In The Heart Of ApS

ISAE 3000 Assurance Report 2022

ONLINECITY 00

ONE KEY TO THE CITY

gatewayapi

IN THE HEART OF APS

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD FROM 1 MAY 2021 TO 30 APRIL 2022 ON THE DESCRIPTION OF GATEWAYAPI AND THE RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN, RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH DATA PROTECTION ACT

BDO

CONTENTS

1 INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD FROM 1 MAY 2021 TO 30 APRIL 2022 ON THE DESCRIPTION OF GATEWAYAPI AND THE RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN, RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH DATA PROTECTION ACT

To: Management of In The Heart Of ApS
In The Heart Of ApS' Customers' (Controllers)

Scope

We have been engaged to report on In The Heart Of ApS' (the Processor) description for the period from 1 May 2021 to 30 April 2022 prepared description in section 3 of GatewayAPI and the related technical and organisational measures and other controls relating to processing and protection of personal data in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free interchange of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions the regulation (Data Protection Act), and on the design and operation effectiveness of the technical and organisational measures and other controls related to the control objectives stated in the above description throughout the period from 1. May 2021 to 30 April 2022.

The Data Processor's Responsibilities

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 Processor is responsible for providing the services covered by the description; stating the control objectives; and designing and implementing and effectively operating controls to achieve the stated control objectives.

Auditor's Independence and Quality Control

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

We are subject to the international standard on quality management ISQC 1, and we thus apply and maintain a comprehensive quality management system, including documented policies and procedures for compliance with ethical rules, professional standards and applicable requirements under law and other regulations.

Auditor's Responsibilities

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

We conducted our engagement in accordance with the International Standard on Assurance Engagement, Assurance 3000, "Reports Other Than Audits or Reviews of Historical Financial Information". That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed and operating effectively.

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

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

Limitations of Controls at a Data Processor

The Data Processor's Description is prepared to meet the common needs of a broad range of controllers and may not, therefore, include every aspect of the use of GatewayAPI that the individual data controller may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect all breaches of the personal data breach. Furthermore, the projection of any evaluation of the operating effectiveness of controls to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Data Processor's statement in section 2. In our opinion, in all material respects:

a. The description of GatewayAPI presents fairly the related technical and organisational measures and other controls relating to processing and protection of personal data according to the EU General Data Protection Regulation and the Data protection Act, as designed and implemented throughout for the period from 1 May 2021 to 30 April 2022.

b. The technical and organisational measures and other controls, relating to the control objectives stated in the description were appropriately designed throughout the period from 1 May 2021 to 30 April 2022 and.

c. The technical and organisational measures and other controls tested, which were necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from 1 May 2021 to 30 April 2022.

Description of Test of Controls

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

Intended Users and Purpose

This report is intended solely for data controllers, who have used the Data Processor GatewayAPI services, and who have a sufficient understanding to consider it, along with other information including information about the technical and organisational measures and other controls, operated by the data controllers themselves, when assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Copenhagen, 3 June 2022

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, State Authorized Public Accountant

Mikkel Jon Larssen
Partner, Head of Risk Assurance, CISA

2. IN THE HEART OF APS' STATEMENT

In The Heart Of ApS processes personal data for our Customers, who are Controllers according to the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions (the Danish Data Protection Act).

The description has been prepared for the information of Controllers who have used GatewayAPI, and who have a sufficient understanding to consider the description along with other information, including information about the technical and organisational measures and other controls operated by the Controllers themselves in assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

In The Heart Of ApS uses sub-processors. These sub-processors' relevant control objectives and related technical and organisational measures and other controls are not included in the accompanying description.

In The Heart Of ApS confirms that the accompanying description in section 3 fairly presents GatewayAPI and the related technical and organisational measures and other controls throughout the period from 1 May 2021 to 30 April 2022. The criteria used in making this statement were that the accompanying description:

1. Presents how GatewayAPI, and how the related technical and organisational measures and other controls were designed and implemented, including:
    - The types of services provided, including the type of personal data processed,
    - The processes in both IT systems and procedures which are used to process personal data and, if necessary, to correct and erase personal data and restrict processing of personal data,
    - The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the Controller,
    - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality,
    - The procedures ensuring upon discontinuation of data processing that, by choice of the Controller, all personal data are deleted or returned to the Controller unless retention of such personal data is required by law or regulation,
    - The procedures supporting in the event of breach of personal data security that the Controller may report this to the supervisory authority and inform the data subjects,
    - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed,
    - The controls that we, in reference to the scope of GatewayAPI, have assumed would be designed and implemented by the Controllers and which, if necessary, in order to achieve the control objectives stated in the description, 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 are relevant to the processing of personal data.

2. Includes relevant information on changes of the GatewayAPI system and the related technical and organisational measures and other controls throughout the period from 1 May 2021 to 30 April 2022.

3. Does not omit or distort information relevant to the scope of GatewayAPI and the related technical and organisational measures and other controls described while acknowledging that this description is prepared to meet the common needs of a broad range of Controllers and may not, therefore, include every aspect of GatewayAPI that the individual Controllers might consider important in their environment.

In The Heart Of ApS confirms that the technical and organisational measures and other controls related to the control objectives stated in the description were appropriately designed and operated effectively throughout the period from 1 May 2021 to 30 April 2022. The criteria used in making this statement were that the accompanying description:

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

2. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

3. The controls were consistently applied as designed, including those manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 May 2021 to 30 April 2022.

In The Heart Of ApS confirms that appropriate technical and organisational measures and other controls were implemented to comply with the agreements with Controllers, sound data processing practices and relevant requirements for data processors in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act.

København, 3 June 2022

In The Heart Of ApS

Birol Altinok
Executive, Partner

3. IN THE HEART OF APS' DESCRIPTION OF GATEWAYAPI

IN THE HEART OF APS

In The Heart Of is a Danish-owned business which develops and operates several online systems to municipalities and different industry sectors in the private market. In The Heart Of has offices in Odense, Aalborg, Copenhagen, and Munich, and wholly owns and operates the company ONLINECITY.IO ApS, which offers the product GatewayAPI.

I In The Heart Of has approximately 30 employees who are specialised in system development, server operation, support, and information security and who are organized in a development department, and operations and support department, a finance department and an administration department.

The GDPR officer and In The Heart Of's IT security committee manage In The Heart Of's personal data security in relation to the processing that In The Heart Of performs on behalf its customers, such as making data processing agreements, responding to request from the Controller, notification of breach of the personal data security, compliance with internal policies and procedures, and similar areas.

GATEWAYAPI AND PROCESSING OF PERSONAL DATA

In The Heart Of offers a SMS gateway as a Software-as-a-Service (SaaS) solution according to a contract with municipalities and private businesses. The SMS gateway is a system 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. In The Heart Of has made data processing agreements with these sub-processors.

In The Heart Of processes personal data on behalf of their customers, who are Controllers, when they use the platform SMS communication. In The Heart Of has made data processing agreements with the 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 number and test messages.

PERSONAL DATA MANAGEMENT

In The Heart Of 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 Controllers, generally accepted data processing practice and relevant requirements for applying to Processors according to GDPR and the Data Protection Act.

The technical and organizational security measures and other controls for protection of personal data are designed according to risks 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 organizational measures and other controls are structured in the following main areas, for which control objectives and control activities have been defined:

ARTICLE	AREA
Article 28(1)	Data Processor's guarantees
Article 28(3)	Data processing agreement
Article 28(3)(a and h) and 28(10) Article 29 Article 32(4)	Instruction for processing of personal data
Article 28(2 and 4)	Sub-processors
Article 28(3)(b)	Secrecy and statutory obligation of confidentiality
Article 28(3)(c)	Technical and organisational measures
Article 25	Data protection by design and by default
Article 28(3)(g)	Erasure and return of personal data
Article 28(3)(e, f and h)	Assistance to the Controller
Article 30(2, 3 and 4)	Record of categories of processing activities
Article 33(2)	Notification of breach of personal data security
Articles 44 to 49	Transfer of personal data to third countries

RISK ASSESSMENT

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

There is a current assessment of which security level that is appropriate. This assessment considers risks relating to the 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. The risk assessment addresses 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 MEASURES AND OTHER CONTROLS

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

The Data Processor's guarantees

In The Heart Of has implemented policies and procedures to ensure that In The Heart Of can provide sufficient guarantees to carry out suitable technical and organizational measures in such a manner that the processing meets the requirements in GDPR and ensures protection of the data subject's rights. In The Heart Of has established an organization of the personal data security and prepared and implemented an information security policy, approved by Management, which is reviewed and updated on a current 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.

Data processing agreements with the Controller

In The Heart Of has implemented policies and procedures for making data processing agreements, which ensure that In The Heart Of 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. In The Heart Of 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.

Instruction for processing of personal data

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

Sub-processors

In The Heart Of 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 In The Heart Of, 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.

In The Heart Of 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 In The Heart Of. In The Heart Of carries out an annual inspection its 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.

Secrecy and statutory duty of confidentiality

In The Heart Of has implemented policies and procedures to ensure confidentiality in the processing of personal data. All personnel at In The Heart Of 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 of personal data and IT security.

Technical and organizational security measures

Risk assessment
In The Heart Of has implemented the technical and organizational security measures based on an assessment of risks relating to confidentiality, integrity and accessibility. We refer to separate description hereof.

Contingency plans
In The Heart Of has established contingency plans, so that In The Heart Of can in time restore the accessibility of and access to personal data in the event of physical or technical incidents. In The Heart Of has established an emergency alert, which becomes effective in such cases. An organization of the emergency alert team has been established and guidelines for activation of the emergency alert have been implemented.

In The Heart Of has designed detailed contingency plans and plans for restore of systems and data, which among others ensure independence of persons in connection with activation of the alert and the restore. A

copy of the plans is kept safe outside In The Heart Of's IT systems. The plans are tested and audited regularly in connection with modifications to systems, etc.

Physical security, including physical access control
In The Heart Of 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 are processed. Customers, suppliers, and other visitors are escorted.

Authorization and rights management
In The Heart Of has implemented procedures to ensure that access to systems and data is 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. Procedures and controls support the process for creation, change and removal of users and allocation of rights and examination hereof.

Remote access to systems and data
In The Heart Of has implemented procedures to ensure that access from workplaces outside In The Heart Of'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 In The Heart Of's premises to all external services uses today HTTPS, which ensures encryption and prevents leak of information which is accessed via the business' Google-account with 2-factor-authentification.

Logical access control
In The Heart Of has implemented procedures to ensure that access to systems and data is via logical controls. The users' continued work-related need for access is evaluated at least once a year, including the relevance and correctness of allocated user rights. Procedures and controls support the process for creation, change and removal of users and allocation of rights and examination hereof.

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.

Encryption of personal data
In The Heart Of has implemented procedures to ensure that databases containing personal data are encrypted, and this also applies to backups. Restore keys and certificates are kept properly.

In The Heart Of has implemented procedures to ensure that data on personal units, which are not protected by special security measures, are encrypted when they are put into use, so that access to data is solely possible for authorized users. Restore keys and certificates are kept properly.

The algorithms and levels of encryption used for encryption of units, servers and data, are currently subject to risk assessment in relation to the current threat scenario.

Network security
In The Heart Of has implemented procedures to ensure that network 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.

In The Heart Of 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 local firewall.

External communication lines
In The Heart Of has implemented procedures to ensure that external communication lines are safeguarded by a 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.

Antivirus
In The Heart Of has implemented procedures to ensure that units with access to network and applications are protected from virus and malware. There is current updating and adjustment of antivirus programs and other protection systems in relation to the current threat scenario, and there is current monitoring of these systems, including periodical test of operating reliability.

Backup and restore of data
In The Heart Of 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 come into the hands of third parties, or that backups are destroyed by fire, water, vandalism, or accidental damage.

Maintenance of system software
In The Heart Of has implemented procedures to ensure that system software is updated currently according to the suppliers' directions and recommendations. Procedures for Patch Management include operating systems, critical services and software installed on servers and workstations.

Logging in systems, databases and network
In The Heart Of 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 are sufficient to identify and prove a potential abuse of systems or data, and log data are examined currently for applicability and anormal behaviors. Log data are protected against loss and erasure.

Monitoring
In The Heart Of has implemented procedures to ensure that systems are monitored currently and that technical security measures have been implemented.

Repair, service and disposal of IT equipment
In The Heart Of has implemented procedures to ensure that equipment handed over to third party for service or repair are handed over with encrypted data disks, and that used or abandoned data media or disks are registered and destroyed by us by using a drilling machine and documentation would be in the form of a photo of the rotary disk with a hole in it.

Data protection by design and by default

In The Heart Of 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/or return of personal data

In The Heart Of has implemented policies and procedures to ensure that personal data are deleted or returned in accordance with instruction from the Controller when the processing of personal data ends at expiry of the contract with the Controller.

Assistance to Controller

In The Heart Of has implemented policies and procedures to ensure that In The Heart Of can assist the Controller meeting the Controller's obligation to respond to requests for exercise of the data subject's rights.

In The Heart Of has implemented policies and procedures to ensure that In The Heart Of 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 the personal data security, and Articles 34 to 36 on impact assessments.

In The Heart Of has implemented policies and procedures to ensure that In The Heart Of can make available to the Controller all information required to prove compliance with the requirements applying to data processors. In The Heart Of also allows and contributes to audits, including inspections, performed by the Controller or other parties authorised to do so by the Controller.

Record of categories of processing activities

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

Notification of breach of personal data security

In The Heart Of has implemented policies and procedures to ensure that breach of the personal data security is registered with detailed information on the incident, and that the Controller is notified without undue delay after In The Heart Of became aware of the breach of the 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.

Transfer of personal data to third countries

In The Heart Of 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.

CHANGES TO THE SYSTEM DESCRIPTION, CONTROLS, RULES AND POLICIES OR BREACH THROUGHOUT THE PERIOD OF AUDIT

The Period of Audit from 1 May 2021 to 30 April 2022 has included no major changes to our System Description nor Information Security Policy. Policies, rules, and controls have been updated accordingly to meet requirements during the audit period, but no major alteration has been applied or implemented.

Throughout the audit period, there have been no data breaches to the SMS gateway system.

COMPLEMENTARY CONTROLS AT THE CONTROLLERS

The Controller is under an obligation to implement the following technical and organizational measures and other controls to achieve the control objectives and to 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 administrator 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.

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND RESULT OF TESTS

Objective and scope

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

BDO has performed procedures to obtain evidence of the information in In The Heart Of ApS' description of GatewayAPI and the design and operating effectiveness of the relating technical and organisational measures and other controls. The procedures elected depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not appropriately designed and operating effectively.

BDO's test of the design and the operating effectiveness of the relating technical and organisational measures and other controls and their implementation and operating effectiveness has included the control objectives and related control activities selected by In The Heart Of ApS, and which are described in the check form below.

In the test form, BDO has described the tests carried out which were assessed necessary to obtain reasonable assurance that the stated control objectives were achieved, and that the related controls were appropriately designed and operated effectively throughout the period from 1 May 2021 to 30 April 2022.

Test procedures

Test of the design of the relating technical and organisational measures and other controls and their implementation was performed by inquiries, inspection, observation, and re-performance.

Type	Description
Inquiry	Inquiries of relevant personnel have been performed for all significant control activities. The purpose of the inquiries was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures, and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, i.e., whether the design of the controls is such that they are expected to be effective, if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals. Tests have been performed of significant system structures of technical platforms, databases and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations 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 control has been implemented.
Re-performance	Controls have been re-performed to obtain additional evidence that the controls operate as assumed.

With respect to the services provided by Hetzner Online GmbH, and Google Cloud Web Hosting within the respective sub-processors' services, we have received TÜV reports, SOC3, SOC2 and SOC1 auditor's reports or other documentation for the relevant sub-processor's technical and organizational measures and other controls.

These sub-processors' relevant control objectives and related controls of these service sub-processors are not included in in In The Heart Of ApS' description of GatewayAPI and the related technical and organisational measures and other controls. Thus, we have solely inspected the documentation received and

tested the controls at In The Heart Of ApS, which ensure appropriate supervision of 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.

Result of test

The result of the test made of technical and organisational measures and other controls has resulted in the following exception noted.

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective,
- 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.

Article 28(1) – The Processor's Guarantees

Control objective

- *To ensure that the Processor can provide sufficient guarantees for protection of the Controller's personal data in accordance with the requirements of the EU General Data Protection Regulation and the protection of the rights of the data subject.*

Control activity	Test performed by BDO	Result of test
The Processor's guarantees ▶ The Processor has prepared and implemented an information security policy. ▶ The Processor has prepared and implemented an access code policy. ▶ The Processor has prepared and implemented a backup policy. ▶ The Processor has prepared and implemented a data protection policy. ▶ The Processor's policies are reviewed and updated as a minimum once a year. ▶ The Processor has prepared an annual cycle of work, which ensures continuous work and updating with IT security and documentation hereof.	We have interviewed relevant personnel at the Processor. We inspected the Processor's information security policy and observed that this has been reviewed during the period subject to audit. We inspected the Processor's access code policy and observed that this has been reviewed and updated during the period subject to audit. We inspected the Processor's backup policy and observed that this has been reviewed and updated during the period subject to audit. We inspected the Processor's data protection policy and observed that this has been reviewed and updated during the period subject to audit. We inspected the Processor's annual cycle of work and observed that the policies have been reviewed and updated during the period subject to audit and as a minimum once a year. We inspected the Processor's annual cycle of work and observed that the work with IT security and documentation hereof is included in the annual cycle of work content.	No deviations noted.
Recruitment of personnel ▶ The Processor has prepared a procedure for recruitment of personnel. ▶ The Processor ensures that new personnel are introduced to IT security via an on-boarding program.	We have interviewed relevant personnel at the Processor. We inspected the Processor's procedure for recruitment of personnel and observed that this has been reviewed and that it includes a description of the process for recruitment of personnel.	No deviations noted.

Article 28(1) – The Processor's Guarantees		
Control objective ▶ *To ensure that the Processor can provide sufficient guarantees for protection of the Controller's personal data in accordance with the requirements of the EU General Data Protection Regulation and the protection of the rights of the data subject.*		
Control activity	**Test performed by BDO**	**Result of test**
	We made a random inspection of documentation that a new employee has signed a confidentiality agreement, which agrees with the Processor's procedure. We inspected the Processor's procedure for education and training of personnel in relation to IT security and procedure for support tasks relating to personal data and awareness in IT security relating to customers. We selected a sample of documentation which confirms that new personnel are introduced the IT security via an on-boarding program. We inspected the Processor's annual cycle of work and observed that activities are planned in relation to IT security, and we observed that such activities have been carried out in the period subject to audit.	
Resigning personnel ▶ The Processor has prepared and implemented a procedure for resigning personnel. ▶ The Processor keeps records of personnel, who have left, in a resignation register. ▶ The Processor ensures that resigned personnel no longer have an active login.	We have interviewed relevant personnel at the Processor. We inspected the Processor's procedure for resigning personnel. We have observed controls which ensure that the login of resigned personnel is deleted. We inspected documentation for resigned personnel and observed that a register is kept hereof in accordance with the Processor's procedure. We observed that the resigned personnel do not appear in extract of personnel with active login. We have observed that accesses and relevant assets from resigned personnel have been withdrawn.	No deviations noted.

Article 28(1) – The Processor's Guarantees		
Control objective ▶ *To ensure that the Processor can provide sufficient guarantees for protection of the Controller's personal data in accordance with the requirements of the EU General Data Protection Regulation and the protection of the rights of the data subject.*		
Control activity	**Test performed by BDO**	**Result of test**
Awareness training of personnel in data protection ▶ The Processor has prepared documentation informing personnel about procedure and policies relating to processing of personal data. ▶ The Processor has prepared and implemented a procedure for training of personnel in relation to IT security. ▶ The Processor ensures that personnel receive awareness training in data protection.	We have interviewed relevant personnel at the Processor. We observed that the Processor has prepared the following documents which we have inspected: • Information security policy • Data protection policy We observed that the Processor's initiatives relating to information to personnel on procedure and policies relating to processing of personal data are described in those documents. We observed that the Processor's process for training of personnel in IT security is described, and that awareness campaigns and training are held within risk assessment and handling of personal data. We inspected documentation, which confirms that personnel receive awareness training in IT security and data protection, and we have inspected documentation for held training sessions.	No deviations noted.

Article 28(3) – Data Processing Agreements and Controllers

Control objective

- *To ensure that the Processor makes a written agreement with the Controller setting out the terms for the processing of the Controller's personal data and that the data processing agreement is stored in electronically.*

Control activity	Test performed by BDO	Result of test
Data processing agreements with the Controller ▶ The Processor has prepared and implemented a standard template which can be used for data processing agreements. ▶ The Processor has prepared and implemented a procedure for making data processing agreements. ▶ The Processor has prepared and implemented a procedure for management of sub-processors to ensure that this done according to agreement with the Controller. ▶ The Processor has made data processing agreements with the Controllers. ▶ The Processor ensures that data processing agreements made are stored electronically. ▶ A data processing agreement includes information on the use of sub-processors.	We have interviewed relevant personnel at the Processor. We inspected the Processor's template for data processing agreements and observed that it complies with the requirements for the content of a data processing agreement according to GDPR Art. 28(3). We inspected the procedure for making data processing agreements. We inspected the procedure for management of sub-processors and observed that written guidelines exist for making agreements with sub-processors, from which it appears the Controller is to be involved in connection with replacement of sub-processors. We inspected randomly selected data processing agreements. We observed that they were signed by both parties and complies with approved standard. We observed the data processing agreements made are stored electronically. We inspected randomly selected data processing agreements and observed that the agreements include information on the use of sub-processors depending on whether it is Google or Hetzner	No deviations noted.

Articles 28, 29 and 32 – Instruction for Processing of Personal Data

Control objectives

- *To ensure that the Processor processes personal data only according to documented instructions from the Controller.*
- *To ensure that the Processor notifies the Controller if an instruction infringes the EU General Data Protection Regulation and the Danish Data Protection Act.*

Control activity	Test performed by BDO	Result of test
Documented instruction from the Controller ▶ The Processor ensures that the Processor acts according to the instruction that the Controller has given in the data processing agreement. ▶ The Processor can document that only sub-processors who have been approved in writing are used. ▶ The data processing agreement includes information on how the Controller must be informed of instructions that infringe legislation.	We have interviewed relevant personnel at the Processor. We inspected the Processor's template for data processing agreements and observed that it states that the Processor must act according to the instruction that the Controller has given in the data processing agreement. We inspected relevant procedures and observed that they instruct the personnel how the processing of personal data must be made. We inspected randomly selected data processing agreements and observed that there is a list of the approved sub-processors. We inspected randomly selected agreements and observed that there is a list of the approved sub-processors. We made a random inspection of selected agreements with sub-processors and observed that these agreements have been signed by both parties. We inspected randomly selected data processing agreements and observed that the agreements include a paragraph on notification of the Controller of instructions that infringe legislation. On inquiry, we were informed that the Processor has not received any instructions which infringe the Regulation or the Data Protection Act. Thus, we have been unable to test whether the control has been implemented and operated effectively.	No deviations noted.

Article 28(2 & 4) - Sub-processors

Control objectives

- *To ensure that the sub-processor is subject to the same data protection obligations as set out in the contract between the Controller and the Processor, by making a written contract including instructions.*
- *To ensure that the Controller has given a prior specific or general written authorisation to the Processor to use sub-processors.*
- *To ensure that the sub-processor can provide the required guarantees for protection of personal data in accordance with the contract.*

Control activity	Test performed by BDO	Result of test
Agreements with and supervision of sub-processors ▶ The Processor has prepared and implemented a procedure for obtaining data processing agreements with sub-processors. ▶ The Processor has prepared a procedure for performance of supervision of sub-processors. ▶ The Processor obtains and examines annual reports and independent auditor's reports from sub-processors.	We have interviewed relevant personnel at the Processor. We inspected procedure for obtaining data processing agreements from sub-processors. We inspected randomly selected agreements with sub-processors and observed that these were signed by both parties. We inspected procedure for supervision of sub-processors. We inspected SOC2 reports for Google Cloud Web Hosting covering the period from 1 May 20202 to 30 November 2021 and observed that In the Heart of ApS has taken conclusion and deviations in the SOC2 report into consideration. We inspected TÜV report from Hetzner Online GmbH dated February 2022 and observed that In the Heart of ApS has taken the TÜV report into consideration.	No deviations noted.

Article 28 (3)(b) – Secrecy and Statutory Obligation of Confidentiality		
Control objective ▶ *To ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.*		
Control activity	**Test performed by BDO**	**Result of test**
Secrecy and confidentiality agreements for personnel and consultants ▶ The Processor has prepared and implemented a procedure for obtaining secrecy and confidentiality agreements with personnel processing personal data. ▶ The Processor ensures that personnel at commencement of their employment sign a secrecy and confidentiality agreement.	We have interviewed relevant personnel at the Processor. We inspected the Processor's procedure for making secrecy and confidentiality agreements with personnel and consultants. We observed that the procedure requires that personnel, who have access to process personal data must sign a secrecy and confidentiality agreement in connection with their employment. We made a random inspection of a signed secrecy and confidentiality agreement and observed that the secrecy and confidentiality agreement has been signed. We made a random inspection of a signed NDA with consultants.	No deviations noted.

Article 28(3)(c) - Technical and Organisational Measures

Control objectives

- *To ensure that the Processor has implemented suitable technical and organisational measures with due regard to the current technical level, implementation costs and the nature of the relevant processing, scope, context and objective, and the risks of varying likelihood and severity for the rights and freedoms of natural persons (risk assessment), including a current examination and updating of risk assessment and security measures.*
- *To ensure that the risk assessment takes into account the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*
- *To ensure confidentiality, integrity and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of access to the personal data in the event of physical or technical incidents.*
- *To ensure regular testing, assessment and evaluation of the operating effectiveness of the technical and organisational measures to safeguard the security of processing.*

Control activity	Test performed by BDO	Result of test
Risk assessment ▶ The Processor has prepared a procedure for preparation of risk assessments, which include the rights and freedoms of natural persons. ▶ The Processor has prepared risk assessments for assets with personal data. ▶ The Processor has prepared and implemented a procedure, which ensures that the security measures are audited and updated.	We have interviewed relevant personnel at the Processor. We inspected procedure for preparation of risk assessments and observed that a process is described which has focus on systems where the Processor stores and/or processes personal data. We inspected risk assessments prepared by the Processor for processing of personal data. We observed that the risk assessments describe the risks identified and how assets with personal data must be protected. We inspected procedure for current assessment and updating of security measures and observed that the procedure describes that an annual update is to be made of the risk assessment. We observed that the annual update of the risk assessment is included in the Processor's annual cycle of work.	No deviations noted.
Contingency plan ▶ The Processor has prepared an IT contingency plan. ▶ The Processor has updated the IT contingency plan.	We have interviewed relevant personnel at the Processor. We inspected the IT contingency plan and observed that it includes a description of, for example, roles and responsibilities in the contingency organization, conditions for activation and plan for escalation. Moreover, we observed that the IT contingency plan was updated and approved by Management in March 2022.	No deviations noted.

Article 28(3)(c) - Technical and Organisational Measures

Control objectives

- *To ensure that the Processor has implemented suitable technical and organisational measures with due regard to the current technical level, implementation costs and the nature of the relevant processing, scope, context and objective, and the risks of varying likelihood and severity for the rights and freedoms of natural persons (risk assessment), including a current examination and updating of risk assessment and security measures.*
- *To ensure that the risk assessment takes into account the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*
- *To ensure confidentiality, integrity and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of access to the personal data in the event of physical or technical incidents.*
- *To ensure regular testing, assessment and evaluation of the operating effectiveness of the technical and organisational measures to safeguard the security of processing.*

Control activity	Test performed by BDO	Result of test
	We observed that the IT contingency plan must be updated annually in continuation of the annual testing. We inspected the completed test of the IT contingency plan.	
Physical security, including physical access control ▶ The Processor has performed a risk assessment of the physical security of office premises. ▶ The Processor has implemented physical access control to office premises.	We have interviewed relevant personnel at the Processor. We inspected the Processor's risk assessment of the physical security and observed that risks relating to the Processor's office premises have been described. We inspected the procedure for physical security and observed that security measures relating physical access control to office premises have been described. On inquiry, we were informed that the office premises are protected by doors with locks. We observed that the disclosed security measures have been implemented. We inspected documentation for handing out keys to the relevant premises and observed that the process is in accordance with the Processor's procedure.	No deviations noted.
Authorization and rights management ▶ The Processor has prepared a procedure for authorization and rights management.	We have interviewed relevant personnel at the Processor.	No deviations noted.

Article 28(3)(c) - Technical and Organisational Measures

Control objectives

- *To ensure that the Processor has implemented suitable technical and organisational measures with due regard to the current technical level, implementation costs and the nature of the relevant processing, scope, context and objective, and the risks of varying likelihood and severity for the rights and freedoms of natural persons (risk assessment), including a current examination and updating of risk assessment and security measures.*
- *To ensure that the risk assessment takes into account the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*
- *To ensure confidentiality, integrity and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of access to the personal data in the event of physical or technical incidents.*
- *To ensure regular testing, assessment and evaluation of the operating effectiveness of the technical and organisational measures to safeguard the security of processing.*

Control activity	Test performed by BDO	Result of test
▶ Authorizations and rights are allocated on the basis of a work-related need. ▶ The Processor performs an annual examination of the employees' rights and authorizations in the Processor's systems. ▶ Rights are allocated to employees, which give access to personal data, based on the employees' roles and level of authorization.	We inspected procedure for authorization and rights management and observed that guidelines have been described for authorization and rights management in relation to the Processor's systems and databases. We made a random inspection of a new employee and we observed that authorizations and rights have been allocated to the employee in the Processor's systems based on the employee's roles and areas of responsibility. We asked for documentation for examination of users and their rights. We were informed that the employees' access has been examined but that the documentation hereof is not retained. We inspected documentation confirming that the personnel have the rights that give access to personal data relating to the employees' roles and level of authorization, which is in accordance with the procedure.	
Remote access to systems and data ▶ The Processor has prepared a procedure for remote work. ▶ The Processor has implemented security measures to access systems and data via remote access. ▶ Work via remote access is by a VPN or SSL encrypted connection.	We have interviewed relevant personnel at the Processor. We inspected the Processor's procedure for remote work. We inspected documentation confirming that two-factor login is used. We inspected documentation confirming that remote connection is by a VPN or SSL encrypted connection.	No deviations noted.

Article 28(3)(c) - Technical and Organisational Measures

Control objectives

- *To ensure that the Processor has implemented suitable technical and organisational measures with due regard to the current technical level, implementation costs and the nature of the relevant processing, scope, context and objective, and the risks of varying likelihood and severity for the rights and freedoms of natural persons (risk assessment), including a current examination and updating of risk assessment and security measures.*
- *To ensure that the risk assessment takes into account the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*
- *To ensure confidentiality, integrity and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of access to the personal data in the event of physical or technical incidents.*
- *To ensure regular testing, assessment and evaluation of the operating effectiveness of the technical and organisational measures to safeguard the security of processing.*

Control activity	Test performed by BDO	Result of test
	We observed that the Processor uses TLS 1.2 encryption by use of a VPN connection. We observed that SSH keys are used and that they are 2048-bit AES encrypted.	
Logical access control - The Processor has prepared and implemented an access code policy. - The Processor has prepared and implemented a procedure for logical access control to areas with personal data. - The Processor has implemented security measures in relation to denied login attempts.	We have interviewed relevant personnel at the Processor. We inspected the Processor's access code policy and observed that requirements are described for strong access codes and the protection of those access codes. We inspected documentation confirming that strong access codes are used. We inspected the Processor's procedure for logical access controls and observed that guidelines have been specified for access controls, including access code policy and control of denied access attempts. We inspected documentation confirming that security measures have been implemented in relation to denied login attempts.	No deviations noted.
Encryption - The Processor has prepared and implemented a procedure for encryption and anonymisation of personal data.	We have interviewed relevant personnel at the Processor.	No deviations noted.

Article 28(3)(c) - Technical and Organisational Measures

Control objectives

- *To ensure that the Processor has implemented suitable technical and organisational measures with due regard to the current technical level, implementation costs and the nature of the relevant processing, scope, context and objective, and the risks of varying likelihood and severity for the rights and freedoms of natural persons (risk assessment), including a current examination and updating of risk assessment and security measures.*
- *To ensure that the risk assessment takes into account the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*
- *To ensure confidentiality, integrity and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of access to the personal data in the event of physical or technical incidents.*
- *To ensure regular testing, assessment and evaluation of the operating effectiveness of the technical and organisational measures to safeguard the security of processing.*

Control activity	Test performed by BDO	Result of test
▶ The Processor has implemented anonymisation of personal data in the Processor's GataawayAPI database.	We inspected the Processor's procedure for encryption of personal data and observed that TLS 1.2 or TLS 1.3 encryption is used. We inspected documentation confirming that hashing and salting of the access codes are carried out. We inspected documentation confirming that personal data are anonymized in the Processor's GatewayAPI database.	
Network security ▶ The Processor's network is segmented. ▶ The Processor uses known network technologies and mechanisms, such as Firewall. ▶ Only authorized personnel can make changes in the Processor's Firewall.	We have interviewed relevant personnel at the Processor. We inspected the Processor's procedure for network security and observed that the technical measures relating to network security are described, including network segmentation. We inspected documentation relating to network segmentation confirming that the network is segmented. We inspected documentation confirming that the network is protected by Firewall. We inspected documentation confirming that only the authorized personnel, who have access to make changes in the Processor's Firewall, have been allocated this right.	No deviations noted.

Article 28(3)(c) - Technical and Organisational Measures

Control objectives

- *To ensure that the Processor has implemented suitable technical and organisational measures with due regard to the current technical level, implementation costs and the nature of the relevant processing, scope, context and objective, and the risks of varying likelihood and severity for the rights and freedoms of natural persons (risk assessment), including a current examination and updating of risk assessment and security measures.*
- *To ensure that the risk assessment takes into account the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*
- *To ensure confidentiality, integrity and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of access to the personal data in the event of physical or technical incidents.*
- *To ensure regular testing, assessment and evaluation of the operating effectiveness of the technical and organisational measures to safeguard the security of processing.*

Control activity	Test performed by BDO	Result of test
External communication connections ▶ The Processor has prepared and implemented a procedure for use of external communication connections. ▶ A secure mail solution based on TLS 1.2 is used.	We have interviewed relevant personnel at the Processor. We inspected the Processor's procedure for external communication connections and observed that guidelines are described for transfer of information via e-mails. We inspected documentation confirming that TLS 1.2 encryption and a secure mail solution is used.	No deviations noted.
Antivirus ▶ The Processor has prepared and implemented a procedure for antivirus. ▶ The Processor ensures that antivirus is installed on the personnel's PCs.	We have interviewed relevant personnel at the Processor. We inspected the Processor's procedure for protection against virus and malware, etc. We inspected documentation relating to installation of antivirus on randomly selected PCs. We observed that antivirus is activated and updated. We found that the Processor receives weekly reports on identified vulnerabilities. We inspected documentation confirming that reports are received weekly from the service solution GitHub, including the Processor's follow-up hereon.	No deviations noted.
Backup ▶ The Processor has prepared and implemented a procedure for backup.	We have interviewed relevant personnel at the Processor.	No deviations noted.

Article 28(3)(c) - Technical and Organisational Measures

Control objectives

- *To ensure that the Processor has implemented suitable technical and organisational measures with due regard to the current technical level, implementation costs and the nature of the relevant processing, scope, context and objective, and the risks of varying likelihood and severity for the rights and freedoms of natural persons (risk assessment), including a current examination and updating of risk assessment and security measures.*
- *To ensure that the risk assessment takes into account the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*
- *To ensure confidentiality, integrity and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of access to the personal data in the event of physical or technical incidents.*
- *To ensure regular testing, assessment and evaluation of the operating effectiveness of the technical and organisational measures to safeguard the security of processing.*

Control activity	Test performed by BDO	Result of test
▶ The Processor ensures that backup is taken of the Processor's infrastructure. ▶ The Processor ensures that backup is taken of the personnel's PCs. ▶ The Processor has prepared and implemented a procedure for restore of data from backup.	We inspected the Processor's backup policy and procedure for backup, including verification and restore of backup. We inspected documentation relating to the Processor's back-up of systems and databases which confirms that backup is taken depending on whether it is Google or Hetzner as sub-processer. We inspected documentation relating to backup of the personnel's PCs which confirms that backup is taken. We inspected documentation relating to restore of backup which confirms that the Processor can restore data from backup.	
Patch management ▶ The Processor has prepared and implemented a procedure for patch management. ▶ The Processor ensures that work units are updated and patched. ▶ The Processor ensures that systems are updated and patched.	We have interviewed relevant personnel at the Processor. We inspected the Processor's procedure for patch management and observed that guidelines are described for updating of the Processor's systems and the personnel's units. We inspected randomly selected PCs for updates which confirms that updates are installed. We inspected documentation relating to set-up of updates of the Processor's systems which confirms that updates are installed.	No deviations noted.

Article 28(3)(c) - Technical and Organisational Measures

Control objectives

- *To ensure that the Processor has implemented suitable technical and organisational measures with due regard to the current technical level, implementation costs and the nature of the relevant processing, scope, context and objective, and the risks of varying likelihood and severity for the rights and freedoms of natural persons (risk assessment), including a current examination and updating of risk assessment and security measures.*
- *To ensure that the risk assessment takes into account the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*
- *To ensure confidentiality, integrity and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of access to the personal data in the event of physical or technical incidents.*
- *To ensure regular testing, assessment and evaluation of the operating effectiveness of the technical and organisational measures to safeguard the security of processing.*

Control activity	Test performed by BDO	Result of test
Logging and monitoring of use of personal data ▶ The Processor has prepared a procedure for logging and monitoring. ▶ Log data of customer activities are deleted after 30 days. ▶ Log files are solely accessible for operations and support staff. ▶ The activities of operations and support staff are logged.	We have interviewed relevant personnel at the Processor. We inspected the Processor's procedure for logging and monitoring and observed that guidelines are described for the Processor's security measures relating to logging and monitoring. We inspected documentation regarding how long log data of customer activities are retained. We inspected documentation confirming that only operations and support staff have access to log files. We inspected documentation confirming that the activities of operations and support staff are logged.	No deviations noted.
Repair, service, sale and discarding of IT equipment ▶ The Processor has prepared and implemented a procedure for sale and discarding of IT equipment. ▶ The Processor has prepared and implemented a procedure for repair and service of IT equipment.	We have interviewed relevant personnel at the Processor. We inspected the Processor's procedure for sale and discarding of IT equipment. We observed that this includes guidelines for discarding of IT equipment and that the Processor does not sell IT equipment. On inquiry, we were informed that discarded IT equipment is cleared of personal data before it is discarded. It has not been	No deviations noted.

Article 28(3)(c) - Technical and Organisational Measures

Control objectives

- *To ensure that the Processor has implemented suitable technical and organisational measures with due regard to the current technical level, implementation costs and the nature of the relevant processing, scope, context and objective, and the risks of varying likelihood and severity for the rights and freedoms of natural persons (risk assessment), including a current examination and updating of risk assessment and security measures.*
- *To ensure that the risk assessment takes into account the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*
- *To ensure confidentiality, integrity and accessibility and robustness of processing systems and services.*
- *To ensure timely restoration of the accessibility of access to the personal data in the event of physical or technical incidents.*
- *To ensure regular testing, assessment and evaluation of the operating effectiveness of the technical and organisational measures to safeguard the security of processing.*

Control activity	Test performed by BDO	Result of test
	possible to test that the procedure has been implemented because no IT equipment was discarded in the period subject to audit. We inspected the Processor's procedure for repair and service of IT equipment. We inspected documentation confirming that the Processor complies with the provisions in the procedure for repair and service of IT equipment.	

Article 25 – Data Protection by Design and by Default

Control objective

- *To ensure that the Processor implements data protection by design and by defaultAt sikre, at databehandleren gennemfører databeskyttelse gennem design og standardindstillinger.*

Control activity	Test performed by BDO	Result of test
Technical and organisational measures relating to development ▶ The Processor has prepared a procedure for the development process which ensures Privacy by Design and Privacy by Default. ▶ The Processor has instructed personnel on Privacy by Design and Privacy by Default. ▶ Developed functions, relating to personal data, are tested and only anonymized data are used as test data. ▶ The progress of development projects is documented currently in GitHub. ▶ Development, tests and production environments are separated. It is ensured that backup is taken. ▶ Version management is secured.	We have interviewed relevant personnel at the Processor. We inspected the Processor's procedure for data protection by design and by default. We inspected documentation confirming that the Processor has instructed personnel on the requirements for Privacy by Design and Privacy by Default. On inquiry, we were informed that the progress of the development projects is documented currently in GitHub. We inspected documentation of a randomly selected development project. We observed that the case is documented in GitHub. We inspected documentation confirming that only anonymized data are used as test data. We have inspected documentation confirming that development, test, and production environments are separated system environments. However, all software developers have access to deploy changes directly into production environment. Management have assessed the lack of segregation of duties in development team and accepted the risk due to the organizational size of the organization. We inspected documentation confirming that backup is taken. We inspected documentation confirming that version management is secured in relation to the development.	No deviations noted.

Article 28(3)(g) - Deletion and/or Return of Personal Data		
Control objective ▶ *To ensure that the Processor can delete and return personal data as instructed by the Controller after the end of the provision of services relating to the processing.*		
Control activity	**Test performed by BDO**	**Result of test**
Deletion and return of personal data ▶ The Processor has prepared and implemented a procedure for deletion and return of personal data.	We have interviewed relevant personnel at the Processor. We inspected procedure for deletion of personal data. We observed that the Processor has implemented technical measures which enable deletion or return of personal data. We observed that customers generally have access to data, but that the Processor has procedures to support the Controller should the need arise. We have inspected that data in SMS messages are deleted automatically after 30 days. On inquiry, we were informed that no requests were received during the period subject to audit from the Controller relating to deletion or return of personal data. Thus, we were unable to verify the efficiency of the procedure.	No deviations noted.

Article 28 (3)(e, f and h) – Assistance to Controller

Control objectives

- *To ensure that the Processor can assist the Controller fulfilling the data subjects' rights.*
- *To ensure that the Processor can assist the Controller in relation to audits and inspections.*
- *To ensure that the Processor can assist the Controller in relation to compliance with special obligations of GDPR, including assistance according to Articles 32 to 36.*

Control activity	Test performed by BDO	Result of test
Assistance – data subjects' rights ▶ The Processor has prepared and implemented a procedure for assistance to the Controller in connection with fulfilment of the data subject's rights.	We have interviewed relevant personnel at the Processor. We inspected procedure for assistance to the Controller in relation to fulfilment of the data subject's rights. We inspected the Processor's standard template for data processing agreements, which shows that the Processor is under an obligation to assist the Controllers in relation to requests for exercising of the data subjects' rights. We inspected several randomly selected incoming data processing agreements. We observed that those data processing agreements include an obligation to assist the Controllers. On inquiry, we were informed that no requests were received from Controller parties for assistance during the period subject to audit. Thus, we were unable to verify the efficiency of the procedures for handling of assistance in relation to fulfilment of the data subject's rights.	No deviations noted.
Assistance – audits and inspections ▶ The Processor has prepared and implemented a procedure for assistance to the Controller in connection with audits and/or inspections.	We have interviewed relevant personnel at the Processor. We inspected procedure for assistance to the Controller in connection with audits and inspections and observed that guidelines are described for the Processor's assistance to the Controller in connection with audits and inspections. On inquiry, we were informed that no requests were received from Controller parties received for assistance during the pe-	No deviations noted.

Article 28 (3)(e, f and h) – Assistance to Controller		
Control objectives ▶ *To ensure that the Processor can assist the Controller fulfilling the data subjects' rights.* ▶ *To ensure that the Processor can assist the Controller in relation to audits and inspections.* ▶ *To ensure that the Processor can assist the Controller in relation to compliance with special obligations of GDPR, including assistance according to Articles 32 to 36.*		
Control activity	**Test performed by BDO**	**Result of test**
	riod subject to audit. Thus, we were unable to verify the efficiency of the procedures for handling of assistance in relation to fulfilment of the data subject's rights.	
Assistance – special obligations of GDPR ▶ The Processor has procedures to handle assistance to the Controller in connection with fulfilment of security of processing (article 32), notification of breach of personal data security to the Controllers (article 33), impact assessment of the data protection (article 35), prior consulting (article 36).	We have interviewed relevant personnel at the Processor. We inspected the following procedures: • Procedure for assistance to Controller • Procedure for registration of breach of the personal data security • Procedure for instruction to personnel processing personal data • Procedure for processing of personal data in 2nd line support from the development department We inspected the Processors standard template for data processing agreements, which shows that the Processor is under an obligation to assist the Controllers with their obligations in relation to articles 32 to 36 GDPR. On inquiry, we were informed that no requests were received for assistance during the period subject to audit. Thus, we were unable to verify the efficiency of the procedure.	No deviations noted.

Article 30(2, 3 and 4) – Records of Processing Activities

- *Control objectives*
- *To ensure that the Processor maintains a written record of all categories of processing activities carried out on behalf of the Controller.*
- *To ensure that the Processor retains the record in writing, including in electronic form.*
- *To ensure that the Processor makes the record available to the supervisory authority.*

Control activity	Test performed by BDO	Result of test
Processing activities ▶ The Processor has prepared records of processing activities. ▶ The Processor has prepared and implemented a procedure for the Data Protection Agency's access to records of processing activities. ▶ The Processor has prepared and implemented a procedure for retention of the records.	We have interviewed relevant personnel at the Processor. We observed that the Processor has prepared records of processing activities. We inspected procedure for the Data Protection Agency's access to records of processing activities and observed that guidelines are described how the Processor gives the Agency access to the records of processing activities. On inquiry, we were informed that no requests were received for access to the records during the period subject to audit. Thus, we were unable to verify the efficiency of the procedure. We inspected procedure for retention of the records. We observed that the records are retained electronically.	No deviations noted.

Article 33(2) – Notification of Breach of Personal Data Security

Control objectives

- *To ensure that the Processor without undue delay notifies the Controller about personal data breaches.*
- *To ensure that the notification to the Controller consists of all required information, so the breach can be reviewed with the intention to notify the supervisory authority and to communicate the breach to the data subject.*

Control activity	Test performed by BDO	Result of test
Registration of breach of personal data security ▶ The Processor has prepared and implemented a procedure for personal data breach. ▶ The Processor has prepared and implemented a procedure for notification of the Controller of personal data breach. ▶ The Processor has prepared and implemented a standard template for registration of personal data breach.	We have interviewed relevant personnel at the Processor. We inspected procedure for breach of personal data security and observed that guidelines are described for registration of personal data breach. We inspected procedure for notification of the Controller of personal data breach and observed that guidelines are described for contact to the Controller without undue delay. We inspected a standard template for registration of personal data breach. On inquiry, we were informed that no personal data breaches occurred during the period subject to audit. Thus, we were unable to verify the efficiency of the procedure for personal data breach and the procedure for notification of the Controller of personal data breaches.	No deviations noted

Articles 44 to 49 – Transfers of Personal Data to Third Countries

Control objectives

- *To ensure that the Processor transfers personal data to a third country or an international organisation only when the conditions of articles 45 to 49 are complied with.*
- *To ensure that the Processor transfers personal data only according to instruction from the Controller and in accordance with a valid transfer basis (articles 45 to 49).*

Control activity	Test performed by BDO	Result of test
Transfers of personal data to third countries ▶ The provisions relating to transfers of personal data to third countries are covered by the Processor's data processing agreements. ▶ The Processor has ensured that transfers are made only to an approved third country, which has provided data protection in accordance with the EU regulation and the Danish data protection act.	We have interviewed relevant personnel at the Processor. We inspected the Processor's template for data processing agreements and observed that it includes provisions relating to transfers of personal data to third countries. We observed that transfers can be made only where this is stated in instruction from the Controller. We observed that personal data regarding GatewayAPI is stored within EU at Google LLC and Hetzner GmbH respectively. However, OnlineCity is aware of the risk that if Google Support is used there will be an increased chance that data are transferred to/accessed by persons from unsecure third countries, and rules have therefore been set up that Google Support must not be used.	For customers using GatwayAPI.com In The Heart of has stated that there is no transfer of personal data to third countries. Furthermore, the company have configured build-in security measures in Google Cloud Web Hosting to protect personal data when using Google as a sub-data processor. However, there is a risk of unintentional transfer to third countries, as Google as a US-owned company is subject to US law. At present, there is no specific practice in this area which determines whether a potential accidental transfer to a third country is unproblematic. This issue is not relevant for customers using GatewayAPI.eu. No other deviations noted.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

HAVNEHOLMEN 29
1561 COPENHAGEN

CVR NO. 20 22 26 70

PENNEO

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

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

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: CVR:20222670-RID:1283706411033
IP: 77.243.xxx.xxx
2022-06-08 07:16:06 UTC
NEM ID

Mikkel Jon Larssen
Partner
Serienummer: CVR:20222670-RID:52744874
IP: 77.243.xxx.xxx
2022-06-08 11:36:08 UTC
NEM ID

Birol Altinok
Executive, Partner
Serienummer: PID:9208-2002-2-832355101479
IP: 77.241.xxx.xxx
2022-06-08 13:11:43 UTC
NEM ID

Penneo dokumentnøgle: PEWS4-0NSS8-L6EC8-PETYK-E5750-S8T1E