(2), (3) & (4)
A.9: Access management	• Policy for access management • Access to network services • User registration and deregistration • Management of access rights • Management of privileged access rights • Management of password requirements	• Art. 28(3)(c)
A.10: Cryptography	• Administration of keys	• Art. 28(3)(c)
A.11: Physical and environmental security	• Physical perimeter safety guarding • Physical access control	• Art. 28(3)(c)
A.12: Operations security	• Operations security procedures • Change management • Capacity management • Separation of development, test, and operation environments • Backup • Incident logging • Administrator and operator logs • Time synchronisation	• Art. 28(3)(c)
A.13: Communication security	• Policies and procedures for transfer of information	• Art. 28(3)(c)
A.14: Acquisition, development, and maintenance of systems	• System acquisition, development, and maintenance of systems	• Art. 25
A.15: Supplier relationships	• Agreements with sub-processors • Approved sub-processors • Supervision of sub-processors	• Art. 28(2) & (4)
A.16: Information security incident management	• Handling of information and personal data security incidents • Reporting of information and personal data security incidents	• Art. 33(2)
A.17: Information security aspects of disaster recovery, contingency and restore management	• Disaster recovery • Security continuity • Restore management	• Art. 28(3)(c)
A.18: Compliance	• Identification of applicable legislation • Data protection agreements with customers • Instruction from customers • Assistance to the customers • Deletion and return of customers data • Independent review of controls	• Art. 28(3)(a), (c), (e)-(h) • Art. 29 • Art. 32(4) • Art. 28(10)

Description of data processing

GCOS provides a technical platform to organisations and companies within the public as well as the private sector.

The platform allows the customer to provision virtual resources in configurations, such as servers and appliances, to support the needs and requirements of their respective businesses.

GCOS has, as a general rule, no knowledge of what workloads and what data is processed, for each configured set of resources, on the platform.

Customers can enter agreements with GCOS, so that GCOS and its employees, may access customer resources to provide management and support for provisioned services.

All processing of personal data is governed by formally documented policies and procedures. All documents are subject to periodic evaluation to ensure compliance with relevant legislation.

The processing of personal data may, under certain circumstances, be outsourced to sub-processors, with whom GCOS has established data processing agreements.

All sub-processors used are declared in any data processing agreement between GCOS and its customers.

Any changes are, as per the data processing agreement, announced reasonable time in advance.

Personal Data

All processing of personal data is governed by the data processing agreements with the data controller.

Depending on the specific data processing agreement, the processing of data may include general personal data, and in some cases additionally special categories of personal data.

Categories of registered persons covered by the data processing are subject to the agreement with the data controller and the nature of the service provided.

Control objectives

To support our role as a data processor, GCOS has designed and implemented controls in support of our GDPR compliance.

Procedures and controls implemented are further described below.

Control objective A - Instructions regarding processing

Procedures and controls are complied with, ensuring that instructions regarding the processing of personal data are complied with in accordance with the data processing agreement.

A data privacy policy is prepared and governs all processing of personal information.

Furthermore, a comprehensive data processing agreement template including detailed appendixes must be prepared and completed for each instance of business relationships where GCOS acts as a data processor.

The data processing agreement serves as the basis for the data processing with additional specific instructions by the data controller.

All data processing agreements are stored electronically in a central repository.

The Contract Management team performs controls that data processing agreements contains markings in the required sections prior to entering the contract information into the Contract management system.

Control objective B - Technical security measures

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

Asset management

GCOS has implemented controls to ensure achievement and maintenance of suitable protection of the organisation's equipment.

Registration of equipment
Relevant equipment, which is utilised, is registered in GCOS' CMDB in service desk system, in which all changes are also registered.

Management of removable media
The rules for use of removable media is contained in the classification system described in the general information security policies, and in GCOS' information security rules.

Procedures for information management
Processing of data follows the guidelines set out in the classification system for GCOS.

Access management

GCOS has implemented controls to ensure that access to systems and data are granted through a documented process in accordance with a work-related need and is rescinded when the relevant access is no longer necessary.

Procedure for access control
As a supplement to our security policy and rules, GCOS has a formal procedure for access management.

Account provisioning
GCOS has procedures for the provisioning and deprovisioning user accounts, which are placed in our service desk system in the form of workflows.

Extended rights
All rights are managed based on the employees' roles and are checked regularly in our quality management system. Extension of standard rights follows our formal access management procedure.

Management of password
Granting of passwords is subject to several rules which are set out in our identity management systems.

Reassessment of user access rights
All accesses and rights are reviewed periodically by the security manager and the GCOS department managers.

User identification and authentication
GCOS has separate admin-profiles for all operational staff on the systems where this is technically possible. All password validation is made via Password Manager systems which manages validation of the individual logins.
Authentication must leverage MFA wherever possible.

Cryptography

GCOS has implemented controls to ensure correct and effective use of cryptography to protect confidentiality, authenticity and/or integrity of data.

In transit
Backup data, sent via dedicated lines to the organisation, are secured by one or more encryption keys.

GCOS performs hardening of encryption configuration through use of best practice baselines wherever possible. Exposed services are monitored for weak configurations.

Physical security

GCOS has implemented controls to ensure that IT equipment is properly protected against unauthorised physical access and environmental incidents.

Physical access control
Safeguarding of offices, premises, and facilities
GlobalConnect premises have access control in the form of a required personal code and a physical access token, e.g., Chipcard, to ensure that only authorised staff have access.

Protection against physical external threats
We refer to a separate ISAE 3402 report on the description of controls, their design and operating effectiveness relating to GlobalConnect's Data Center solution.

Storing of equipment and protection of equipment
Critical equipment is placed in a server room to which only technical staff and GlobalConnect's partners have access.

Backup of information

Backup is performed for all important data according to the backup requirements related to data classifications, and on customer systems according to customer agreements made. Errors in backup are identified by the relevant backup management tools and registered in GCOS' service desk. Restore test are carried out on a monthly basis.

Logging and monitoring

GCOS has implemented controls to ensure that relevant logs are collected, monitored, and stored in suitable systems

Audit log

User transactions, exceptions and security incidents are logged, and the log is stored according to the retention periods set out in the company policy or as agreed with the customer.

Use of monitoring systems

GCOS has implemented internal procedures to ensure that alerts and alarms are addressed to respond to relevant incidents and act accordingly. All alarms are monitored and reviewed continuously by GCOS' operations department and are reported to customers because cases are created on the basis hereof.

Logging of administrator and operator

System administrators' actions are logged automatically in our service desk system and relevant log-collection solutions as applicable by a specific system or platform.

Logging of errors

Monitoring has been set up for the purpose of future analysis of errors and incidents in our service desk.

Patch management

GCOS has implemented controls to ensure that systems receive relevant patches and security updates in a timely fashion as updates and patches are provided by the respective software vendors.

Scheduled updates

Security patches are applied at fixed intervals in the service windows agreed respectively with the system owner or the customers. All other Major upgrades, i.e service packs and similar are installed solely at request, or by approval by the system owner or customer respectively, following a recommendation by GCOS, and follows the process in our service desk system in the form of formalised workflows.

Control of technical vulnerabilities

Scanning for updates to systems is done using software tools. Hereafter, GCOS' formal procedure for patching is followed.

Communication security

GCOS has implemented controls to ensure that operation of material infrastructure components is carried out in a structured and secure manner.

Security services on the network

Access to GCOS' systems for our customers goes either through public networks where access is via VPN, MPLS or firewall. Access and communication between our servers and the internet go through our centrally managed firewall, where logging has been set up. All incoming network traffic goes through our redundant firewalls. Only approved network traffic, as configured filter rules, is allowed through the firewall based on a customer request. All internal and customer networks

are segregated by routers and firewalls, to the effect that customers and employees cannot reach networks for which they do not have authorization.

Control objective C - Organizational security measures

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

The General Data Protection Regulation specifies that appropriate technical and organizational security measures should be established.

GCOS governs the security setup by implemented rules, policies, processes, and procedures, covering all relevant controls areas of the ISO 27001, Annex A, such as but not limited to:

- Information security
- Logical access control
- Data backup
- Patch management
- Encryption
- Confidentiality
- Data breach

These policies set the overall requirements to prevent accidental or illegal destruction, loss, modification or unauthorised transfer or access to personal data.

In addition to the overall policies, a set of procedures specifically relating to the handling of personal data and how to act in accordance with the GDPR have been implemented.

Information and guidelines regarding collecting, storing and other processing of personal data is available to all employees on our intranet.

All employees receive mandatory training on data protection, and ongoing awareness campaigns are integrated into our annual security communication plan.

All employees have a strict confidentiality clause in their employment contract. Furthermore, all GCOS' employees are obliged to adhere to strict confidentiality.

GCOS has signed data processing agreements for all business relationships, where GCOS acts as a data processor.

It is the responsibility of the data controller to specify requirements for protecting the rights of the data subject and the processing of personal information.

Each data processing agreement will state the terms for the processing and protection of personal information specified by and approved by the data controller.

Control objective D - The right to erasing ("the right to be forgotten")

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.

All processing of personal data, where GCOS acts as a data processor, is governed by internal policies ensuring that:

- Information should be collected on a need-to-know-basis in accordance with the principle of data minimization.
- Data should be stored in a format permitting identification of data subjects solely for as long as necessary to fulfil the purpose, however dependant on information provided by customers.
- Data should be deleted in accordance with the data processing agreement.

Control objective E - Storing personal data

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.

GCOS can potentially handle special categories of personal data since information on the services provisioned on the platform at customers discretion, and the data that it processes, are not provided to GCOS by default.

GCOS has established procedures and processes for managing access to the platform and customer systems and services.

Access to customer systems, services or other configurations provisioned on platforms provided by GCOS are governed by strict access controls based on tiered access models and roles, and all sessions are logged and monitored.

Control objective F - Subprocessors

Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such sub-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.

GCOS uses several technology vendors for different information processing services, these are managed and evaluated according to classifications of the services provided. Vendor evaluations and risk assessments are performed periodically or before entering into agreements with new vendors

Management of security in agreements with third party
If the sub-suppliers are an integral part of our services, we inspect the controls implemented by the supplier by obtaining an ISAE 3402 auditor's report or equivalent. Relevant providers and consultants are to sign a non-disclosure agreement and confirm that they are familiar with our security policies and rules.

To the extent that GCOS' sub-suppliers store or otherwise manage personal data on behalf of GCOS' customers in the course of the sub-supplier's provision of services to GCOS, the sub-supplier acts as data processor solely according to instructions from GCOS and GCOS' customer. Thus,

GCOS's sub-suppliers commit themselves to take the necessary technical and organisational security measures to ensure that personal data are not accidentally or illegally destroyed, lost or impaired, and that they are not disclosed to unauthorised parties, misused or otherwise processed in violation of data protection legislation.

Control objective G - Transfer of personal data to third country

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

Data privacy policy addresses the transfer of personal data and states that any transfers outside of the EU/EEA must be in accordance with the GDPR.

Additionally, the procedures advise that any transfer of personal data outside EU/EEA should only use lawful means of transfer according to GDPR article 46.

Additionally, each Data Processing Agreement between GCOS and our customers states, whether transfer of personal information to third countries may take place.

Control objective H - Assisting the data controller

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.

GCOS will not act upon a request from a data subject without notifying and involving the data controller and no disclosure of information will be made to the data subject without prior written consent from the data controller, unless GCOS are legally obliged to do so.

Control objective I - Breaches of personal data security

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.

GCOS has implemented a security incident management policy stating GCOS' over-all responsibility in cases of security incidents as part of the overall policy, and GCOS has implemented detailed Incident management processes and procedures, which specifically defines how to handle incidents, including remediation and reporting.

Furthermore, GCOS has defined guidelines addressing personal data incidents, according to which it should be considered in every case, whether the incident requires notification to the Danish Data Protection Agency and/or the individuals concerned.

In accordance with the incident management procedures, the data controller must always be notified of an incident involving personal data processed by GCOS on behalf of the data controller.

Complementary controls at the data controllers

Some of the control objectives stated in GCOS' system description can only be met in connection with complementary controls that are operating effectively at the data controller.

This report does not cover the appropriateness of the design, implementation and operative effectiveness of such controls.

It is the responsibility of the data controller that they have implemented appropriate policies and procedures to comply with responsibility and the obligations for a Data Controller as set forth in the General Data Processing Agreement, covering the following, but not limited to:

- The personal data provided to GCOS is updated and correct,
- Ensuring the legality of the instructions provided to GCOS in relation to the Data Protection Laws in force at the time in question,
- That the instructions comply with the Data Processing Agreements and the services provided from GCOS,
- That access provisioning for personal data at the Data Controller is appropriate,
- That consent from the data subject is collected prior to processing of the personal data. The consent must reflect the processing performed in detail, and only be valid for as long as the relevant service is performed regarding the data subject,
- That the data subject is informed about the purpose and the extent of the processing of personal data,
- That adequate training and awareness of users in the Data Controllers organisation, regarding procedures for handling personal data, is performed,
- That the subscribed security measures are adequate for ensuring a sufficient protection of the processing of personal data.
- Configurations specific to customer environments are implemented in such a manner that they provide adequate protection for the personal data processed in the environment, including but not limited to:
    - Logging
    - Network segmentation
    - Network inspection
    - Firewall rules
    - Encryption
    - Vulnerability monitoring

CHAPTER 4:

Auditor's description of control objectives, security measures, tests, and findings

Control objective A Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.		
GlobalConnect's control procedures	Auditor's test of controls	Test findings
A.1 Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have interviewed relevant staff at GlobalConnect. We have checked by way of inspection that formalised procedures exist to ensure that personal data are only processed according to instructions. We have inspected relevant documentation and found that assessments are updated on a regular basis.	During our test we did not identify any material deviations.
A.2 The data processor only processes personal data stated in the instructions from the data controller.	We have interviewed relevant staff at GlobalConnect. We have inspected relevant documentation and enquired into the handling of the instructions from the data controller in the daily work routines and procedures. We have inspected the DPA Repository (Record of Processing). We have inspected that the contract management team procedure controls ensure that all new agreements are quality assured.	During our test we have found that not all data processing agreements, especially older ones, in the record of processing activities are fully updated. It is an identified risk where we have seen marked improvement in closing in the audit period, but it is not yet fully rectified. During our test we did not identify any further material deviations.

A.3 The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	We have interviewed relevant staff at GlobalConnect. We have inspected relevant documentation and enquired into how the data processor informs the data controller. We have inspected that it is part of the standard DPA that GlobalConnect are obliged to inform the customer if instructions are in breach of applicable laws.	During our test we did not identify any material deviations.

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.		
GlobalConnect control procedures	Auditor's test of controls	Test findings
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.	We have interviewed relevant staff at GlobalConnect. We have inspected that formalised procedures exist to ensure establishment of the safeguards agreed. Checked by way of inspection that procedures are up to date.	During our test we did not identify any material deviations.
B.2 The data processor has performed a risk assessment and, based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller.	We have interviewed relevant staff at GlobalConnect. We have enquired into how the formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. We have enquired the data processor as to how they have implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment.	During our test we did not identify any material deviations.
B.3 External access to systems and used in the processing of personal data takes place through a secured firewall.	We have interviewed relevant staff at GlobalConnect. We have enquired into the securing of access to personal data.	During our test we did not identify any material deviations.
B.4 Internal networks have been segmented to ensure restricted access to systems and used in the processing of personal data.	We have interviewed relevant staff at GlobalConnect. We have inquired as to whether internal networks have been segmented and seen documentation for this. We have inspected network documentation to ensure appropriate segmentation.	During our test we did not identify any material deviations.
B.5 Access to personal data is isolated to users with a work-related need for such access.	We have interviewed relevant staff at GlobalConnect.	During our test we did not identify any material deviations.

	We have inspected how access at GlobalConnect is given based on work-related requirements.	
B.6 For the systems used in the processing of personal data, system monitoring has been established with an alarm feature. This monitoring comprises, including but not limited to: • Capacity thresholds • Service State • Certificate expiration • System events	We have interviewed relevant staff at GlobalConnect. We have inspected system monitors with alarms and interviewed monitoring staff.	During our test we did not identify any material deviations.
B.7 Effective encryption is applied when transmitting confidential and sensitive personal data through the internet.	We have interviewed relevant staff at GlobalConnect. Checked by way of inspection that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet. Checked by way of inspection that technological encryption solutions have been available and active throughout the assurance period.	During our test we did not identify any material deviations.
B.8 Logging of the following matters has been established in systems and networks: Activities performed by system administrators and others holding special rights. Security incidents comprising: • Changes in log set-ups, including disabling of logging • Changes in users' system rights • Failed attempts to log on to systems, networks Logon data are protected against manipulation and technical errors and are reviewed regularly.	We have interviewed relevant staff at GlobalConnect. Checked by way of interview that user activity data collected in logs are protected against manipulation or deletion. Checked by way of interview that documentation exists regarding the follow-up performed for activities carried by system administrators and others holding special rights.	During our test we did not identify any material deviations.
B.9 The technical measures established are tested on a	We have interviewed relevant staff at GlobalConnect.	During our test we did not identify any material deviations.

regular basis in vulnerability scans tests.	Checked by way of inspection that regular testing of technical measures, including for performing vulnerability scans and penetration tests is performed. We have inquired into how any deviations or weaknesses in the technical measures are responded to.	
B.10 Changes to systems or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	We have interviewed relevant staff at GlobalConnect. We have inspected the formalised procedures that exist for handling of changes to systems networks, including handling of relevant updates, patches, and security patches.	During our test we did not identify any material deviations.
B.11 A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	We have interviewed relevant staff at GlobalConnect. We have inspected the procedures that exist for granting and removing users' access to systems used to process personal data. We have inspected samples of resigned or dismissed employees that their access to systems was deactivated or removed on a timely basis.	During our test we did not identify any material deviations.
B.12 Systems processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	We have interviewed relevant staff at GlobalConnect. We have inquired into how access to systems processing personal data by data owners own staff is regulated by the data owner (customer). We have inspected that GlobalConnect has implemented two-factor authentication for their staff.	During our test we did not identify any material deviations.
B.13 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 are stored and processed.	We have interviewed relevant staff at GlobalConnect. We have inspected the data centers and inquired about procedures, and seen documentation, for the access authorised persons to premises.	During our test we did not identify any material deviations.

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.		
GlobalConnect control procedures	Auditor's test of controls	Test findings
C.1 Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	We have interviewed relevant staff at GlobalConnect. We have inspected that the IS-policy is maintained and communicated to all relevant stakeholders.	During our test we did not identify any material deviations.
C.2 Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	We have interviewed relevant staff at GlobalConnect. We have inspected documentation that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered. Checked by way of inspection of the standard data processing agreement that the requirements in the agreement are covered by the requirements of the information security policy for safeguards and security of processing.	During our test we did not identify any material deviations.
C.3 A background check is made of all job candidates in accordance with business requirements and the function to be held by the employee. Employment at GlobalConnect requires always that a criminal record can be shown. When the customer or the task requires security clearance, this is obtained for the relevant employees in accordance with the relevant procedure for this purpose.	We have interviewed relevant staff at GlobalConnect. We have inspected relevant procedures and workflow and tested samples that show that the controls are fulfilled.	During our test we did not identify any material deviations.

C.4 Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	We have interviewed relevant staff at GlobalConnect. Checked by way of inspection of employees appointed during the assurance period that the relevant employees have: • Signed a confidentiality agreement • Been introduced to the Information security policy • Procedures for processing data and other relevant information.	During our test we did not identify any material deviations.
C.5 For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	We have interviewed relevant staff at GlobalConnect. We have 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. We have checked through inspection of employees resigned or dismissed during the assurance period that rights have been deactivated or terminated and that assets have been returned.	During our test we did not identify any material deviations.
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.	We have interviewed relevant staff at GlobalConnect. We have checked by way of inspection that the confidentiality agreements clearly state they remain in place after resignation.	During our test we did not identify any material deviations.
C.7 Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	We have interviewed relevant staff at GlobalConnect. We have inspected documentation for the mandatory training program including schedule and percentage trained.	During our test we did not identify any material deviations.

CONTROL OBJECTIVE A.7: HUMAN RESOURCE SECURITY

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.		
GlobalConnect' control procedures	Auditor's test of controls	Test findings
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 a regular basis – and at least once a year – as to whether the procedures should be updated	We have interviewed relevant staff at GlobalConnect. Checked by way of inspection that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. Checked by way of inspection that the procedures are up to date.	During our test we did not identify any material deviations.
D.2 The following specific requirements have been agreed with respect to the data processor's storage periods and deletion routines: • according to agreement with the customer	We have interviewed relevant staff at GlobalConnect. Checked by way of inspection that the existing agreement for storage and deletion include specific requirements for the data processor's storage periods and deletion routines.	During our test we did not identify any material deviations.
D.3 Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: • Returned to the data controller; and/or • Deleted if this is not in conflict with other legislation.	We have interviewed relevant staff at GlobalConnect. We have inspected the standard DPA and found that its provisions comply with the control parameters.	During our test we did not identify any material deviations.
D.4 Information should be collected on a need-to-know-basis in accordance with the principle of data minimization	Checked by way of interview that GCOS do not collect data wherefore the control is not currently relevant.	During our test we did not identify any material deviations.

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.		
GlobalConnect's control procedures	Auditor's test of controls	Test findings
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.	We have interviewed relevant staff at GlobalConnect. We have inspected that formalised policies exist for only storing and processing personal data in accordance with the data processing agreements. We have checked by way of inspection that the procedures are up to date.	During our test we did not identify any material deviations.
E.2 Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	We have interviewed relevant staff at GlobalConnect. We have inquired in to how only GlobalConnect Outsourcing Services process data in Denmark.	During our test we did not identify any material deviations.
E.3 The data processor has established procedures and processes for managing access to the platform and customer systems and services.	We have interviewed relevant staff at GlobalConnect. We have inquired as to how the data processor has established procedures and processes for managing access to the platform and customer systems and services.	During our test we did not identify any material deviations.
E.4 Access to customer systems, services or other configurations provisioned on platforms provided by the data processor are governed by strict access controls based on tiered access models and roles, and all sessions are logged and monitored.	We have interviewed relevant staff at GlobalConnect. We have inquired as to how the data processor has ensured that access is governed by strict access controls based on tiered access models and roles, and all sessions are logged and monitored.	During our test we did not identify any material deviations.

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.		
GlobalConnect's control procedures	Auditor's test of controls	Test findings
F.1 Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have interviewed relevant staff at GlobalConnect. We inquired in to whether there is use of sub-processors in the audit period. We are informed that there is no use of sub-processors in the audit period.	During our test we did not identify any material deviations.
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.	We have interviewed relevant staff at GlobalConnect. We are informed that there is no use of sub-processors in the audit period. We have inspected that GlobalConnect have procedures in place for approval vendors.	During our test we did not identify any material deviations.
F.3 When changing the generally approved sub-data processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-data processors used, this has been approved by the data controller.	We have interviewed relevant staff at GlobalConnect. We have inspected that the standard DPA specifically gives a 30-day notice period in case We are informed that there is no use of sub-processors in the audit period.	During our test we did not identify any material deviations.
F.4 The data processor has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	We have interviewed relevant staff at GlobalConnect. We have inspected the standard DPA that states that if GlobalConnect engage with a new sub-processor then the sub-processor will be contractually subjected to the same protection obligations as GlobalConnect.	During our test we did not identify any material deviations.
F.5 The data processor has a list of approved sub-data processors disclosing: • Name	Checked by way of inspection that the data processor has a complete and updated list of sub-data processors used and approved.	During our test we did not identify any material deviations.

• Business Registration No. • Address • Description of the processing.	Checked by way of inspection that, as a minimum, the list includes the required details about each sub-data processor.	
F.6 Based on an updated risk assessment of each sub-data processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-data processor.	We have interviewed relevant staff at GlobalConnect. We have inspected that GlobalConnect have procedures in place for approval and continual follow-up on vendors. We are informed that there is no use of sub-processors in the audit period.	During our test we did not identify any material deviations.

Control objective G Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.		
GlobalConnect's control procedures	Auditor's test of controls	Test findings
G.1 Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have interviewed relevant staff at GlobalConnect. We have inspected that formalised procedures exist to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Checked by way of inspection that procedures are up to date.	During our test we did not identify any material deviations.
G.2 The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	We have interviewed relevant staff at GlobalConnect. We have inquired as to where it is stated that the data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller. We have inspected documentation.	During our test we did not identify any material deviations.
G.3 Procedures advise that any transfer of personal data outside EU/EEA should only use lawful means of transfer according to GDPR article 46.	We have interviewed relevant staff at GlobalConnect. We have inquired as to where it is stated that transfer of personal data outside EU/EEA should only use lawful means of transfer according to GDPR article 46. We have inspected documentation.	During our test we did not identify any material deviations.

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 infor-mation on the processing of personal data to the data subject.		
GlobalConnect's control procedures	Auditor's test of controls	Test findings
H.1 Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have interviewed relevant staff at GlobalConnect. We have inspected that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. Checked by way of inspection that procedures are up to date.	During our test we did not identify any material deviations.
H.2 The data processor has established procedures in so far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting, or restricting or providing information about the processing of personal data to data subjects.	We have interviewed relevant staff at GlobalConnect. Checked by way of inspection that the procedures in place for assisting the data controller.	During our test we did not identify any material deviations.

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.		
GlobalConnect' control procedures	Auditor's test of controls	Test findings
I.1 GlobalConnect has implemented formal operating procedures, which are available to all users having a function-related need for insight.	We have interviewed relevant staff at GlobalConnect. We have inspected that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. Checked by way of inspection that procedures are up to date.	During our test we did not identify any material deviations.
I.2 The data processor has established the following controls to identify any personal data breaches: • Awareness of employees • Monitoring of network traffic • Follow-up on logging of access to personal data	We have interviewed relevant staff at GlobalConnect. We have inspected that the data processor provides the controls as specified.	During our test we did not identify any material deviations.
I.3 If any personal data breach occurred, the data processor informed the data controller without undue delay and no later than the amount of hours specified in the DPA after having become aware of such personal data breach at the data processor or a sub-data processor.	We have interviewed relevant staff at GlobalConnect. We have made inquiries as to whether they have identified any personal data breaches throughout the assurance period. There were none. We are informed that GlobalConnect Outsourcing Services does has not utilized person data sub-processors in the audit period.	During our test we did not identify any material deviations.
I.4 The data processor has established procedures for assisting 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.	We have interviewed relevant staff at GlobalConnect. We have inspected that the standard DPA states GlobalConnects obligation in case of a data breach to: • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach.	During our test we did not identify any material deviations.

	We have walked through how procedures work and which roles are involved should a breach occur.	

Chapter 5

Additional information from GLOBALCONNECT Outsourcing Services of GLOBALCONNECT A/S

Regarding control A.2:

GlobalConnect is aware of the few outstanding Data Processing Agreements and is working with the customers to get it in place.

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

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

Peter Nicolai Riis
BEIERHOLM, STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 32895468
IT-auditor
Serienummer: 135ccee6-9c8d-426c-bec0-ba9ff5898423
IP: 212.98.xxx.xxx
2024-02-16 08:04:13 UTC

Kim Holm Larsen
BEIERHOLM, STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 32895468
Statsautoriseret revisor
På vegne af: Beierholm
Serienummer: bff7239f-6800-4339-865f-dbc13a357020
IP: 212.98.xxx.xxx
2024-02-16 15:29:53 UTC

Monika Juul Henriksen
GLOBALCONNECT A/S CVR: 26759722
Senior Vice President, Head of Nordic Enterprise
Serienummer: 8a8a0a1a-bff0-4e7d-96b9-46f32ed2e07c
IP: 217.61.xxx.xxx
2024-02-19 12:49:45 UTC