ONLINECITY.IO

ONLINECITY.GROUP ApS

ISAE 3000 Assurance Report 2026

RELATION CITY OMNI CHANNEL

gatewayapi

OCCS
ONLINECITY CUSTOMIZED SOLUTIONS

BDO

CONTENT

1. INDEPENDENT AUDITOR'S OPINION 2

2. ONLINECITY GROUP APS' STATEMENT 5

3. ONLINECITY GROUP APS DESCRIPTION OF GATEWAYAPI, RELATIONCITY, POLARIS 7

ONLINECITY Group ApS 7

GatewayAPI, RelationCity, Polaris and Processing of Personal Data 7

Personal data security management 7

Risk assessment 9

Technical and organisational security measures and other controls 9

Complementary controls at the Data Controllers 14

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND TEST RESULTS 15

Risk assessment 17

A.5 Organisational measures 18

A.6 Person-related measures 29

A.7 Physical measures 31

A.8 Technological measures 32

1. INDEPENDENT AUDITOR'S OPINION

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD 1 MAY 2025 TO 30 APRIL 2026 ON THE DESCRIPTION OF GATEWAYAPI, RELATIONCITY, POLARIS AND THE ASSOCIATED TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS, THEIR DESIGN AND OPERATIONAL EFFECTIVENESS RELATING TO THE PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE GENERAL DATA PROTECTION REGULATION AND THE DATA PROTECTION ACT

To: The Management of ONLINECITY Group ApS
ONLINECITY Group ApS' Customers

Scope

We have been tasked with providing a declaration of the description prepared by ONLINECITY Group ApS (the Data Processor) for the entire period 1 May 2025 to 30 April 2026 in section 3 of GatewayAPI, RelationCity, Polaris and the associated technical and organisational security measures and other controls, aimed at the processing and protection of personal data in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons in connection with the processing of personal data and on the free movement of such data (the General Data Protection Regulation) and the Act on Supplementary Provisions to the General Data Protection Regulation (the Data Protection Act), and on the design and operational effectiveness of the technical and organisational security measures and other controls linked to the control objectives stated in the description for the period 1 May 2025 to 30 April 2026.

ONLINECITY Group ApS uses sub-processors in connection with their role as Data Processor. This assurance report has been prepared using the partial method and therefore does not include control objectives and controls at these sub-processors.

Responsibilities of the Data Processor

The Data Processor is responsible for preparing the statement in section 2 and the accompanying description including the completeness, accuracy, and method of presenting the statement and the description. Furthermore, the Data Processor is responsible for providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor independence and quality management

We have complied with the requirements of independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Guidelines for Auditors' Ethical Conduct (IESBA Code), which is based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct, as well as ethical requirements applicable in Denmark.

BDO Statsautoriseret revisionspartnerselskab applies the International Standard on Quality Management 1, ISQM 1, which requires us to design, implement and operate a quality management system, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable laws and other regulations.

Auditor's Responsibilities

Our responsibility is to express an opinion on the Data Processor's description and on the design and operating effectiveness of controls related to the control objectives stated in that Description, based on our procedures.

We have performed our work in accordance with ISAE 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether the description is fairly presented, in all material respects, and whether the controls are suitably designed and operated effectively.

An assurance engagement to provide a statement on the description, design, and operational effectiveness of controls at a Data Processor involves performing procedures to obtain evidence about the information in the Data Processor's description and about the design and operational effectiveness of the controls. The selected procedures depend on the Data Processor's auditor's judgment, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls, that we consider necessary to provide a high level of assurance that the control objectives stated in the description were achieved. A report assignment of this type also includes evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified and described by the Data Processor in section 2.

It is our opinion that the evidence obtained is sufficient and appropriate to provide a basis for our conclusion.

Limitations on controls at a Data Processor

The Data Processor's description is prepared to meet the common needs of a broad range of Data Controllers and therefore may not include all the aspects of the use of GatewayAPI, RelationCity, Polaris that each individual Data Controller may consider important based on their specific circumstances. Furthermore, due to their nature, controls at a Data Processor may not prevent or detect all breaches of personal data security. Additionally, any projection of the assessment of the operational effectiveness of controls to future periods is subject to the risk that controls at a Data Processor may become inadequate or fail.

Conclusion

Our conclusion is based on the matters outlined in this report. The criteria we used in forming our conclusion are the criteria described in the Data Processor's statement in section 2. It is our opinion:

a. that the description of GatewayAPI, RelationCity, Polaris and the associated technical and organisational security measures and other controls aimed at the processing and protection of personal data in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act, as they were designed and implemented throughout the period 1 May 2025 to 30 April 2026, is fairly presented in all material respects, and

b. that the technical and organisational security measures and other controls related to the control objectives stated in the description were suitably designed throughout the period 1 May 2025 to 30 April 2026, and

c. that the tested technical and organisational security measures and other controls, which were necessary to provide a high level of assurance that the control objectives in the description were achieved in all material respects, operated effectively throughout the period 1 May 2025 to 30 April 2026.

Description of testing controls

The specific controls tested, and the results of these tests are set out in Section 4.

Intended users and purposes

This report is intended only for Data Controllers who have used the Data Processor's GatewayAPI, RelationCity, Polaris and who have sufficient understanding to consider it along with other information, including the technical and organisational security measures and other controls that the Data Controllers themselves have implemented, when assessing whether the requirements of GDPR and the Danish Data Protection Act have been met.

Copenhagen, 27 May 2026

BDO Statsautoriseret revisionspartnerselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Mikkel Jon Larssen
Partner, Head of Risk Assurance, CISA, CRISC

2. ONLINECITY GROUP APS' STATEMENT

ONLINECITY Group ApS processes personal data in connection with GatewayAPI, RelationCity, Polaris for our customers who are Data Controllers in accordance with 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 General Data Protection Regulation) and the Act on Supplementary Provisions to the General Data Protection Regulation (the Danish Data Protection Act).

The accompanying description is prepared for use of Data Controllers who have used GatewayAPI, RelationCity, Polaris and who have sufficient understanding to consider the description along with other information, including the technical and organisational security measures and other controls that the Data Controllers themselves have implemented, when assessing whether the requirements of GDPR and the Danish Data Protection Act have been complied with.

ONLINECITY Group ApS uses sub-processors. The relevant control objectives and associated technical and organisational security measures and other controls of sub-processors are not included in the accompanying description.

ONLINECITY Group ApS confirms that the accompanying description in section 3 provides a fair description of GatewayAPI, RelationCity, Polaris and the associated technical and organisational security measures and other controls throughout the period from 1 May 2025 to 30 April 2026. The criteria used to give this opinion were that the accompanying description:

1. Describe GatewayAPI, RelationCity, Polaris and how the associated technical and organisational security measures and other controls were designed and implemented, including an account of:
    - The types of services provided, including the type of personal data processed.
    - The processes in both IT systems and business procedures used to process personal data and, if necessary, to correct and delete personal data as well as to restrict the processing of personal data.
    - The processes used to ensure that the data processing carried out is in accordance with a contract, instruction or agreement with the Data Controller.
    - The processes that, ensure that the persons authorised to process personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.
    - The processes that, upon termination of data processing, that all personal data is deleted or returned to the Data Controller at the Data Controller's choice, unless the law or regulation requires the retention of the personal data. The processes, that in the event of a personal data breach, support the Data Controller in notifying the supervisory authority and informing the data subjects.
    - The processes that ensure appropriate technical and organisational security measures for the processing of personal data, considering the risks posed by processing, particularly accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
    - The controls that we have assumed, based on the scope of GatewayAPI, RelationCity, Polaris, have been designed and implemented by the Data Controllers and which, if necessary to achieve the control objectives, are identified in the description.
    - The other aspects of the control environment, risk assessment process, information systems and communication, control activities, and monitoring controls that have been relevant to the processing of personal data.

2. Includes relevant information about changes in GatewayAPI, RelationCity, Polaris and the associated technical and organisational security measures and other controls made during the period 1 May 2025 to 30 April 2026.

3. Does leave out or misrepresent information relevant to the scope of GatewayAPI, RelationCity, Polaris and the associated technical and organisational security measures and other controls, considering that this description prepared to meet the common needs of a broad range of Data Controllers and therefore cannot include every aspect of GatewayAPI, RelationCity, Polaris that each individual Data Controller may consider important according to their particular circumstances.

ONLINECITY Group ApS confirms that the technical and organisational security measures and other controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 1 May 2025 to 30 April 2026. The criteria used to provide this statement were that:

1. The risks that threatened the achievement of the control objectives stated in the description were identified.

2. The identified controls, if performed as described, would provide a high level of assurance that the relevant risks would not prevent the achievement of the stated control objectives.

3. The controls were consistently applied as designed, including that manual controls were performed by persons with appropriate competence and authority, throughout the period 1 May 2025 to 30 April 2026.

ONLINECITY Group ApS confirms that appropriate technical and organisational security measures and other controls have been implemented and maintained to fulfil the agreements with the Data Controllers, good data processing practices and relevant requirements for Data Processors in accordance with the General Data Protection Regulation and the Data Protection Act.

Odense, 27 May 2026

ONLINECITY Group ApS

Thomas Richard Hofmann Chairman of the board	Birol Altinok Executive	Martin Eland Pløger Executive

3. ONLINECITY GROUP APS DESCRIPTION OF GATEWAYAPI, RELATIONCITY, POLARIS

ONLINECITY GROUP APS

ONLINECITY Group is a Danish-owned business which develops and operates several online systems to municipalities and different industry sectors in the private market. ONLINECITY Group has offices in Odense and Copenhagen, and wholly owns and operates the companies ONLINECITY.IO ApS, RelationCity ApS, and OC Customized Solutions ApS, which offers the products GatewayAPI, RelationCity, and Polaris, respectively.

ONLINECITY Group has approximately 50 employees who are specialised in system development, server operation, support, and information security and who are organized in a development department, an operations and support department, a finance department, and an administration department.

The Compliance team and ONLINECITY Group's IT Security Committee manage ONLINECITY Group's personal data security in relation to the processing that ONLINECITY Group performs on behalf of its customers, such as making data processing agreements, responding to requests from the Data Controller, notification of breach of the personal data security, compliance with internal policies and procedures, and similar areas.

GATEWAYAPI, RELATIONCITY, POLARIS AND PROCESSING OF PERSONAL DATA

ONLINECITY Group offers SMS gateways as a Software-as-a-Service (SaaS) solution according to a contract with municipalities and private businesses. The SMS gateways are systems for sending and receiving SMS.

The GatewayAPI product is constructed as two independent platforms, GatewayAPI.com and GatewayAPI.eu. These platforms are developed independently in Denmark and operated from Google and Hetzner, respectively. GatewayAPI is a product which targets a wide variety of different customers, who can sign up themselves, and start using the product.

The RelationCity product is an independent platform, which customers may also sign up to use by themselves, but offers other features than GatewayAPI, which makes it more suitable for customers who focus on marketing and relationship building. This platform is developed independently in Denmark and operated from Hetzner.

The Polaris product is an independent platform, which is specifically built and customized for selected clients and partners and is not available to the wider public. This platform is developed independently in Denmark and operated from Hetzner. ONLINECITY Group has made data processing agreements with the sub-processors mentioned above. ONLINECITY Group processes personal data on behalf of their customers, who are Data Controllers, when they use the platforms for SMS communication and have made data processing agreements with the Data Controllers relating to this processing.

The personal data processed are governed by Art. 6 of the EU General Data Protection Regulation (GDPR) and include telephone numbers and text messages.

PERSONAL DATA SECURITY MANAGEMENT

ONLINECITY Group has laid down requirements for establishment, implementation, maintenance, and current improvement of system for management of personal data security, which ensures compliance with agreements made with Data Controllers, generally accepted data processing practice and relevant requirements applying to Data Processors according to the GDPR and the Data Protection Act.

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

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

ISO 27001 RANGE	CONTROL AREA	ARTICLE
Risk assessment	Risk assessment	Article 28(3)(c)
A.5 Organisational measures	Information security policies and information security policy review	Article 28(1)
	Information security policies in accordance with data processing agreements	Article 28(1)
	List of categories of processing activities	Article 30(2), (3) and (4).
	Procedure for transfers of personal data to third countries	Articles 44 to 49.
	Instructions for the transfer of personal data to third countries	Articles 44 to 49.
	Valid transfer basis	Articles 44 to 49.
	Managing access and reviewing access rights	Article 28(3)(c).
	Use of secret authentication information	Article 28(3)(c).
	Sub-data processing agreement and instructions	Article 28(3)(c).
	Approval of sub-processors	Article 28(3)(c).
	Changes in approved sub-processors	Article 28(3)(c).
	The subprocessor's obligations	Article 28(3)(c).
	Overview of sub-processors	Article 30(2)
	Supervision of sub-processors	Article 28(3)(c).
	Notification of personal data breaches	Article 28(3)(c).
	Identifying personal data breaches	Article 28(3)(c).
	Assistance to Data Controllers in the event of a personal data breach	Article 28(3)(c).
	Timely notification of personal data breaches	Article 28(3)(c).
	Procedure for processing personal data	Article 28(3).
	Compliance with instructions for processing personal data	Articles 28(3), 29 and 32(4).
	Agreed security measures	Article 28(3)(c).
	Notification of the Data Controller in the event of an unlawful instruction	Article 28(3)(h).
	Procedure for fulfilling the rights of data subjects	Article 28(3)(e).
	Technical measures for the fulfilment of data subjects' rights	Article 28(3)(e).
	Storage of information is in accordance with the Data Controller's requirements	Article 28(3)(c).
	Location of processing and storage of information	Article 28(3).
A.6 Person-related measures	Recruitment of employees - Screening	Article 28(1).
	Recruitment of employees - Confidentiality and confidentiality agreement with employees	Article 28(3)(b).
	Awareness, education and training regarding information security	Article 28(1)
	Resignation of employees - information about confidentiality and professional secrecy	Article 28(3)(b).

ISO 27001 RANGE	CONTROL AREA	ARTICLE
	Termination of employees - withdrawal of access rights and assets	Article 28(1)
A.7 Physical measures	Physical access control	Article 28(3)(c).
	Repair, service and destruction of IT equipment	Article 28(3)(c).
A.8 Technological measures	Secure authentication	Article 28(3)(c).
	Monitoring of systems and environments	Article 28(3)(c).
	Antivirus program	Article 28(3)(c).
	Data backup and recovery	Article 28(3)(c).
	Logging	Article 28(3)(c).
	System Software Maintenance	Article 28(3)(c).
	Firewall	Article 28(3)(c).
	Network security	Article 28(3)(c).
	Remote workplaces and remote access to systems and data	Article 28(3)(c).
	Encryption when transmitting personal data	Article 28(3)(c).
	Deletion of information in accordance with the Data Controller's requirements	Article 28(3)(g).
	Requirements for the storage and deletion period of data are in accordance with the Data Controller's requirements	Article 28(3)(g).
	Deletion and return upon termination of customer relationship	Article 28(3)(g).
	Change management and privacy-by-design	Article 25.
	Implementing change in the production environment	Article 25.
	Separation of development, test and production environment	Article 25.
	Access to source code	Article 25.
	Anonymisation of personal data in development tasks	Article 25.

RISK ASSESSMENT

Management is responsible for implementing all initiatives that address the threat scenario which ONLINECITY Group is facing from time to time, so that implemented security measures and controls are appropriate, and the risk of breach of personal data security is reduced to an appropriate level.

There is a current assessment of which security level is appropriate. This assessment considers risks relating to accidental or illegal destruction, loss or alteration or unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

As a basis for updating the technical and organisational measures and other controls, a risk assessment is carried out annually on each platform. The risk assessments address the likelihood and consequences of incidents that may threaten the security of personal data and thus the rights and freedoms of natural persons, including random, intentional, and unintentional incidents. The risk assessment considers the current technical level and costs of implementation.

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES AND OTHER CONTROLS

The technical and organisational measures and other controls are related to all processes and systems processing personal data on behalf of the Data Controller. The control objectives and control activities stated in the control schedule are an integral part of the following description.

A.5 Organisational measures

Data Processor's Guarantees

ONLINECITY Group has implemented policies and procedures to ensure that ONLINECITY Group can provide sufficient guarantees to carry out suitable technical and organisational measures in such a manner that the processing meets the requirements in GDPR and ensures protection of the data subject's rights. ONLINECITY Group has established an organization of personal data security and prepared and implemented an information security policy, approved by Management, which is reviewed and updated on an annual basis. Procedures exist for recruitment and resignation of personnel and guidelines for training and instruction of personnel processing personal data, such as completed awareness training and education campaigns.

List of categories of processing activities

ONLINECITY Group has implemented policies and procedures to ensure that a record of processing activities is kept of categories of processing activities performed on behalf of the Controller. The records are updated regularly and are examined during the annual review of policies and procedures, etc. The records of activities are stored electronically and can be made available to the supervisory authority on request.

Transfer of personal data to third countries

ONLINECITY Group has implemented policies and procedures to ensure that the transfer of personal data to sub-processors in non-EU countries is in accordance with standard contract or other valid basis of transfer and according to instruction from the Controller.

Logical access security and access management

ONLINECITY Group has implemented procedures to ensure that access to systems and data is controlled through logical controls and protected by an authorization system. The user is created with a unique user identification and password, and the user identification is used when access to resources and systems is allocated. All allocations of rights in systems are based on a work-related need for access, such as relevance and correctness of allocated user rights. The user's continued work-related need for access is evaluated at least once a year. Procedures and controls support the process of creating, modifying, and decommissioning users and assigning rights and reviewing them.

The design of requirements for, among others, length, complexity, current change, and history of passwords as well as closing of user accounts after unsuccessful access attempts are in accordance with best practice for a safe logical access control. Technical measures supporting these requirements have been designed.

Sub-data processing agreement and instructions

ONLINECITY Group has implemented policies and procedures to ensure that the same data protection obligations are imposed on sub-processors, as specified in the data processing agreement between the Controller and ONLINECITY Group, and that the sub-processors can give sufficient guarantees for protection of personal data. Procedures ensure that the Controller gives a prior, specific, or general written approval of sub-processors, and that changes in approved sub-processors are managed.

ONLINECITY Group evaluates the sub-processor and the sub-processor's guarantees before an agreement is made to ensure that the sub-processor can fulfil the obligations imposed on ONLINECITY Group. ONLINECITY Group carries out an annual inspection of their sub-processors, based on a risk assessment of the specific processing of personal data, for example by obtaining independent auditor's reports or similar documentation.

Notification of personal data breaches

ONLINECITY Group has implemented policies and procedures to ensure that a breach of personal data security is registered with detailed information on the incident, and that the Controller is notified without undue delay after ONLINECITY Group became aware of the breach of personal data security. The registered information enables the Controller to assess whether the supervisory authority should be notified of the breach of personal data security and whether the data subjects should be notified.

Assistance to the Data Controller in relation to personal data breaches

ONLINECITY Group has implemented policies and procedures to ensure that ONLINECITY Group can assist the Controller in ensuring compliance with the obligations in Article 32 on security of processing, Article 33 on notification and communication of breach of personal data security, and Articles 34 to 36 on impact assessments.

Entering into a data processing agreement with Data Controllers

ONLINECITY Group has implemented policies and procedures for making data processing agreements, which ensure that ONLINECITY Group in connection with the customer contract makes a data processing agreement which specifies the conditions for processing of personal data on behalf of the Controller. ONLINECITY Group uses a template for data processing agreements in accordance with the services delivered, such as information on the use of sub-processors. The data processing agreements are signed digitally and stored electronically.

ONLINECITY Group has implemented policies and procedures to ensure that ONLINECITY Group can make available to the Controller all information required to prove compliance with the requirements applying to Data Processors. ONLINECITY Group also allows and contributes to audits, including inspections performed by the Controller or other parties authorised to do so by the Controller.

Instructions for processing personal data

ONLINECITY Group has implemented policies and procedures to ensure that ONLINECITY Group acts according to the instruction that the Controller has given in the data processing agreement. The instructions are maintained in relation to procedures instructing the personnel how processing of personal data should be done, including who can give binding instructions to ONLINECITY Group. The procedure also ensures that ONLINECITY Group informs the Controller when the Controller's instruction infringes the data protection legislation.

Agreed security measures

ONLINECITY Group has introduced procedures to ensure that agreed safeguards are in place for the processing of personal data in accordance with the agreement with the Data Controller.

Assistance to the Data Controller in relation to the rights of the data subject

Assistance to the Controller ONLINECITY Group has implemented policies and procedures to ensure that ONLINECITY Group can assist the Controller meeting with the Controller's obligation to respond to requests for exercise of the data subject's rights under Article 12-23, Article 28.

Storage of personal data

ONLINECITY Group has introduced procedures that ensure that the storage of personal data is only carried out in accordance with the contract with the Data Controller and the list of locations in the associated data processing agreement.

A.6 Person-related measures

Recruitment and resignation of employees

ONLINECITY Group has implemented policies and procedures for recruitment and resignation of personnel and guidelines for training and instruction of personnel processing personal data, such as awareness training and education campaigns.

Confidentiality and statutory confidentiality

ONLINECITY Group has implemented policies and procedures to ensure confidentiality in the processing of personal data. All personnel at ONLINECITY Group have committed themselves to confidentiality by signing an employment contract, which includes terms and conditions relating to secrecy and confidentiality.

Only authorized personnel with a relevant job role will process or have access to personal data. These employees receive regular training in handling personal data and IT security.

A.7 Physical measures

Physical security, including physical access control

ONLINECITY Group has implemented procedures to ensure that premises are protected from unauthorized access. Only persons with a work-related or other legitimate need have access to the premises, and special measures have been implemented for areas where personal data is processed. Customers, suppliers, and other visitors are escorted.

Repair, service and disposal of IT equipment

ONLINECITY Group has implemented procedures to ensure that equipment sent to third parties for service or repair is handed over with encrypted data disks. Additionally, used or decommissioned data media and disks are securely destroyed.

A.8 Technological measures

External communication links

ONLINECITY Group has implemented procedures to ensure that external communication lines are safeguarded by strong encryption, and that emails and other communication, containing sensitive personal data, are encrypted in the transmission by using TLS 1.2 as a minimum.

System Software Maintenance

ONLINECITY Group has implemented procedures to ensure that system software is updated according to the suppliers' directions and recommendations. Procedures for Patch Management include operating systems, critical services and software installed on servers and workstations.

Antivirus program

ONLINECITY Group has put in place procedures to ensure that devices with access to networks and applications are protected from viruses and malware. Antivirus programs and other protection systems are updated and adjusted to the current threat level, and monitoring of these systems is set up, including periodic testing for functionality.

Data backup and recovery

ONLINECITY Group has implemented procedures to ensure that backup is taken of systems and data to prevent loss of data or loss of accessibility in case of crashes. Backups are kept at an alternative location. Backups are protected by physical and logical security measures to prevent that data falling into the hands of third parties, or that backups are destroyed by fire, water, vandalism, or accidental damage.

Logging in systems, databases and networks

ONLINECITY Group has implemented procedures to ensure that logging has been set up in accordance with the requirements in legislation and business needs, based on a risk assessment of systems and the current

threat scenario. The scope and quality of log data is sufficient to identify and prove a potential abuse of systems or data, and log data are examined for applicability and abnormal behaviours. Log data is protected against loss and erasure.

Monitoring
ONLINECITY Group has implemented procedures to ensure that systems are monitored and that technical security measures have been implemented.

Network security
ONLINECITY Group has implemented procedures to ensure that networks in relation to use and security are divided into several virtual networks (VLAN), in which traffic between the individual networks is controlled by a firewall. Servers with an integrated firewall use this to ensure that access is given only to the necessary services.

Firewall
ONLINECITY Group has implemented procedures to ensure that traffic between the internet and the network is controlled by a firewall. Access from the outside via ports in the firewall is limited as much as possible and access rights are allocated via specific ports to specific segments. Workstations use the local firewall.

Remote workplaces and remote access to systems and data
ONLINECITY Group has implemented procedures to ensure that access from workplaces outside ONLINECITY Group's premises and remote access to systems and data is via VPN-connections with two-factor authentication to systems with personal data. Access from workplaces outside ONLINECITY Group's premises to all external services uses HTTPS, which ensures encryption and prevents leak of information which is accessed via the business' Google-account with two-factor authentication.

Data protection by design and default settings
ONLINECITY Group has implemented policies and procedures for development and maintenance of platforms to ensure a managed change process. A Change Management system is used to manage development and change tasks, and all tasks follow a uniform process which starts with a risk assessment in accordance with the requirements for data protection by design and by default.
The development, test and production environments are separated, and there is segregation of duties between the employees in the development department and the operations and support department. All development and change tasks go through a test cycle and anonymized production data are used as test data. Procedures for version control, logging and backup have been implemented, so that it is possible to reinstall earlier versions.

Deletion and return of personal data
ONLINECITY Group has policies and procedures in place to ensure that personal data is deleted or returned in accordance with instructions from the Data Controller when the processing of personal data ceases at the end of the contract with the Data Controller.

Changes in the period 1 May 2025 to 30 April 2026
ONLINECITY Group has not made any significant changes to the GatewayAPI, RelationCity, and Polaris products' functionalities in the period from 1 May 2025 to 30 April 2026.

COMPLEMENTARY CONTROLS AT THE DATA CONTROLLERS

The Data Controller is obliged to implement the following technical and organisational security measures and other controls in order to achieve the control objectives and thus comply with the data protection legislation:

- It is the responsibility of the Controller to ensure that the administrators' use of the platforms and the processing of personal data carried out in the system comply with the data protection legislation.
- The Controller manages the user rights in the platforms, including to whom administrators' access is allocated and which rights are allocated to the individual administrators.
- The Controller is not allowed to use the platforms for processing, including retention, of sensitive personal data, and it is the Controller's responsibility to ensure that such personal data are not entered into or uploaded to the platforms.
- The Controller is responsible for the data that is processed on the RelationCity platform according to the description in the data processing agreement.

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND TEST RESULTS

Purpose and scope

We conducted our engagement in accordance with ISAE 3000, Assurance Reports Other Than Audits or Reviews of Historical Financial Information.

BDO has undertaken actions to obtain evidence for the information in ONLINECITY Group ApS' description of GatewayAPI, RelationCity, Polaris as well as for the design of the associated technical and organisational security measures and other controls. The procedures selected depend on BDO's judgement, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed or operating effectively.

BDO's testing of the design and operational effectiveness of technical and organisational security measures and other controls has included the control objectives and associated control activities selected by ONLINECITY Group ApS and set out in the subsequent control chart.

In the control form, BDO has described the tests carried out that were deemed necessary in order to obtain a high level of assurance that the stated control objectives were achieved and that the associated were suitably designed and operated effectively throughout the period 1 May 2025 to 30 April 2026.

Performed test actions

Testing of the design of technical and organisational security measures and other controls, as well as their implementation and operational effectiveness, has been carried out by means of inquiry, inspection, observation and re-execution.

Type	Description
Query	Inquiries by appropriate personnel have been carried out for all essential control activities. The queries were carried out in order to, among other things, obtain knowledge and further information on policies and procedures in place, including how the control activities are carried out, as well as to confirm evidence of policies, procedures and controls.
Inspection	Documents and reports indicating the performance of the controls are reviewed for the purpose of assessing the design and monitoring of the specific controls, including whether the controls are designed to be effective if implemented, and whether the controls are adequately monitored and controlled at appropriate intervals. Tests of essential system setups of technical platforms, databases and network equipment have been carried out to ensure that controls have been implemented, including, for example, assessment of logging, backups, patch management, authorizations and access controls, data transmission and inspection of equipment and locations.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the controls are implemented.
Re-performance	Controls have been re-performed to obtain additional evidence that the controls operate as assumed.

For the services provided by Google Cloud Web Hosting within Hosting we have received SOC 2 report for the period spanning from the 1. November 2025 to the 31. October 2026, and ISO 27001 certificate for the sub-processor's technical and organisational security measures and other controls.

For the services provided by Hetzner Online GmbH within Hosting, we have received an updated TÜV report and ISO 27001 certificate for the sub-processor's technical and organisational security measures and other controls.

These sub-processors and service organisations relevant control objectives and related controls are not included in ONLINECITY Group's description of GatewayAPI, RelationCity and Polaris and relevant controls related to operation of GatewayAPI, RelationCity and Polaris. Thus, we have solely assessed the reports and tested the controls at ONLINECITY Group, which ensures appropriate supervision of the sub-processor's compliance with the data processing agreement made between the sub-processor and the Data Processor and compliance with the General Data Protection Regulation and the Danish Data Protection Act.

Test result

The results of the tests carried out on technical and organisational security measures and other controls indicate whether the tests described have given rise to the detection of deviations.

A deviation exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective, and
- Technical and organisational measures and other controls related to a control objective are not suitably designed and implemented or did not operate effectively throughout the period.

Risk assessment			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Risk assessment To ensure that the Data Processor performs an annual risk assessment in relation to the consequences for the data subjects, which forms the basis for the technical and organisational security measures.	▶ A risk assessment is carried out on an ongoing basis and at least once a year based on potential risks to the accessibility, confidentiality and integrity of data in relation to the rights and freedoms of the data subject. ▶ Risks are minimized based on the assessment of their probability, consequence, and derived implementation costs.	We have made inquiries with relevant personnel. We have inspected that the Data Processor has carried out a risk assessment based on potential risks to the availability, confidentiality and integrity of the data in relation to the rights of the data subject. We have inspected that the risk assessment carried out has been updated and approved.	No exceptions noted.

A.5 Organisational measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Information security policies and information security policy review To ensure ongoing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, regulatory, regulatory and contractual requirements, in accordance with ISO/IEC 27001 A.5.1 and GDPR Article 28(1).	▶ The Data Processor has prepared and implemented an information security policy. ▶ An assessment is made on an ongoing basis – and at least once a year – of whether the IT security policy needs to be updated.	We have made inquiries with relevant personnel. We have inspected that there is an information security policy that the management has processed and approved. We have inspected documentation that the information security policy has been communicated to relevant stakeholders, including the Data Processor's employees. We have inspected that procedures have been updated and approved during the declaration period.	No exceptions noted
Information security policies in accordance with data processing agreements To ensure compliance with legal, regulatory, regulatory, and contractual requirements related to information security and personal data protection, according to ISO/IEC 27001 A.5.1, A.5.31, and A.5.34 and GDPR Article 28(1).	▶ The Data Processor's management has ensured that the information security policy is not in conflict with the data processing agreements entered into.	We have made inquiries with relevant personnel. We have inspected data processing agreements to ensure that the requirements in the agreements do not conflict with the information security policy.	No exceptions noted.
List of categories of processing activities To clarify the organization's information and supporting assets to maintain information security and assign appropriate ownership, according to ISO/IEC 27001 A.5.9 and GDPR Article 30(2), (3) and (4).	▶ The Data Processor has established a list of categories of processing activities as a Data Processor. The list must include: • the name and contact details of the Data Controller; • the categories of processing carried out on behalf of the Controllers; • the name and contact details of each sub-processor;	We have made inquiries with relevant personnel. We have inspected that the Data Processor's record of categories of processing activities as a Data Processor and observed that it contains relevant information, and that the record is stored electronically. We have inspected that the record has been updated in the declaration period.	We have established that the Danish Data Protection Agency did not request the disclosure of the record of categories during the declaration period. We are therefore unable to test the implementation and efficiency of this control. No exceptions noted.

A.5 Organisational measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
	• indication of any transfer of personal data to a third country. ▶ The record is stored electronically in the Data Processor's system/file drive. ▶ The Data Processor will provide the register at the request of the Danish Data Protection Agency.	On request, we have been informed that the Danish Data Protection Agency has not requested disclosure of the list during the declaration period.	
Procedure for transfers of personal data to third countries To maintain information security when transferring internally an organization and to external Stakeholders, according to ISO/IEC 27001 A.5.14 and GDPR Articles 44-49.	▶ There are written procedures that require the Data Processor to transfer personal data only to third countries or international organisations in accordance with the agreement with the Data Controller on the basis of a valid transfer basis. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place to ensure that personal data is only transferred to third countries or international organisations in accordance with an agreement with the Data Controller based on a valid basis for transfer. We have inspected that the procedures have been updated and approved during the declaration period.	No exceptions noted.
Instructions for the transfer of personal data to third countries To maintain information security when transferring internally an organization and to external Stakeholders, according to ISO/IEC 27001 A.5.14 and GDPR Articles 44-49.	▶ The Data Processor may only transfer personal data to third countries or international organisations on the instructions of the Data Controller.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place to ensure that personal data is only transferred to third countries or international organisations in accordance with an agreement with the Data Controller based on a valid basis for transfer. We have inspected that the procedures have been updated and approved during the declaration period.	No exceptions noted.

A.5 Organisational measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Valid transfer basis To maintain information security when transferring internally an organization and to external Stakeholders, according to ISO/IEC 27001 A.5.14 and GDPR Article 28(3)(a) and Articles 44-49.	▶ In connection with the transfer of personal data to third countries or international organisations, the Data Processor has assessed and documented that a valid basis for transfer exists.	We have made inquiries with relevant personnel. We have inspected that the Data Processor has assessed and documented that there is a valid basis for transfer in connection with the transfer of personal data to third countries or international organisations.	No exceptions noted.
Managing access and reviewing access rights To ensure authorized access and prevent unauthorized access to information and supporting assets, in accordance with ISO/IEC 27001 A.5.15 and 5.18 and GDPR Article 28(3)(c).	▶ The Data Processor has implemented a procedure for user administration that ensures that user creations and closures follow a controlled process, and that all user creations are authorized and are based on a work-related need. ▶ Privileged (administrative) access rights are granted to systems and devices based on work-related needs. ▶ Users' access is regularly reviewed, including that rights can still be justified by a work-related need.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place for granting and discontinuing users' access to systems and databases used for the processing of personal data. During the declaration period, we have by random samples inspected that the employees' access to systems where personal data is processed has been approved and that the employees have a work-related need for access. During the declaration period, we have by random samples inspected resigned employees to ensure that their removal of access to systems and databases has been deactivated or discontinued in due time. During the declaration period, we have by a random sample inspected that privileged access to the Data Processors systems has been approved and that the employee has a work-related need for the access. We have inspected that the Data Processor has assessed and approved user access during the declaration period.	No exceptions noted.

A.5 Organisational measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Use of secret authentication information To ensure correct entity authentication and prevent errors in authentication processes, according to ISO/IEC 27001 A.5.17 and GDPR Article 28(3)(c).	▶ The Data Processor has established rules for password requirements, which must be followed by all employees as well as external consultants.	We have made inquiries with relevant personnel. We have inspected that users' access to carry out the processing of personal data is done through passwords that reflect the risk of the processing activity. We have inspected that multifactor authentication is configured for systems used for processing personal data.	No exceptions noted.
Sub-data processing agreement and instructions To maintain an agreed level of information security in supplier relationships, in accordance with ISO/IEC 27001 A.5.19, A.5.20 and A.5.21 and GDPR Article 28(3)(c).	▶ There are written procedures that contain requirements for the Data Processor when using sub-processors, including requirements for sub-data processing agreements and instructions. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have made inquiries with relevant personnel. We have inspected that there are formalised procedures for the use of sub-processors, including requirements for sub-data processing agreements and instructions. We have inspected that the procedures have been updated and approved during the application period.	No exceptions noted.
Approval of sub-processors To ensure compliance with legal, regulatory, regulatory, and contractual requirements related to information security, according to ISO/IEC 27001 A.5.19, A.5.20 and A.5.21 and GDPR Article 28(3)(c).	▶ The Data Processor only uses sub-processors for the processing of personal data that has been specifically or generally approved by the Data Controller.	We have made inquiries with relevant personnel. We have inspected that the Data Processor has a comprehensive and updated overview of the sub-processors used. We have randomly inspected sub-processors from the Data Processor's overview of sub-processors to ensure that there is documentation that the sub-processors' data processing is stated in data processing agreements entered into with a Data Controller.	No exceptions noted.

A.5 Organisational measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Changes in approved sub-processors To ensure compliance with legal, regulatory, regulatory, and contractual requirements related to information security, according to ISO/IEC 27001 A.5.19, A.5.20 and A.5.21 and GDPR Article 28(3)(c).	▶ In the event of changes in the use of generally approved sub-processors, the Data Controller is informed in a timely manner in relation to being able to object and/or withdraw personal data from the Data Processor. In the event of changes in the use of specifically approved sub-processors, this is approved by the Data Controller.	We have made inquiries with relevant personnel. We have inspected that there are formalised procedures for notifying the Data Controller of changes in the use of sub-processors. We have upon inquiry been informed that the Data Processor has added a new sub-processor in the declaration period. We have inspected that the Data Controllers were informed of the new sub-processor in accordance with the requirements outlined in the data processing agreement.	No exceptions noted.
The sub-processor's obligations To maintain an agreed level of information security in supplier relationships, in accordance with ISO/IEC 27001 A.5.19, A.5.20 and A.5.21 and GDPR Article 28(3)(c).	▶ The Data Processor has imposed on the sub-processor the same data protection obligations as those provided for in the Data Processing Agreement or similar with the Data Controller.	We have made inquiries with relevant personnel. We have inspected that data processing agreements have been entered into with the sub-processors used. We have randomly inspected sub-data processing agreements to ensure that these contain the same requirements and obligations as are stated in the data processing agreements between the Data Controllers and the Data Processor.	No exceptions noted.
Overview of sub-processors To maintain an agreed level of information security in supplier relationships, in accordance with ISO/IEC 27001 A.5.19, A.5.20 and A.5.21 and GDPR Article 30(2).	▶ The Data Processor has a list of approved sub-processors stating: • Name • CVR no. • Address • Description of the treatment.	We have made inquiries with relevant personnel. We have inspected that the Data Processor has a comprehensive and updated overview of used and approved sub-processors.	No exceptions noted.

A.5 Organisational measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
		We have inspected that the overview contains at least the required information about the individual sub-processors.	
Supervision of sub-processors To maintain an agreed level of information security in supplier relationships, in accordance with ISO/IEC 27001 A.5.22 and GDPR Article 28(3)(c).	▶ On the basis of an updated risk assessment of the individual sub-processor and the activity carried out by the sub-processor, the Data Processor conducts an ongoing follow-up of this at meetings, inspections, review of the audit statement or similar. ▶ The Data Controller is informed of the follow-up that has been carried out at the sub-processor.	We have made inquiries with relevant personnel. We have inspected documentation that a risk assessment has been made of the individual sub-processor and the current processing activity of the sub-processor. We have inspected that the Data Processor has carried out supervision, including obtaining and reviewing the sub-Data Processor's auditor's statements, certifications and the like. We have inspected that the Data Processor's supervision of sub-processors has not given rise to any further action.	No exceptions noted.
Notification of personal data breaches To ensure effective categorization and prioritization of information security incidents, as well as to ensure effective handling of information security incidents, in accordance with ISO/IEC 27001 A.5.25 and A.5.26 and GDPR Article 28(3)(c).	▶ There are written procedures that require the Data Processor to notify the Data Controllers in the event of a personal data breach. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have made inquiries with relevant personnel. We have inspected that there are formalized procedures that contain requirements for notifying the Data Controllers in the event of a personal data breach. We have inspected that the procedure has been updated and approved. We have inspected that the Data Processor has an overview of security incidents with an indication of whether the individual incident has resulted in a breach of personal data security. We have upon inquiry been informed that there have been no personal data breaches in the declaration period.	We have established that there have not been any personal data breaches during the declaration period. We are therefore unable to test the implementation and efficiency of this control. No exceptions noted.

A.5 Organisational measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Identifying personal data breaches To ensure effective categorization and prioritization of information security incidents, in accordance with ISO/IEC 27001 A.5.25 and GDPR Article 28(3)(c).	▶ The Data Processor has set up measures to identify breaches of personal data security.	We have made inquiries with relevant personnel. We have inspected that the Data Processor provides awareness training to employees in relation to the identification of any personal data breaches. We have inspected documentation to ensure that there is timely follow-up on logging of access to personal data, including follow-up on repeated attempts at access.	No exceptions noted.
Assistance to Data Controllers in the event of a personal data breach To ensure uniform and effective management of evidence in relation to information security incidents in connection with sanctions and court proceedings, as well as to ensure effective management of information security incidents, in accordance with ISO/IEC 27001 A.5.26 and A.5.27 and GDPR Article 28(3)(c).	▶ The Data Processor has established procedures for assistance to the Data Controller in its notification to the Danish Data Protection Agency: • The nature of personal data breach • Likely consequences of personal data breach Measures that have been taken or are proposed to be taken to deal with the breach of personal data security.	We have made inquiries with relevant personnel. We have inspected that the procedures available for notifying Data Controllers in the event of a personal data breach contain detailed procedures for: • Description of the nature of personal data breach • Description of the likely consequences of personal data breach • Description of measures taken or proposed to be taken to deal with the personal data breach. We have upon inquiry been informed that there have been no personal data breaches in the declaration period.	We have established that there have not been any personal data breaches during the declaration period. We are therefore unable to test the implementation and efficiency of this control. No exceptions noted.

A.5 Organisational measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Timely notification of personal data breaches To ensure effective management of information security incidents, in accordance with ISO/IEC 27001 A.5.25 and GDPR Article 28(3)(c).	▶ The Data Processor notifies the Data Controller of a breach of personal data security without undue delay.	We have made inquiries with relevant personnel. We have inspected that the Data Processor has an overview of security incidents with an indication of whether the individual incident has resulted in a breach of personal data security. We have upon inquiry been informed that there have been no personal data breaches in the declaration period.	We have established that there have not been any personal data breaches during the declaration period. We are therefore unable to test the implementation and efficiency of this control. No exceptions noted.
Procedure for processing personal data To ensure that the Data Processor's processing of personal data is done in accordance with the Data Controller's instructions to maintain lawfulness, integrity and confidentiality of the processing, in accordance with GDPR Article 28(3).	▶ There are written procedures that require that personal data may only be processed when there is an instruction. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have made inquiries with relevant personnel. We have inspected that there is a formalised procedure in place to ensure that the processing of personal data only takes place in accordance with instructions. We have inspected that the procedure includes a requirement for a minimum annual assessment of the need for updating, including changes in the Data Controller's instructions or changes in data processing. We have inspected that the procedure has been updated, and management approved during the declaration period.	No exceptions noted.
Compliance with instructions for processing personal data To ensure compliance with legal, regulatory, regulatory, and contractual requirements in relation to the information security aspects of personal data protection, according to ISO/IEC 27001 A.5.34 and GDPR Articles 28(3), 29, and 32(4).	▶ The data processing agreement contains instructions from the Data Controller. ▶ The Data Processor only performs the processing of personal data that is stated in the instructions from the Data Controller.	We have made inquiries with relevant personnel. We have randomly inspected data processing agreements entered into with Data Controllers during the declaration period and observed that the agreements contain instructions from the Data Controllers.	No exceptions noted.

A.5 Organisational measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
		We have inspected the Data Processor's record of processing activities and randomly inspected that the processing takes place in accordance with instructions from the Data Controller.	
Agreed security measures To ensure compliance with legal, regulatory, regulatory, and contractual requirements in relation to information security, according to ISO/IEC 27001 A.5.31 and GDPR Article 28(3)(c).	▶ There are written procedures that require that agreed safeguards are put in place for the processing of personal data in accordance with the agreement with the Data Controller. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place to ensure that the agreed security measures are put in place. We have inspected that procedures have been updated and approved during the declaration period. We have by random samples inspected that data processing agreements entered into with Data Controllers defines requirements for agreed security measures.	No exceptions noted.
Notification of the Data Controller in the event of an unlawful instruction To ensure that any instructions that are in breach of applicable data protection legislation are detected and dealt with in a timely manner, in order to protect the rights of data subjects and maintain the lawfulness of the data processing, in accordance with GDPR Article 28(3)(h).	▶ The Data Processor shall immediately notify the Data Controller in cases where the Data Controller's instructions are in conflict with data protection legislation.	We have made inquiries with relevant personnel. We have inspected the Data Processor's template for entering into data processing agreements with the Data Controller and randomly selected data processing agreements with a Data Controller and observed that the Data Processor is obliged to notify the Data Controller in cases where an instruction is deemed to conflict with the law. We have by inquiry been informed that during the declaration period there have been no cases where instructions have been assessed contrary to legislation.	We have found that there have been no cases where instructions have been assessed as contrary to legislation. We are therefore unable to test the implementation and efficiency of this control. No exceptions noted.

A.5 Organisational measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Procedure for fulfilling the rights of data subjects To ensure compliance with legal, regulatory, regulatory and contractual requirements in relation to the information security aspects of the protection of personal data, according to ISO/IEC 27001 A.5.34 and GDPR Article 28(3)(e).	▶ There are written procedures that require the Data Processor to assist the Data Controller in relation to the rights of the data subjects. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have made inquiries with relevant personnel. We have inspected that there are formalised procedures in place for the Data Processor's assistance of the Data Controller in relation to the rights of the data subjects. We have inspected that the procedures have been updated and approved during the declaration period.	No exceptions noted.
Technical measures for the fulfilment of data subjects' rights To ensure compliance with legal, regulatory, regulatory and contractual requirements in relation to the information security aspects of the protection of personal data, according to ISO/IEC 27001 A.5.34 and GDPR Article 28(3)(e).	▶ The Data Processor has established procedures which, to the extent agreed, enable timely assistance to the Data Controller in relation to the disclosure, correction, deletion or restriction of, and information about the processing of, personal data to the data subject.	We have made inquiries with relevant personnel. We have inspected that the available procedures for assistance to the Data Controller contain detailed procedures for: • Disclosure of information • Correction of information • Deletion of information • Restriction of processing of personal data • Information about the processing of personal data for the data subject. We have inspected that the Data Processor has made assistance in relation to the rights of the data subjects during the declaration period.	No exceptions noted.

A.5 Organisational measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Storage of information is in accordance with the Data Controller's requirements To ensure compliance with legal, regulatory, regulatory, and contractual *requirements* in relation to information security, according to ISO/IEC 27001 A.5.31 and GDPR Article 28(3)(c).	▶ There are written procedures that require that personal data is only stored in accordance with the agreement with the Data Controller. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have made inquiries with relevant personnel. We have inspected that there are formalised procedures for only storing and processing personal data in accordance with the data processing agreements. We have inspected that the procedures have been updated and approved during the declaration period.	No exceptions noted.
Location of processing and storage of information To ensure compliance with legal, regulatory, regulatory, and contractual *requirements* in relation to information security, according to ISO/IEC 27001 A.5.31 and GDPR Article 28(3).	▶ The data processing by the Data Processor, including storage, may only take place in the locations, countries or territories approved by the Data Controller.	We have made inquiries with relevant personnel. We have inspected data processing from the Data Processor's overview of processing activities to ensure that there is documentation that the data processing, including storage of personal data, is only carried out at the locations stated in the data processing agreements – or has otherwise been approved by the Data Controller.	No exceptions noted.

A.6 Person-related measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Recruitment of employees - Screening To ensure that all employees are fit for the roles for which they are considered and remain fit during their employment, in accordance with ISO/IEC 27001 A.6.1 and GDPR Article 28(1).	▶ The Data Processor carries out screening and background checks on all job candidates in accordance with the Data Processor's procedure and the function that the job candidate must hold.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place to ensure the performance of screening and background checks of the Data Processor's employees in connection with employment. We have randomly inspected that the Data Processor has carried out verification of candidates before employment, and that the checks have included relevant documentation.	No exceptions noted.
Recruitment of employees - Confidentiality and confidentiality agreement with employees To maintain the confidentiality of information accessible to employees or external parties in accordance with ISO/IEC 27001 A.6.6 and GDPR Articles 28(1) and 28(3)(b).	▶ The Data Processor carries out screening and background checks on all job candidates in accordance with the Data Processor's procedure and the function that the job candidate must hold.	We have made inquiries with relevant personnel. During the declaration period, we have randomly inspected that the employees in question have signed a requirement for professional secrecy in the employment contract.	No exceptions noted.
Awareness, education and training regarding information security To ensure that employees and relevant stakeholders are aware of and live up to their information security responsibilities, in accordance with ISO/IEC 27001 A.6.3 and GDPR Article 28(1).	▶ An introductory course is being held for new employees, including on the processing of Data Controllers' personal data. ▶ The Data Processor continuously conducts awareness, training and education of employees in relation to data protection and information security.	We have made inquiries with relevant personnel. We have inspected that the Data Processor is conducting an introductory course for new employees, including on the processing of Data Controllers' personal data. We have inspected that the Data Processor conducts ongoing awareness, training and education of employees covering general IT security and processing security in relation to personal data.	No exceptions noted.

A.6 Person-related measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
		We have inspected documentation that all employees who either have access to or process personal data have completed the training offered.	
Resignation of employees - information about confidentiality and professional secrecy To maintain the confidentiality of information accessible to employees or external parties in accordance with ISO/IEC 27001 A.6.6 and GDPR Articles 28(1) and 28(3)(b).	▶ Upon resignation, the employee is informed that the signed confidentiality agreement is still valid.	We have made inquiries with relevant personnel. During the declaration period, we have inspected that the Data Processor has informed the resigned employees that the duty of confidentiality continues to apply after termination of employment.	No exceptions noted.
Termination of employees - withdrawal of access rights and assets To protect the interests of the organization as part of the modification or termination of the employment relationship or contracts, in accordance with ISO/IEC 27001 A.6.5 and GDPR Article 28(1).	▶ Upon resignation, a process has been implemented by the Data Processor to ensure that the user's rights become inactive or cease, including that assets are confiscated.	We have made inquiries with relevant personnel. We have inspected procedures that ensure that the rights of resigned employees are inactivated or terminated upon resignation, and that assets such as access cards, computers, mobile phones, etc. are confiscated During the declaration period, we have inspected resigned employees to ensure that rights have been inactivated or terminated, and that assets have been withdrawn in a timely manner.	No exceptions noted.

A.7 Physical measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Physical access control To ensure that only authorized physical access is made to the organization's information and supporting assets, according to ISO/IEC 27001 A.7.2 and GDPR Article 28(3)(c).	▶ Physical access controls have been established to prevent the likelihood of unauthorised access to the Data Processor's offices, facilities and personal data, including ensuring that only authorised persons have access.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place to ensure that only authorised persons can gain physical access to the Data Processor's premises. We have inspected documentation supporting that only authorised persons have physical access to premises.	No exceptions noted.
Repair, service and destruction of IT equipment To avoid loss, damage, theft or compromise of information and supporting assets as well as operational disruptions in the organization due to lack of maintenance, according to ISO/IEC 27001 A.7.13 and GDPR Article 28(3)(c).	▶ The Data Processor has established a procedure for repair, service and destruction of IT equipment that ensures secure handling of IT equipment containing personal data. ▶ The Data Processor sends IT equipment for repair and service without any personal data. ▶ The Data Processor disposes of IT equipment by physical destruction of data-bearing media or carries out secure deletion of data on data-bearing media.	We have made inquiries with relevant personnel. We have inspected that the Data Processor has formalised procedures for repair, service and destruction of IT equipment. Upon inquiry, we have been informed that no IT equipment has been sent for repair, service or destruction during the declaration period.	We have established that the Data Processor has not sent IT equipment for repair, service or destruction. We are therefore unable to test the implementation and efficiency of this control. No exceptions noted.

A.8 Technological measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Secure authentication To ensure that a user or entity is securely authenticated when accessing systems, applications and services, in accordance with ISO/IEC 27001 A.8.5 and GDPR Article 28(3)(c).	▶ The Data Processor has established logical access control to systems with personal data, including two-factor authentication.	We have made inquiries with relevant personnel. We have inspected that the Data Processor has established logical access control to systems with personal data, including the use of two-factor authentication.	No exceptions noted.
Monitoring of systems and environments To ensure the necessary capacity within information processing facilities, HR, offices and other facilities, as well as to detect abnormal behaviour and potential information security incidents, in accordance with ISO/IEC 27001 A.8.6 and A.8.16 and GDPR Article 28(3)(c).	▶ For the systems and databases used for the processing of personal data, system monitoring with alarms has been established. The monitoring includes: • uptime • access • performance and capacity	We have made inquiries with relevant personnel. We have inspected that systems and databases used for the processing of personal data have established system monitoring, including uptime, performance and capacity, with alarms. We have inspected that the Data Processor follows up on alarms.	No exceptions noted.
Antivirus program To ensure that information and supporting assets are protected from malware, in accordance with ISO/IEC 27001 A.8.7 and GDPR Article 28(3)(c).	▶ Antivirus is installed for the workstations and systems used for the processing of personal data, which is continuously updated.	We have made inquiries with relevant personnel. We have randomly inspected that for PCs used for the processing of personal data, antivirus has been installed and that the antivirus has been updated.	No exceptions noted.
Data backup and recovery To enable recovery after loss of data or systems, in accordance with ISO/IEC 27001 A.8.13 and GDPR Article 28(3)(c).	▶ The Data Processor has established a procedure for backup and re-establishment of data and systems that ensures that relevant systems and data are backed up and stored at another physical location, and that systems and data can be re-established.	We have made inquiries with relevant personnel. We have inspected that formalized procedures are in place to ensure backup and restoration of relevant data and systems, and that backups are stored in another physical location.	No exceptions noted.

A.8 Technological measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
		We have inspected that backups of relevant systems and data are made in accordance with the procedure. We have inspected that backups have been restored during the declaration period.	
Logging To record incidents, generate evidence, ensure the integrity of log information, prevent unauthorized access, identify information security incidents that may lead to an information security incident, and support investigations, in accordance with ISO/IEC 27001 A.8.15 and GDPR Article 28(3)(c).	▶ All successful and unsuccessful access attempts to the Data Processor's systems and data are logged. ▶ All user changes in the system and databases are logged. ▶ The Data Processor monitors and logs network traffic. ▶ Log information is protected from manipulation and technical errors and is reviewed on an ongoing basis.	We have made inquiries with relevant personnel. We have inspected that logging of user activities in systems, databases and networks used for the processing and transmission of personal data is configured and enabled. We have inspected that collected information about user activity in logs is protected from manipulation and deletion. We have inspected that only authorized personnel can access logs. We have inspected that there are alarms on logs.	No exceptions noted.
System Software Maintenance To ensure the integrity of test and production systems and prevent the exploitation of technical vulnerabilities, according to ISO/IEC 27001 A.8.19 and GDPR Article 28(3)(c).	▶ Changes to systems, workstations, databases, and networks follow established procedures that ensure maintenance with relevant updates and patches, including security patches.	We have made inquiries with relevant personnel. We have inspected by extraction that databases and networks are updated with relevant updates and security patches. We have randomly inspected that a workstation is updated with the latest system update. We have inspected that the Data Processor has implemented continuous vulnerability scans and maintains a comprehensive overview of vulnerability patches.	No exceptions noted.

A.8 Technological measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Firewall To ensure security in the use of network services, as well as to divide the network with security boundaries and manage traffic between them based on business needs, according to ISO/IEC 27001 A.8.21 and A.8.22 and GDPR Article 28(3)(c).	▶ The Data Processor has configured the firewall correctly according to best-practice standards. ▶ The Data Processor only uses services/ports that they need.	We have made inquiries with relevant personnel. We have inspected that external access to systems and databases used for the processing of personal data is only through the firewall. We have inspected that the firewall is configured according to internal policy for this.	No exceptions noted.
Network security To divide the network with security boundaries and manage traffic between them based on business needs, according to ISO/IEC 27001 A.8.22 and GDPR Article 28(3)(c).	▶ Internal networks are segmented to ensure limited access to systems and databases used for the processing of personal data.	We have made inquiries with relevant personnel. We have inspected the Data Processor's network topology and observed that networks are segmented to ensure limited access to systems and databases used for the processing of personal data. We have inspected documentation that the Data Processor's network is set up in accordance with the network topology.	No exceptions noted.
Remote workplaces and remote access to systems and data To ensure security in the use of network services, in accordance with ISO/IEC 27001 A.8.21 and A.8.22 and GDPR Article 28(3)(c).	▶ External access to systems and databases used for the processing of personal data is done by VPN connection.	We have made inquiries with relevant personnel. We have inspected the Data Processor's network topology and observed that remote access to systems and data can only be achieved through VPN. We have inspected documentation that the Data Processor's network is set up in accordance with the network topology. We have observed documentation that access to the VPN connection is done with established security measures.	No exceptions noted.

A.8 Technological measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
Encryption when transmitting personal data To ensure the correct and effective use of cryptography to protect the confidentiality, authenticity or integrity of information in accordance with business and information security requirements, according to ISO/IEC 27001 A.8.24 and GDPR Article 28(3)(c).	▶ Encryption is used for the transmission of confidential and sensitive personal data via the internet and e-mail.	We have made inquiries with relevant personnel. We have inspected the use of encryption for transmissions of sensitive and confidential personal data via the internet or by e-mail.	No exceptions noted.
Deletion of information in accordance with the Data Controller's requirements To prevent unnecessary exposure of sensitive information and to comply with legal, regulatory, regulatory, and contractual requirements for the deletion of information, as well as to ensure compliance with legal, regulatory, regulatory, and contractual requirements related to information security, in accordance with ISO/IEC 27001 A.8.10 and A.5.31 and GDPR Article 28(3)(g).	▶ There are written procedures that require that personal data is stored and deleted in accordance with the agreement with the Data Controller. ▶ An assessment is made on an ongoing basis – and at least once a year – as to whether the procedures need to be updated.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place for the storage and deletion of personal data in accordance with the agreement with the Data Controller. We have inspected that the procedures have been updated and approved during the declaration period.	No exceptions noted.
Requirements for the storage and deletion period of data are in accordance with the Data Controller's requirements To prevent unnecessary exposure of sensitive information and to comply with legal, regulatory, regulatory, and contractual requirements for the deletion of information, as well as to ensure compliance with legal, regulatory, regulatory, and contractual requirements related to information security, in accordance with ISO/IEC 27001 A.8.10 and A.5.31 and GDPR Article 28(3)(g).	▶ The following specific requirements have been agreed for the Data Processor's storage periods and deletion routines: • Data is deleted upon termination of the data processing services.	We have made inquiries with relevant personnel. We have inspected that the available procedures for storing and deleting personal data contain specific requirements for the Data Processor's retention periods and deletion routines. We have inspected data processing from the Data Processor's record of processing activities to ensure that there is documentation that personal data is stored in accordance with the agreed storage periods.	No exceptions noted.

A.8 Technological measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
		We have inspected data processing from the Data Processor's overview of processing activities to ensure that there is documentation that personal data has been deleted in accordance with the agreed deletion routines.	
Deletion and return upon termination of customer relationship To prevent unnecessary exposure of sensitive information and to comply with legal, regulatory, regulatory, and contractual requirements for the deletion of information, as well as to ensure compliance with legal, regulatory, regulatory, and contractual requirements related to information security, in accordance with ISO/IEC 27001 A.8.10 and A.5.31 and GDPR Article 28(3)(g).	▶ Upon termination of processing of personal data by the Data Controller, data in accordance with the agreement with the Data Controller are: • Returned to the Data Controller, and/or • Deleted where it does not conflict with other legislation.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place for the return and/or deletion of the Data Controller's data upon cessation of processing of personal data. On request, we have been informed that it is individually agreed with the customer how the treatment is carried out. On request, we have been informed that there has been no return of data during the withdrawal period.	We have established that there has been no return of data. We are therefore unable to test the implementation and efficiency of this control. No exceptions noted.
Change management and privacy-by-design To ensure that information security is organized and implemented in the secure development lifecycle of the software and systems, as well as to ensure that all information security requirements are identified and managed when developing or acquiring applications, and to validate whether information security requirements are met when applications or code are implemented in the production environment, as well as maintaining information security when performing changes, in accordance with ISO/IEC 27001 A.8.25, A.8.26, A.8.27, A.8.29 and A.8.32 and GDPR Article 25.	▶ The Data Processor has established a procedure for development and change tasks that ensure compliance with the privacy-by-design principles, and that all development and change tasks follow a formalized process that ensures testing and requirements for approval before implementation.	We have made inquiries with relevant personnel. We have inspected that the Data Processor has established a procedure for development and modification tasks that ensure compliance with the privacy-by-design principles, and that all development and modification tasks follow a formalized process that ensures testing and requirements for approval before implementation. We have randomly inspected implemented changes and found that compliance with the privacy-by-design principles has been ensured in the development/change task. We have also inspected that the changes have followed the for-	No exceptions noted.

A.8 Technological measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
		malised process, and that tests have been carried out and that the changes have been approved before implementation.	
Implementing change in the production environment To validate whether the information security requirements are met when applications or code are deployed in the production environment, as well as to maintain information security when performing changes, according to ISO/IEC 27001 A.8.29 and A.8.32 and GDPR Article 25.	▶ The Data Processor has established a procedure for implementing changes in the production environment that ensures separation of functions in the implementation process.	We have made inquiries with relevant personnel. We have inspected that there is a separation of functions so that developers cannot implement changes directly in the production environment.	No exceptions noted.
Separation of development, test and production environment To protect the production environment and data from compromise as a result of development and testing activities, according to ISO/IEC 27001 A.8.31 and GDPR Article 25.	▶ Development and testing are performed in development environments that are separate from production environments.	We have made inquiries with relevant personnel. We have inspected that the development, testing and production environments are separated.	No exceptions noted.
Access to source code To prevent unauthorized functionality, avoid accidental or harmful modifications, and maintain the confidentiality of valuable intellectual property, in accordance with ISO/IEC 27001 A.8.4 and GDPR Article 25.	▶ Source code is protected from unauthorized modification and deletion.	We have made inquiries with relevant personnel. We have inspected that only the Data Processor's developers have access to source code. We have inspected documentation that the source code is protected against unauthorized modification and deletion.	No exceptions noted.
Anonymisation of personal data in development tasks To ensure the relevance of testing and protection of operational information used for testing,	▶ Anonymized test data is used in the development and test environment.	We have made inquiries with relevant personnel.	No exceptions noted.

A.8 Technological measures			
Control objectives	**Control activity**	**Tests conducted by BDO**	**Test result**
according to ISO/IEC 27001 A.8.33 and GDPR Article 25.		We have been inspected that the Data Processor strictly uses fictional data during development and testing. We have observed that the data is anonymized and deleted after 31 days.	

BDO STATSAUTORISERET REVISIONSPARTNERSELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

PENNEO

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

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

Martin Eland Pløger
Executive
Serienummer: 920bff87-27da-4280-8d09-3f4383fc2b82
IP: 185.229.xxx.xxx
2026-05-29 08:13:38 UTC

Mit ID

Birol Altinok
Executive
Serienummer: 14a524ff-0318-45f4-9755-75fa8e5c965d
IP: 152.115.xxx.xxx
2026-05-29 08:28:21 UTC

Mit ID

Thomas Richard Hofmann
Chairman of the board
Serienummer: 92543bc8-b721-487f-acd5-3044efd86591
IP: 80.208.xxx.xxx
2026-06-01 10:00:19 UTC

Mit ID

Nicolai Tobias Visti Pedersen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Statsautoriseret revisor
På vegne af: BDO Statsautoriseret Revisionspartnerse…
Serienummer: c42f66e9-59bb-478a-9d92-2a2b8602724e
IP: 37.96.xxx.xxx
2026-06-01 11:22:13 UTC

Mit ID

Mikkel Jon Larssen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Partner
På vegne af: BDO Statsautoriseret Revisionspartnerse…
Serienummer: cd9a38dd-e75c-40f7-80d6-ec5b5d0841d6
IP: 77.243.xxx.xxx
2026-06-01 16:07:35 UTC

Mit ID