EG SAFETYNET

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE TYPE-II REPORT FOR THE PERIOD FROM 1ST MARCH 2021 TO 28TH FEBRUARY 2022 ON THE DESCRIPTION OF EG SAFETYNET AND THE RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS, RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

CONTENTS

This document is an unofficial translation of the original Danish text, and in case of any discrepancy between the Danish text and the English translation, the Danish text shall prevail.

INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD FROM 1ST MARCH 2021 TO 28TH FEBRUARY 2022 ON THE DESCRIPTION OF EG SAFETYNET AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS, RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

To: The Management of EG SafetyNet - EG A/S
EG SafetyNet - EG A/S' Customers (Data Controllers)

Scope

We were engaged to report on EG SafetyNet - EG A/S' (Data Processor) description in section 3 of EG SafetyNet and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the Regulation of the European Parliament and of the Council on protection of natural persons with regard to processing of personal data and on the free movement of such data (EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions to the Regulation (Danish Data Protection Act), and on the design and operating effectiveness of the technical and organisational measures and other controls relating to the control objectives stated in the description, throughout the period from 1st March 2021 to 28th February 2022.

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, 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 is 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 according to 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 Engagements 3000, "Assurance 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 developed to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the use of EG SafetyNet, that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the 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 presents fairly EG SafetyNet and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act, as designed and implemented, throughout the period from 1st March 2021 to 28th February 2022; and

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 1st March 2021 to 28th February 2022; and

c. The technical and organisational measures and other controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1st March 2021 to 28th February 2022.

Highlighting of matters relating to the transfer of personal data to third countries, cf. Chapter V of the Data Protection Regulation

We emphasize that the data processor's used legal basis for valid transfer of personal data to the United States in the form of Privacy Shield after the declaration period is known to be invalid, cf. the judgment of the European Court of Justice in case C-311/18 (Schrems II case). Our conclusion is not modified as a result of this relationship.

Description of Test of Controls

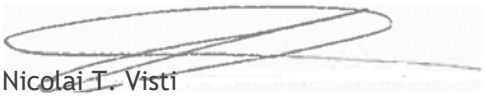
The specific controls tested and the results of those tests are listed in section 4.

Intended Users and Purpose

This report is intended solely for data controllers who have used the Data Processor's EG SafetyNet, 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 in assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Copenhagen, 20th May 2022

BDO Statsautoriseret revisionsaktieselskab



Nicolai T. Visti
Partner, State Authorised Public Accountant

Mikkel Jon Larssen
Partner, Head of Risk Assurance

EG SAFETYNET - EG A/S' STATEMENT

EG SafetyNet - EG A/S processes personal data in relation to EG SafetyNet to our Customers, who are Data 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 Data Controllers who have used EG SafetyNet, 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 data controllers themselves in assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

EG SafetyNet - EG A/S 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.

EG SafetyNet - EG A/S confirms that the accompanying description in section 3 fairly presents EG SafetyNet and the related technical and organisational measures and other controls throughout the period from 1st March 2021 to 28th February 2022. The criteria used in making this statement were that the accompanying description:

1. Presents how EG SafetyNet, 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 data controller;
    - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality;
    - The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation;
    - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects;
    - The procedures ensuring appropriate technical and organisational 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 EG SafetyNet, have assumed would be designed and implemented by the data controllers and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description;
    - 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 in EG SafetyNet and the related technical and organisational measures and other controls throughout the period from 1st March 2021 to 28th February 2022.

3. Does not omit or distort information relevant to the scope of EG SafetyNet 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 data controllers and may not, therefore, include every aspect of EG SafetyNet that the individual data controllers might consider important in their particular circumstances.

EG SafetyNet - EG A/S 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 1st March 2021 to 28th February 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 that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1st March 2021 to 28th February 2022.

EG SafetyNet - EG A/S confirms that appropriate technical and organisational measures and other controls were implemented and maintained to comply with the agreements with data 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.

Copenhagen, 16th May 2022

EG SafetyNet - EG A/S

Brian Poulsgaard
CEO

EG SAFETYNET - EG A/S' DESCRIPTION OF EG SAFETYNET

INTRODUCTION

The purpose of this company description is to provide information and insight to EG SafetyNet - EG A/S' customers and their auditors in relation to the IT general controls relating to security, data protection and protection of personal data used in EG SafetyNet - EG A/S.

SIGNIFICANT CHANGES IN THE PERIOD.

During the period, FrontAvenue A/S was merged with EG A/S. EG SafetyNet - EG A/S operates under EG A/S and is subject to Information Security policies and procedures prepared by EG A/S. In connection with the transition, a risk assessment has been made of the changes in information security policies and organization that have been made. It is EG SafetyNet - EG A/S' assessment that the effectiveness of the safety measures is unchanged, which is also compared with the fact that EG SafetyNet Hosting is unchanged during the period.

GENERAL DESCRIPTION OF EG SAFETYNET

EG SafetyNet - EG A/S employs about 15 people in Denmark (Copenhagen) and about 20 people in our subsidiary in India (Bangalore and Mangalore), all having focus on the Cloud/SaaS (software-as-a-service) solution called EG SafetyNet. The Danish office is responsible for marketing, sale, education, support, delivery management, development, testing, installation and operation of the customers' EG SafetyNet solutions whereas our Indian employees are focused on development and quality assurance/testing on the basis of specifications prepared by the Danish office.

Types of personal data covered by the processing include general personal data, sensitive personal data and information on CPR numbers.

EG SafetyNet - EG A/S is for more than 10 years a Microsoft Gold Partner, and EG SafetyNet is developed using Microsoft tools and is running under Microsoft SPLA licenses on MS Windows servers as Web server platform, and with MS SQL Server as the database platform. A "hybrid" EG SafetyNet APP has been developed which is running on Android and IOS, and which is used to ensure simple recordings with for example picture documentation.

EG SafetyNet is hosted at Sentia Denmark and Microsoft Azure, which both make professional and certified data centers available. Production data and backup hereof exist only in our hosting center.

EG SafetyNet - EG A/S deletes data as instructed by the customer who is the data controller. This is most often done in an automated routine which has been set up in accordance with the customer's wishes and needs. It is the customer's responsibility to ensure that data are deleted in accordance with applicable legislation. EG SafetyNet - EG A/S provides the tools to fulfill the obligations that data controllers maintain.

BUSINESS STRATEGY/IT SECURITY STRATEGY

It is EG SafetyNet - EG A/S' strategy that the business should contain the required security, so that unacceptable risks are not imposed on either EG SafetyNet customers or the business itself.

The objective of EG SafetyNet - EG A/S' IT security strategy is to ensure that:

- The conditions for a secure EG SafetyNet operating environment exist.

- EG SafetyNet platforms and data are protected from external incidents.
- EG SafetyNet platforms and data can be restored with predictability and according to known routines.
- EG SafetyNet customer's data can only be accessed by EG SafetyNet - EG A/S personnel in connection with performance of the required support or delivery tasks.
- That solely authorized persons have access to the EG SafetyNet operating environments, systems and data.
- That all personnel at EG SafetyNet - EG A/S are aware of their duty of non-disclosure and EG SafetyNet - EG A/S´ information security policy.

EG SafetyNet - EG A/S is working with IT security at a business strategic level. Thus, they currently aim to ensure a high level of service, accessibility, support and quality. Management prioritises, through its security policy that IT security should be, and is, an important element of the company's business culture.

The information security policies are reviewed at least annually in connection with the risk assessment.

EG SafetyNet - EG A/S has chosen to base its IT security strategy on ISO27001:2013 and has thus used the ISO methodology to implement the relevant security measures in the following areas:

- A.2 Risk management
- A.5 Information security policies
- A.6 Organisation of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access management
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security
- A.13 Communication security
- A.14 Acquisition, development and maintenance of systems
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security continuity
- A.18 Compliance with legislative and contractual requirements

A.2 RISK ASSESSMENT

EG SafetyNet - EG A/S carries out annually a risk assessment, which includes the IT installations and the use of them. This is based on the existing threat scenario and the risk assessment is part of the documentation for annual IT audit. Based on the auditors' recommendations this may form basis for new projects to strengthen the security of all EG SafetyNet - EG A/S IT platforms.

A.5 INFORMATION SECURITY POLICIES

EG SafetyNet - EG A/S has prepared an information security policy which is audited once a year or if there are incidents or changes that have an impact on the policy.

The information security policy applies to EG SafetyNet - EG A/S' employees, partners and external consultants and is signed by all parties when the employment starts, and it is reviewed at least once a year or

in connection changes to it. The information security policy applies to any work with data and IT equipment within hosting and in-house at EG SafetyNet - EG A/S.

A.6 ORGANISATION OF INFORMATION SECURITY

It is EG SafetyNet - EG A/S' partners (senior management) who are responsible for the information security and all employees are informed of and acknowledge by their signature the employee information policy. A risk-based approach is used which is combined with a role-based and functionally separated access to the systems. A system owner is designated for each system and the owner is responsible for granting user rights, risk assessment, and the day-to-day operations.

Mobile equipment is safeguarded by registration before it is handed over, and workstations are installed with Bitlocker including boot password, antivirus software, and are updated automatically with Microsoft Windows update. Remote access is possible only through encrypted two-factor VPN connections to both internal systems and hosting systems.

A.7 HUMAN RESOURCE SECURITY

EG SafetyNet - EG A/S has designed procedures to manage all phases of an employment.

Before employment
At employment, candidates are screened in connection with the recruitment process. Documentary proof of the employee's identity is obtained. As regards positions of trust, a criminal record may be obtained for the candidates. All candidates are assessed with respect to their qualifications and relevant references are obtained.

At employment, the employee must sign a non-disclosure agreement in which the legal responsibilities and sanctions are described. The employees acknowledge receipt of the information security policy and confirms to have read the policy by their signature.

The employee is informed of the information security and other conditions relevant to the position for which the person is employed.

Commencement and during employment
Employees attend an individual induction course when the employment starts and is trained in security measures relating to processing of personal data.
The information security policy in force at any time is available to the employees. Employees are informed of current threats as required. An appraisal interview is made annually during which the individual needs for training are identified and planned.

Resignation (end or change of employment)
When employees resign from their position at EG SafetyNet - EG A/S all their IT accounts including VPN access are closed and keys and other equipment received are returned.
In addition, it is emphasized that their duty of non-disclosure applies also after resignation.

A.8 ASSET MANAGEMENT

All mission-critical assets are registered in a centralized record and workstations handed over must be used solely for work-related purposes. Workstations and other mobile equipment are secured by Bitlocker and screenlock and remote access to the company's network and systems is possible only through an encrypted two-factor VPN connection.

Procedures have been laid down for secure hand-over and return of equipment and all data-bearing media must be Bitlocked and will, in connection with destruction, either be deleted/formatted with an acknowledged deletion software or physically destroyed.
EG SafetyNet - EG A/S uses the following systems:

- AD domain controls
- File and print server
- Development & Test environments
- CRM
- Change management system
- Website
- Mail
- Support system
- IP telephony
- Mobile telephony

A.9 ACCESS MANAGEMENT

EG SafetyNet - EG A/S has prepared a policy for access management which is audited annually.

Rules are defined for passwords and rules for change hereof, and passwords to servers are encrypted and password protected.

Access to all systems require a valid user-id and privileged access rights are granted on the basis of a work-related need, which is ensured by granting of the required user roles/user rights. Remote access is allowed solely through an encrypted two-factor VPN connection whereas guests are not allowed access to EG SafetyNet - EG A/S' network. Only employees in Denmark have access to personal data.

In connection with resignation or if abuse is suspected, user-id and rights will be closed down.

A.10 CRYPTOGRAPHY

EG SafetyNet - EG A/S uses Bitlocker on all workstations and data-bearing USB keys, and communication connections to the company, customers and business partners are encrypted VPN or SSL (HTTPS) encrypted.

A.11 PHYSICAL AND ENVIRONMENTAL SECURITY

EG SafetyNet - EG A/S has defined a policy for physical and environmental security which is audited annually. There is a sharp distinction between the customers' production data, which are solely in EG SafetyNet - EG A/S' hosting environments at Sentia or Microsoft Azure, whereas development, test and training environments contain only anonymized data.

All data-bearing media from production environments must be destroyed or deleted/formatted immediately if removed from the hosting center.

All employees are, as part of the information security policy and their duty of non-disclosure, responsible for ensuring that confidential documents are safeguarded, and that they are shredded after ended processing.

A.12 OPERATIONS SECURITY

EG SafetyNet - EG A/S has, in addition to a policy for operations security, laid down and described a number of procedures for backup and restore in case of crashes, where the operating environments are sharply separated from the development, test and training environments.

All incidents are registered in our incident system and categorized as: Incident, weakness, risk or security breach. All employees at EG SafetyNet - EG A/S are acquainted with procedure reporting of different types of incidents and weaknesses, which may have an impact on the IT and operations security. Security incidents and weaknesses must be reported to the Management as soon as possible.

EG SafetyNet - EG A/S uses only virtualized servers in the hosting, which ensures a uniform backup and restore procedure. Combined with an extra physical server operating as ”hot standby”, restore can be made using the least possible time.

All customer environments are checked by Site24x7, which in case of non-accessibility sends a mail to IT Admin (IT responsible and partner and infrastructure manager), so that quick check and action can be made in case of issues.

All backup jobs send mails regarding ”success” or ”failure”, and the readability of the backup media and ability to be used for restore is tested by monthly controls.

A.13 COMMUNICATION SECURITY

EG SafetyNet - EG A/S has prepared a policy for transfer of information, which is audited annually according to the year wheel.
All employees are subject to and have signed both the non-disclosure and the information security policy and only employees with a work-related need have access to the network unit configurations.
EG SafetyNet - EG A/S’ hosting and in-house network is divided into a DMZ and a LAN zone, which are firewall protected, and all communication is encrypted by either https, ftps, sftp, tls or two-factor VPN connection.

Sub-processing agreements and non-disclosure agreements have been made with suppliers who have access to personal data in the hosting environment.

Import of customer basic data (department hierarchy and employees):
- Transferred by encrypted traffic either via an HTTPS Web service call or via FTPS/SFTP transferred csv/xml files.
- Imported basic data files are deleted after end of use.

A.14 ACQUISITION, DEVELOPMENT AND MAINTENANCE OF SYSTEMS

EG SafetyNet - EG A/S has prepared a policy for acquisitions, development and maintenance of systems which ensure a risk-based approach to the security requirements made for changes, such as new acquisitions, change of suppliers, development and test of changes within both security, personal data, system set-up and operating effectiveness. For all changes, “privacy by design” and ”privacy by default” will be taken into account.

Descriptions of procedures have been prepared to deal with the above and all data in development and test environments are masked.

A.15 SUPPLIER RELATIONSHIPS

When carrying out our service it may be necessary to make use of external assistance. We will always ensure that agreements with external suppliers and out-source-suppliers are formalized, where relevant, and that suppliers and business partners are acquainted with our IT security policy and have signed a non-disclosure agreement and data processing agreements.

As regards supplier services that are critical to our operations we obtain and review the annual ISAE 3000, ISAE 3402 or SOC-2 auditor’s reports to ensure there is consistency with EG SafetyNet - EG A/S’ information security policy and sub-processing agreements made. Supplier deviations are registered as an incident and type, and they form at least annually basis for an assessment and possible follow-up with the supplier.

A.16 INFORMATION SECURITY INCIDENT MANAGEMENT

EG SafetyNet - EG A/S has prepared a policy and laid down a procedure for reporting and management of information security incidents, including reporting to data controllers. Incidents are registered in our incident registration system and all incidents are assessed in relation of type and confidentiality, integrity and accessibility.

A.17 INFORMATION SECURITY CONTINUITY

An IT emergency response plan has been prepared for information security breaches or other incidents having an impact on critical information systems. The emergency response plan covers both communication with involved parties and detailed emergency response plans containing procedures for error tracing and procedures for a potential ”restore/recovery” of the impacted information systems.

A.18 COMPLIANCE WITH LEGISLATIVE AND CONTRACTUAL REQUIREMENTS

A policy has been prepared for compliance with legislative and contractual requirements and it is ensured that data processing agreements are made with all customers. As part of this, an ISAE 3000 report is prepared annually which gives insight into the IT controls carried out relating to security, data protection and protection of personal data.
Personal data are retained in Denmark and are not transferred to third countries or organizations that are not covered by EU-US Privacy Shield.

In addition, there are procedures relating to personal data/GDPR:

- Assessment of instructions, notification of illegal instructions and compliance with instructions for processing personal data.
- Notification to the data controller of breach.

- Procedure for assistance to the data controller in relation to audit and inspection, including to make available required information.
- Procedures supporting the data controller's obligations in relation to the data subject.

DESCRIPTION OF CONTROLS WHICH ARE THE RESPONSIBILITY OF THE DATA CONTROLLER

In relation to personal data, EG SafetyNet - EG A/S is always operating according to instruction from the customer, who is data controller, when processing the customer's data. It is the responsibility of the customer that the processing is lawful, but EG SafetyNet - EG A/S reserves the right to refrain from carrying out an instruction which is assessed to be contrary to applicable legislation. In that case, the customer is informed without delay.

The data controller is responsible for:

- Ensuring limited access to personal data for its own employees.
- Ensuring rectification of registered personal data.
- Ensuring return of registered data to the data subject.
- Ensuring legal basis for the registrations made by the data controller.

CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND RESULT OF TESTS

Objective and scope

BDO conducted the 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 EG SafetyNet - EG A/S' description of EG SafetyNet 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 technical and organisational measures and other controls has included the control objectives and related control activities selected by EG SafetyNet - EG A/S, and which are described in the test 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 1st March 2021 to 28th February 2022.

Test procedures

Test of the design of the technical and organisational measures and other controls and their implementation and operating effectiveness 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.

For the services provided by Sentia Denmark within Hosting and IT operation we have received an Independent auditor's ISAE 3000 and ISAE 3402 assurance report on internal controls regarding data protection and processing of personal data for the period from 1st January 2021 to 31st December 2021.

For the services provided by Microsoft Azure within Hosting and IT operation we have received Azure (Public & Government) SOC 2 Type II Report for the period from 1st October 2020 to 30th September 2021.

Those sub-processors' relevant control objectives and related controls are not included in EG SafetyNet - EG A/S' description of EG SafetyNet and the relating technical and organisational security measures and other controls. Accordingly, we have solely inspected the documentation received and tested the controls at EG SafetyNet - EG A/S which ensure performance of proper supervision of the sub-processor's compliance with the data processing agreement made by and between the sub-processor and processor and compliance with the EU 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 describes whether the test has resulted in exceptions noted.

An exception exists when:

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

A.2 – Risk assessment

Control objective

- *To provide guidelines for and support the information security in accordance with business requirements and relevant laws and regulations. GDPR Art. 28 (1), Art. 28 (3) (c)*

Control activity	Test performed by BDO	Result of test
Control - Risk assessment ▶ A risk assessment is made of EG SafetyNet - EG A/S' information systems and assets for confidentiality, integrity and accessibility for the data subject. ▶ The risk assessment is reviewed at least once a year. ▶ The company's risk log of information assets is updated in relation to the findings from the risk analysis.	We interviewed relevant personnel and inspected material received. We have received and inspected the policy for the risk assessment. We observed that a procedure has been designed for assessment of risks relating to changes to legislation, registered incidents or the threat scenario. We observed that a risk assessment is made of the data subject's rights. We received and inspected the most recent risk assessment. We observed that the risk assessment is updated. We observed that changes were implemented in the period as a follow-up on risks identified. We observed that the risk assessment was reviewed and audited in the period 14th December 2021 to 3rd march 2022.	No exceptions noted.

A.5 - Information security policies

Control objective

- *To provide guidelines for and supporting information security in accordance with business requirements and relevant laws and regulations. GDPR Art. 28 (1), Art. 28 (3) (c)*

Control activity	Test performed by BDO	Result of test
Control - Information security policies ▶ A policy for information security policies is laid down and documented. ▶ Policies for information security are as a minimum subject to internal audit once a year or when there are material changes at EG SafetyNet - EG A/S.	We interviewed relevant personnel and inspected material received. We received and inspected the information security policy. We observed that a policy has been laid down for information security, and that data protection is included in the information security policy. We inspected the year wheel system. We observed that recurring controls are planned in the system. We observed that the policies were reviewed and audited in the period.	No exceptions noted.

A.6 - Organisation of information security

Control objectives

- *To establish a management basis for initiating and managing the implementation and operation of information security in the organisation. GDPR Art. 37 (1).*
- *To safeguard remote workplaces and the use of mobile equipment. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
Policy for organisation of information security ▶ A policy for organisation of information security is laid down and documented. ▶ The policy for organisation of information security is reassessed annually.	We interviewed relevant personnel and inspected material received. We received and inspected policies for organisation of the information security. We observed that policies for organisation, responsibilities and roles for information security are laid down. We also inspected the data processor's year wheel and observed that review and assessment of policies for organisation of information security is planned. We observed that policies were reviewed and audited in the period.	No exceptions noted.
Roles and responsibilities for information security ▶ All assets and information security processes are identified, defined and a responsible person with the required competence has been designated. ▶ Responsibility, authorisations and frame for information security controls are defined and documented for each process or asset. ▶ Information security in relation to suppliers for the specific process or asset is coordinated and ensured by the system owner. ▶ EG SafetyNet - EG A/S' Management ensures sufficient segregation of duties as regards functions critical to operations. If this is not possible compensating controls are carried out. ▶ EG SafetyNet - EG A/S' Management is responsible for the contact to relevant authorities and interest groups.	We interviewed relevant personnel and inspected material received. We received and inspected record of information assets. We observed that system owners are designated for all systems. We inspected the policy for organisation of information security. We observed that tasks and responsibilities are specified for system owners. We observed that supplier statements are reviewed and assessed. We observed that the system owner is responsible for controls for supplier security. We observed that the annual review of organisation and segregation of duties is planned in the data processor's year wheel. We inspected controls for segregation of duties. We observed that granted rights were reviewed in connection with the system owner control.	No exceptions noted.

A.6 - Organisation of information security

Control objectives

- *To establish a management basis for initiating and managing the implementation and operation of information security in the organisation. GDPR Art. 37 (1).*
- *To safeguard remote workplaces and the use of mobile equipment. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
	We inspected and assessed the compensating controls for failing segregation of duties. We observed that compensating controls are implemented in the form of logging and alerts. We observed that policies are laid down for contact to authorities. We observed that the data processor's Management is responsible for the contact. The Management's understanding for the control was confirmed by inquiries of the data processor's Management.	
Project management information security - All projects are assessed for risk in relation to information security and personal data. - As regards material changes to projects a new information security assessment must be made. - Systems are designed and implemented to ensure data protection by means of default settings and by design of processes and operating effectiveness.	We interviewed relevant personnel, made observations and inspected selected material. We were informed that no major projects were completed in the period. We inspected creation of customers in EG SafetyNet for a sample. We observed that creation of customers was standard creation. We inspected changes made for a sample. We observed that for changes involving personal data additional protection was considered, including encryption of data. We observed that personal data in test environment are protected by default settings.	No exceptions noted.
Policy for mobile equipment - Mobile equipment is registered when supplied to the user. - Employees are only authorised to install approved, work-related software on workstations. - Workstations are updated automatically from Microsoft update. - Workstations are encrypted with BitLocker.	We interviewed relevant personnel, made observations and inspected selected material. We inspected record of assets. We observed that supplied assets are registered when supplied. We inspected policies for management of assets and procedure for installation of workstations. We observed that a list of software approved for installation has been prepared. We inspected	No exceptions noted.

A.6 - Organisation of information security

Control objectives

- *To establish a management basis for initiating and managing the implementation and operation of information security in the organisation. GDPR Art. 37 (1).*
- *To safeguard remote workplaces and the use of mobile equipment. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
▶ Mobile units, telephones and tablets are protected by screen lock (pin code, fingerprint or the like). ▶ Active and updated antivirus software is installed on workstations.	workstations for a sample. We observed that employees do not have access to install software. We observed upstart of a randomly selected workstation. We observed for a sample that hard disks in workstations are encrypted. We inspected system for antivirus and inspected workstations for a sample. We observed that antivirus software is installed and updated. We observed also that users do not have access to deactivation of antivirus software.	
Remote workplaces ▶ Encrypted VPN is used when working from remote workplaces. ▶ Documents and units must be protected against theft, loss and malicious damage. ▶ Employees are informed of information security when working on remote workplace.	We interviewed relevant personnel, made observations and inspected selected material. We inspected system for remote access. We observed that VPN is configured with two-factor authentication. We inspected the information security policy and observed that guidelines have been described for working with and storing of units and documents. The employee's understanding for information security in connection with work at home was confirmed by inquiries of relevant personnel.	No exceptions noted.

A.7 - Human resource security

Control objectives

- *To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles for which they are intended. GDPR Art. 28 (1), Art. 28 (3) (b), and Art. 37 (1)*
- *To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR Art. 28 (1), Art. 28 (3) (c).*
- *To protect the organisation's interests as part of change or termination of the employment. GDPR Art. 28 (3) (b).*

Control activity	Test performed by BDO	Result of test
Policy for human resource security ▶ A policy for human resource security has been laid down and documented. ▶ The policy for human resource security is audited annually.	We interviewed relevant personnel and inspected material received. We have received and inspected the human resource policy. We observed that a policy has been prepared for human resource security. We observed also that policies must be reviewed annually or in connections with material changes and audited, if required. We inspected system for year wheel. We observed that recurring controls are planned in the system and there is a follow-up overview in which action plans can be created based on the specific control item. We observed that policies for human resource security were reviewed and assessed in connection with review and assessment of the information security in the period.	No exceptions noted.
Before employment ▶ All candidates are before employment screened and assessed in relation to references, confirmation of education and professional qualifications, proof of identity and in special cases, criminal records. ▶ All employees sing a non-disclosure agreement at employment which states the employee's legal responsibilities and sanctions in case of breach of confidentiality. ▶ The employees are informed of the information security and other conditions applying to the position for which the person is employed.	We interviewed relevant personnel, made observations and inspected selected material. We received and inspected the policy for human resource security. We observed that a procedure has been designed for screening of employees in connection with the employment process. We observed also that an annual review of the policy is planned in the plan for recurring controls. We have observed that no employment has been made during the period, which is why there is no incident for use in testing the control. We have inspected policies and procedures as well as made inquiries with relevant staff. We have confirmed the employees' understanding of the control.	No exceptions noted.

A.7 - Human resource security

Control objectives

- *To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles for which they are intended. GDPR Art. 28 (1), Art. 28 (3) (b), and Art. 37 (1)*
- *To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR Art. 28 (1), Art. 28 (3) (c).*
- *To protect the organisation's interests as part of change or termination of the employment. GDPR Art. 28 (3) (b).*

Control activity	Test performed by BDO	Result of test
	We received and inspected template for non-disclosure agreement for employees. We observed that the employees' legal responsibilities and sanctions are described herein. We observed also that the employees are informed that the duty of non-disclosure applies after end of the employment. By interview of a randomly selected employees, it was confirmed that the non-disclosure agreement was received at employment and that it was signed after it had been read. It was also confirmed that information was given of the information security at the employment.	
During employment ▶ Employees attend an individual induction course for new employees. The employee receives training in security measures relating to processing of sensitive and confidential data. ▶ The information security policy is available to all employees. ▶ At the start of the employment and minimum once a year in connection with the quarterly meeting, information will be given on the policy. ▶ If required, employees will be informed by mail of relevant threats. ▶ An appraisal interview is held annually where individual needs for training are identified and planned.	We interviewed relevant personnel, made observations and inspected selected material. We inspected plan for receiving employees. We observed that an induction course is planned for the employee. On inquiry of relevant personnel, it was confirmed that the employee has attended an induction course for new employees. It was also confirmed that the information security policies were reviewed. We inspected the intranet. We observed that information security policies are available to employees. We have inspected the Control manager. We have observed that in connection with the hiring / transfer of employees to EG and continuously during the period, campaigns and quizzes have been issued in information security. By inquiry of relevant personnel, it was confirmed that appraisal interviews will be held in 2022 at which the need for training was discussed.	No exceptions noted.

A.7 - Human resource security

Control objectives

- *To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles for which they are intended. GDPR Art. 28 (1), Art. 28 (3) (b), and Art. 37 (1)*
- *To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR Art. 28 (1), Art. 28 (3) (c).*
- *To protect the organisation's interests as part of change or termination of the employment. GDPR Art. 28 (3) (b).*

Control activity	Test performed by BDO	Result of test
End or change of employment ▶ All employees are at their employment informed of responsibilities, demands and sanctions which apply after the end of the employment.	We interviewed relevant personnel and inspected selected material. We inspected non-disclosure agreement and observed that the employee is informed that it applies after end of employment.	No exceptions noted.

A.8 - Asset management

Control objectives

- *To identify the organisation's assets and define appropriate responsibilities for its protection. GDPR Art. 30 (2) and (3), Art. 32 (2).*
- *To ensure adequate protection of information that is in relation to the importance of the information for the organisation. GDPR Art. 30 (3) and Art. 30 (4).*
- *To prevent unauthorised disclosure, modification, removal or destruction of information stored on media. GDPR Art. 28 (3) (c).*
- *To keep written, electronic records of all categories of processing activities.*

Control activity	Test performed by BDO	Result of test
Record of assets ▶ The Management has prepared, approved and communicated the policy for use and management of units and media. ▶ Business critical assets are identified and documented in a record which is maintained currently. ▶ A system owner is designated for all systems who is responsible for day-to-day operations and maintenance. ▶ Data in customer-focused operating systems are classified and treated as confidential data.	We interviewed relevant personnel and inspected material received. We received and inspected policy for management of assets. We observed that policies and guidelines are designed for use, accepted use, classification and management of media and information assets. We inspected the information security policy and interviewed relevant personnel and the employees understanding for use and management of information assets was confirmed. We received and inspected record of assets. We observed that a system owner is designated for information assets. We observed also that data are classified.	No exceptions noted.
Management of units and physical media ▶ All units and media are protected by encryption. ▶ Units delivered to employees or third parties are registered at delivery and at return. ▶ At delivery it is ensured that the units do not contain any confidential or sensitive data. ▶ Employees using units or media outside the organisation are responsible for safeguarding these against theft, loss or malicious damage.	We interviewed relevant personnel, made observations and inspected material received. For a sample, we inspected workstations. We observed that the workstation is encrypted with BitLocker. We received and inspected record of assets. We observed that the assets delivered are registered for the employee who can use the asset. We inspected procedures for delivery of units. We observed that workstations or other assets are deleted and that a new image is made before delivery. There were no incidents to be used for test of the control for reuse of units, and therefore we cannot comment hereon.	No exceptions noted.

A.8 - Asset management

Control objectives

- *To identify the organisation's assets and define appropriate responsibilities for its protection. GDPR Art. 30 (2) and (3), Art. 32 (2).*
- *To ensure adequate protection of information that is in relation to the importance of the information for the organisation. GDPR Art. 30 (3) and Art. 30 (4).*
- *To prevent unauthorised disclosure, modification, removal or destruction of information stored on media. GDPR Art. 28 (3) (c).*
- *To keep written, electronic records of all categories of processing activities.*

Control activity	Test performed by BDO	Result of test
	We interviewed a randomly selected employee and the employee's understanding for management of units outside the organisation was confirmed.	
Management of media - USB media or other portable media with confidential or sensitive personal data are encrypted. - Disks and media are destroyed when taken out of operation. - Disks and media are deleted and formatted before they are used again.	We interviewed relevant personnel and inspected material received. We received and inspected information to employees on use and encryption of USB media. At the date of this report, there were no incidents to be used for test of implementation of the control for deletion, formatting or destruction of media, and therefore we cannot comment hereon. We inspected procedures and policies. By inquiry of relevant personnel, the employees understanding for the control was confirmed.	No exceptions noted.

A.9 - Access management

Control objectives

- *To restrict access to information and information processing facilities. GDPR Art. 28 (3) (c).*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR Art. 28 (3) (c).*
- *To make users responsible for securing their authentication information. GDPR Art. 28 (3) (c).*
- *To prevent unauthorised access to systems and applications. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
Policy for access management - A policy for access management to systems and data is laid down and documented. - The policy for access management is audited annually.	We interviewed relevant personnel and inspected material received. We received and inspected policies for access management. We observed that policies and procedures for access management	No exceptions noted.

A.9 - Access management

Control objectives

- *To restrict access to information and information processing facilities. GDPR Art. 28 (3) (c).*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR Art. 28 (3) (c).*
- *To make users responsible for securing their authentication information. GDPR Art. 28 (3) (c).*
- *To prevent unauthorised access to systems and applications. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
	are designed and that requirements for access security are defined. We also inspected the year wheel and observed that a review and assessment of policies for access management has been planned. We observed that the policies were reviewed and audited in the period.	
Access to network and network services ▶ Access to network and network services requires a valid user-id. ▶ To access the business network it is required to create a VPN with two-factor authentication. ▶ Access is given to systems and data and is granted to users with a work-related need. ▶ Only employees in Denmark have access to personal data.	We interviewed relevant personnel and inspected material received. We inspected the system for access to systems. We observed that named user-id is created to the employees. We observed that access to the hosting environment is managed by a separate Active Directory, and that access to the system is restricted to employees with a work-related need via AD group. We inspected system configuration for VPN and observed that access to the system is via special AD group. We inspected system configuration for VPN server and observed that two-factor authentication is configured for users who connect to the hosting environment. We inspected the configuration of two-factor application on VPN server. We inspected system for two-factor authentication and observed that users are registered with a unit which can be used for verification of login. We reperformed login for a user and observed that an authentication request is sent to the mobile phone.	No exceptions noted.

A.9 - Access management

Control objectives

- *To restrict access to information and information processing facilities. GDPR Art. 28 (3) (c).*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR Art. 28 (3) (c).*
- *To make users responsible for securing their authentication information. GDPR Art. 28 (3) (c).*
- *To prevent unauthorised access to systems and applications. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
	We observed that only personnel in Denmark are granted access to systems with personal data.	
Creation, change and deregistration of users ▶ The company has designed a procedure for start, change and end of business relations. ▶ Creation of users is authorised by immediate manager. ▶ Granting of user access is role-based and based on the user's function and role. ▶ The user is given a temporary password at creation and this is changed at first log-on. ▶ Access rights are reassessed when changes are made to business relations. Granting of rights requires approval by immediate manager. ▶ When a business relationship is ended, the user is deactivated in all granted systems so that access to the company's system is prevented.	We interviewed relevant personnel and inspected material received. We inspected policies and procedures. We observed that procedures are designed for start, change and end of employments. We received and inspected documentation for creation of users. We observed that users are created as described in the procedure for creation of users internally in the data processor's domain. We observed that user creations are authorised by the employee's immediate manager. We inspected procedures for creation of users. We observed that users must be created with a temporary password at creation. By inquiry of relevant personnel, it was confirmed that password is changed at first login. We inspected Active Directory. We observed that rights are granted with standard roles based on the user's role. We were informed that none of the employees had their granted rights changed in the period, and thus there were no incidents to be used to test the control. The employee's understanding for the control was confirmed by inquiry of relevant personnel.	No exceptions noted.

A.9 - Access management

Control objectives

- *To restrict access to information and information processing facilities. GDPR Art. 28 (3) (c).*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR Art. 28 (3) (c).*
- *To make users responsible for securing their authentication information. GDPR Art. 28 (3) (c).*
- *To prevent unauthorised access to systems and applications. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
	We inspected Active Directory. We observed that resigned users are deactivated or deleted in Active Directory and do not have access to log-on.	
Management of privileged access rights ▶ Privileged access rights are granted on the basis of a work-related need. ▶ Privileged access rights are made on a special user-id. ▶ Use of privileged rights and granting of rights are logged and IT Management receives a notification hereof.	We interviewed relevant personnel and inspected material received. We inspected Active Directory and observed that internal users granted Domain Admin privileges are granted this on a special user-id. We observed that users with access to privileged access rights have a work-related need. We inspected system for logging and observed that Management is notified of use of administrative privileges and change of system critical configurations.	No exceptions noted.
Review of user access rights ▶ Granted accesses are reviewed at least once a year by the system owner.	We interviewed relevant personnel and inspected material received. We inspected the year wheel and observed that an annual review was made of granted accesses in March 2021. We observed that the review was made by the system owner.	No exceptions noted.
Management of secret authentication information ▶ Secret authentication information for system and service users is stored in an encrypted and access protected document. ▶ Only users with a special work-related need have access to passwords. ▶ Access to password document is granted by IT Management. ▶ Granting of rights to password management system is reviewed at least once a year.	We interviewed relevant personnel and inspected material received and system configuration. We inspected system for storing of system passwords. We observed that they are stored in an encrypted file. We inspected access rights for access to secret authentication information. We observed that only personnel with a work-related need are granted access. We observed also that the granting of rights is limited to the data processor's Management.	No exceptions noted.

A.9 - Access management

Control objectives

- *To restrict access to information and information processing facilities. GDPR Art. 28 (3) (c).*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR Art. 28 (3) (c).*
- *To make users responsible for securing their authentication information. GDPR Art. 28 (3) (c).*
- *To prevent unauthorised access to systems and applications. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
	We inspected the year wheel and observed that an annual review was made of granted accesses in March 2021. We observed that the review was made by the system owner.	
Limited access to information - Access to systems and file system is decided by a work-related need. Granting of access is authorised by the company's Management and/or system owner and is reviewed at least once a year.	We interviewed relevant personnel and inspected material received and system configuration. We inspected the year wheel and observed that an annual review was made of granted accesses in March 2021. We observed that the review was made by the system owner.	No exceptions noted.
Procedures for secure log-on - The user account will be locked automatically if several failing log-on attempts are made. - If an account is locked, and it cannot be related to the user, it will be registered in the incident log. - Log-on attempts are logged centrally. - Privileged access to customer-focused systems are protected by two-factor authentication. - Password are transmitted in encrypted form.	We interviewed relevant personnel and inspected material received. We inspected incident log. We observed that failing login attempts are registered in the incident log. We inspected domain policy for Active Directory in internal and hosting environment. We observed that user accounts are locked if several failing log-on attempts are made. We inspected system for log monitoring. We observed that failing login attempts are logged centrally in system for logging. We inspected system configuration for EG SafetyNet environment. We observed that two-factor authentication is used for privileged access to customer systems. We observed that default setup is that passwords are not transmitted in plain text over the network.	No exceptions noted.

A.9 - Access management

Control objectives

- *To restrict access to information and information processing facilities. GDPR Art. 28 (3) (c).*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR Art. 28 (3) (c).*
- *To make users responsible for securing their authentication information. GDPR Art. 28 (3) (c).*
- *To prevent unauthorised access to systems and applications. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
System for administration of passwords ▶ Users are given a personal user-id. ▶ Users can choose and change their own password. ▶ Passwords comply with the recommendations applicable at any time to safeguard passwords as regards, among others, length, complexity and change. ▶ Passwords are transmitted between client and server in encrypted form. ▶ Users must change password at first log-on.	We interviewed relevant personnel, made observations and inspected material received. We inspected system configuration for Active Directory. We observed that users are given a unique, personal user-id. We inspected domain policy for internal and EG SafetyNet Active Directory. We observed that appropriate requirements are defined for password for users in both domains. We inspected procedure for creation of users. We observed that user-id must be configured to change of password at first login.	No exceptions noted.
Use of privileged system programs - centralised systems ▶ Use of privileged system programs on servers require administrative rights. ▶ Only employees with a work-related need have access to use privileged system programs. ▶ Use of privileged system programs on servers is logged.	We interviewed relevant personnel, made observations and inspected material received. We inspected system configuration for domain controller. We observed that only employees with a work-related need are granted privileges to use system programs. We inspected system for logging. We observed that logging of changes is performed with privileged system programs.	No exceptions noted.
Management of source codes to programs - centralised systems ▶ Access to source codes is granted according to a work-related need. ▶ Source code is version managed in a centralised storage system.	We interviewed relevant personnel, made observations and inspected material received.	No exceptions noted.

A.9 - Access management

Control objectives

- *To restrict access to information and information processing facilities. GDPR Art. 28 (3) (c).*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR Art. 28 (3) (c).*
- *To make users responsible for securing their authentication information. GDPR Art. 28 (3) (c).*
- *To prevent unauthorised access to systems and applications. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
▶ Access to source code is granted by IT Management. ▶ Access to storage system is reviewed minimum once a year or at creation/closing of projects.	We inspected system configuration for Active Directory. We observed that users are granted specific rights in system for management of access to source code. We reviewed the granting of rights with Management. We observed that access is granted according to the employee's work-related need. We inspected system for storing of source code. We observed that source code is stored in projects and is version managed. We inspected the year wheel and observed that an annual review was made of granted accesses in March 2021. We observed that the review was made by the system owner.	

A.10 - Cryptography

Control objective

- *To ensure correct and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
Policy for use of cryptography ▶ Policy for use cryptography has been laid down and documented. ▶ Policy for use of cryptography is audited minimum once a year.	We interviewed relevant personnel and inspected material received. We received and inspected policies for cryptography. We observed that policies and procedures are designed and that requirements for cryptography are defined. We also inspected the year wheel and observed that review and assessment of policies for access management is planned. We inspected the year wheel and observed that an annual review was made of granted accesses in the period.	No exceptions noted.
Protection and encryption of information ▶ All workstations and delivered units are encrypted. ▶ The company's communication lines between the company, customers and business partners are protected by VPN or HTTPS.	We interviewed relevant personnel, made observations and inspected material received. We inspected for a sample the configuration of SMTP setups for production server. We observed that TLS encryption is activated and required. We inspected the web-server configuration for a suitable sample. We observed that communication over the internet is encrypted.	No exceptions noted.

A.11 – Physical and environmental security

Control objectives

- *To prevent unauthorised physical access to, and damage/disruption of the organisation's information and information processing facilities. GDPR Art. 28 (3) (c).*
- *To avoid loss, damage, theft or compromise of assets and disruptions in the organisation. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
Policy for physical and environmental security ▶ A policy for physical and environmental security has been laid down and documented. ▶ The policy for physical and environmental security is audited at least once a year.	We interviewed relevant personnel and inspected material received. We received and inspected the policies for physical and environmental security. We observed that policies and procedures are designed, and that requirements for physical and environmental security are defined. We also inspected the year wheel and observed that a review and assessment of policies for physical and environmental security is planned. We inspected the year wheel and observed that an annual review was made of policies in the period.	No exceptions noted.
Physical perimeter security ▶ Doors and windows are locked when not being used.	We interviewed relevant personnel and inspected office premises. We were informed that all doors and windows are locked when the workplace is left.	No exceptions noted.
Physical access control - data center ▶ The company reviews annually, see the year wheel, relevant reports and data processing agreement with Sentia Hosting.	We interviewed relevant personnel and inspected material received. We inspected procedure for review of report and compliance with requirements to service sub-suppliers with respect to physical and environmental security. We observed the implemented controls for review of reports, and a review and assessment of the service sub-supplier's report in the period. We inspected ISAE 3000 report for Sentia Denmark A/S' hosting activities (ISAE 3000 type 2 report for the period from 1st January 2021 to 31st December 2021). We observed that no qualifications and material comments are noted by the issuing auditor for the report.	No exceptions noted.

A.11 – Physical and environmental security

Control objectives

- *To prevent unauthorised physical access to, and damage/disruption of the organisation's information and information processing facilities. GDPR Art. 28 (3) (c).*
- *To avoid loss, damage, theft or compromise of assets and disruptions in the organisation. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
	We received and inspected SOC-2 report for Microsoft Azure for the period from 1st October 2020 to 30th September 2021. We observed that it is free of qualifications and material comments from the auditor issuing the report. We also observed that a Bridge Letter was obtained for the period from 1st October 2021 to 31st December 2021. We observed that no qualifications and material comments are noted by the issuing auditor for the report.	
Maintenance of equipment / removal of assets ▶ Equipment delivered to third party for service, repair or disposal are delivered without data disks. ▶ Information assets are removed only subject to prior approval by EG-IT.	We interviewed relevant personnel and inspected procedure and policies. We inspected procedure for maintenance and delivery of information assets. On inquiry of relevant personnel their understanding for the control was confirmed, and it was confirmed that the employee was informed of guidelines for maintenance and delivery of information assets. We have received and inspected cooperation agreements with external partners. At the date of this report, there were no incidents to be used for test of the control relating to maintenance and delivery of information assets, and we are therefore unable to comment on the implementation of the control.	No exceptions noted.
Secure disposal or reuse of equipment ▶ Equipment which is scrapped or is to be destroyed is stored in a secure room. ▶ Used or scrapped data media and disks are registered and destroyed.	We interviewed relevant personnel and inspected procedure and policies. We inspected policy for disposal reuse of equipment. By inquiry of relevant personnel, we have reviewed the procedure for destruction and deletion. The understanding of relevant personnel for the control was confirmed and it was confirmed that the employee was informed of guidelines for secure disposal or reuse of equipment.	No exceptions noted.

A.11 – Physical and environmental security

Control objectives

- *To prevent unauthorised physical access to, and damage/disruption of the organisation's information and information processing facilities. GDPR Art. 28 (3) (c).*
- *To avoid loss, damage, theft or compromise of assets and disruptions in the organisation. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
	At the date of this report, there were no incidents to be used for test of the control relating to disposal or reuse of equipment, and we are therefore unable to comment on the implementation of the control.	
Policy for clear desk and blank screen ▶ Documents with confidential or sensitive information are shredded when the documents are no longer to be used for the purpose for which they were printed out. ▶ Printers are placed in a printer room with limited access. ▶ Printouts containing confidential information are immediately collected in the printer. ▶ PC is locked with screen lock when the workplace is left.	We interviewed relevant personnel and inspected procedure and policies. We inspected configuration of group policy in Active Directory for screen lock. We observed that automated screen lock after 15 minutes is configured and that the screen is password protected. We inspected for a sample the configuration of screensaver on workstations. We observed that screensaver is configured and that the user does not have access to deactivate it. We were informed that personal data are not printed out.	No exceptions noted.

A.12 - Operations security

Control objectives

- *To ensure proper and secure operation of information processing facilities. GDPR Art. 25, Art. 28 (3) (c).*
- *To ensure that information and information processing facilities are protected against malware. GDPR Art. 28 (3) (c).*
- *To protect against data loss. GDPR Art. 28 (3) (c).*
- *To record incidents and provide evidence. GDPR Art. 33 (2).*
- *To ensure the integrity of operating systems. GDPR Art. 28 (3) (c).*
- *To prevent technical vulnerabilities being exploited. GDPR Art. 28 (3) (c).*
- *To minimize the impact of audit activities on operating systems. GDPR Art. 28 (1).*

Control activity	Test performed by BDO	Result of test
Policy for operations security ▶ Policy for operations security has been laid down and documented. ▶ Policy for operations security is audited annually.	We interviewed relevant personnel and inspected material received. We received and inspected policies for operations security. We observed that policies and procedures are designed for IT operations and that requirements for operations security. We also inspected the year wheel and observed that a review and assessment of the policies for operations security is planned. We inspected the year wheel and observed that an annual review was made of policies in the period.	No exceptions noted.
Documented operations procedure ▶ Descriptions of procedures or working instructions are prepared for routine tasks. ▶ Material interruptions of operations and irregularities which impact business critical applications are registered in an incident log. ▶ Instructions are prepared for restore of mission-critical systems.	We interviewed relevant personnel and inspected material received. We inspected procedures and work descriptions received. We observed that instructions for routine tasks were prepared. We observed that an incident log is created for incidents relating to operations. We inspected the incident log and observed that, based on a registered incident, an action plan was initiated to address similar incidents. We observed that instructions are prepared for restore of mission-critical systems.	No exceptions noted.

A.12 - Operations security

Control objectives

- *To ensure proper and secure operation of information processing facilities. GDPR Art. 25, Art. 28 (3) (c).*
- *To ensure that information and information processing facilities are protected against malware. GDPR Art. 28 (3) (c).*
- *To protect against data loss. GDPR Art. 28 (3) (c).*
- *To record incidents and provide evidence. GDPR Art. 33 (2).*
- *To ensure the integrity of operating systems. GDPR Art. 28 (3) (c).*
- *To prevent technical vulnerabilities being exploited. GDPR Art. 28 (3) (c).*
- *To minimize the impact of audit activities on operating systems. GDPR Art. 28 (1).*

Control activity	Test performed by BDO	Result of test
Patch management - system software ▶ All material changes are identified, managed and documented in Patch Management System. ▶ Test and deployment is planned as part of the patch management procedure. ▶ All material changes are approved before implementation. ▶ Information security is ensured as part of patch management. ▶ All relevant stakeholders are informed and involved to the necessary extent. ▶ All material changes are subject to risk assessment before implementation. ▶ Emergency procedures and fallback are planned as part of patch management.	We interviewed relevant personnel and inspected system configuration and material received. We observed that the updates for automated installation have been assessed. We observed that installation of all existing updates is made without delay. We inspected system for update of third-party software. We observed that workstations are updated. We inspected the updating policy. We observed that all applications are updated automatically. We inspected group policy in Active Directory. We observed that workstations are updated automatically. We inspected system configuration for server updates. We observed for a sample that updates are installed automatically once a week.	No exceptions noted.
Capacity management ▶ Systems critical to operations are monitored in real time for capacity utilization and resource scarceness.	We interviewed relevant personnel and inspected system configuration. We inspected system for capacity monitoring. We observed that capacity monitoring is configured of disk, CPU, memory and partition. We observed also that there is application-specific monitoring of SQL, web and other servers. We observed that alerts are sent to recipients at the sub-processor who are responsible for taking corrective measures.	No exceptions noted.

A.12 – Operations security

Control objectives

- *To ensure proper and secure operation of information processing facilities. GDPR Art. 25, Art. 28 (3) (c).*
- *To ensure that information and information processing facilities are protected against malware. GDPR Art. 28 (3) (c).*
- *To protect against data loss. GDPR Art. 28 (3) (c).*
- *To record incidents and provide evidence. GDPR Art. 33 (2).*
- *To ensure the integrity of operating systems. GDPR Art. 28 (3) (c).*
- *To prevent technical vulnerabilities being exploited. GDPR Art. 28 (3) (c).*
- *To minimize the impact of audit activities on operating systems. GDPR Art. 28 (1).*

Control activity	Test performed by BDO	Result of test
Controls against malware ▶ Servers and workstations are protected with Antivirus. ▶ Antivirus software is updated regularly. ▶ Procedure for management of malware outbreaks is described and implemented.	We interviewed relevant personnel and inspected system configuration and material received. We inspected system for malware protection. We observed that there is a centrally managed antivirus system. We extracted and inspected status report on installed agents. We inspected policy for updating of definitions. We observed that automated updating is activated. We inspected for a sample servers and workstations. We observed that agent is installed and activated. We inspected procedures and policies. We observed that procedures for management of malware outbreaks are described. The employees' understanding for the control was confirmed by inquiry of relevant personnel.	No exceptions noted.
Backup of information ▶ Backup is taken of all servers and data drives. ▶ Backup rotation, retention time and scope are based on a risk assessment. ▶ Backup is checked daily. ▶ Readability of backup media is tested currently. ▶ Restore tests of mission-critical systems are carried out currently.	We interviewed relevant personnel and inspected system configuration and material received. We inspected system for backup We observed that daily backup is set up and that retention is set to six months on-site. We observed that the latest backup is copied to Microsoft Azure environment for the purpose of Disaster Recovery. Backup data are encrypted before transit to Azure.	No exceptions noted.

A.12 - Operations security

Control objectives

- *To ensure proper and secure operation of information processing facilities. GDPR Art. 25, Art. 28 (3) (c).*
- *To ensure that information and information processing facilities are protected against malware. GDPR Art. 28 (3) (c).*
- *To protect against data loss. GDPR Art. 28 (3) (c).*
- *To record incidents and provide evidence. GDPR Art. 33 (2).*
- *To ensure the integrity of operating systems. GDPR Art. 28 (3) (c).*
- *To prevent technical vulnerabilities being exploited. GDPR Art. 28 (3) (c).*
- *To minimize the impact of audit activities on operating systems. GDPR Art. 28 (1).*

Control activity	Test performed by BDO	Result of test
	We observed that alerting via email is configured and that there is weekly an integrity test of last week's backup. We observed that a system restore of server was carried out on 8th April and 6th September 2021.	
Incident logging, protection of log data, administrator and operator log - There is logging for network and servers of critical importance to operations, logging is collected and analysed. - Alarms are monitored and managed by IT manager. - Only employees with a work-related need have access to logging. - There is separate logging for users with administrative privileges. - Logging is collected and safeguarded in a centralised database.	We interviewed relevant personnel and inspected system configuration. We inspected system for logging. We observed that there is a centralised collection of logging. We observed that material changes and incidents are reported. We observed also that data are analysed in the system, and that a notification is sent in case of suspicious behaviour. We observed that access is granted for logging for employees with a work-related need. One user is created in system for logging. We inspected system for storing of system password. We observed that only employees with a work-related need have access to login data for system for logging. We inspected the logging policy for Domain Controller. We observed that all available incidents are logged and that logging is configured for logging for use of administrative privileges. We inspected logging in EG SafetyNet. We observed that access to and editing of personal data in EG SafetyNet are logged.	No exceptions noted.

A.12 – Operations security

Control objectives

- *To ensure proper and secure operation of information processing facilities. GDPR Art. 25, Art. 28 (3) (c).*
- *To ensure that information and information processing facilities are protected against malware. GDPR Art. 28 (3) (c).*
- *To protect against data loss. GDPR Art. 28 (3) (c).*
- *To record incidents and provide evidence. GDPR Art. 33 (2).*
- *To ensure the integrity of operating systems. GDPR Art. 28 (3) (c).*
- *To prevent technical vulnerabilities being exploited. GDPR Art. 28 (3) (c).*
- *To minimize the impact of audit activities on operating systems. GDPR Art. 28 (1).*

Control activity	Test performed by BDO	Result of test
Software installation on operating systems ▶ Software installation on operating systems is subject to change management.	We interviewed relevant personnel and inspected system configuration and material received. There were no incidents to be used for test of implementation of the control. We inspected procedure for software installation on operating systems and system for registration of changes. We observed that a system has been implemented for management of changes. By interviews, relevant employees' understanding for the control was confirmed.	No exceptions noted.
Technical vulnerability management ▶ A weekly external vulnerability scanning is carried out by an external partner on services exposed towards the internet.	We interviewed relevant personnel and inspected material received. We received and reviewed documentation performed vulnerability scanning. We observed that a vulnerability scanning was carried out. We observed also that the findings were assessed.	No exceptions noted.
Limitations on software installation ▶ The IT policy sets out the frames for use and installation of software. ▶ Installation of software requires prior approval from the entity's Management.	We interviewed relevant personnel and inspected system configuration and material received. We have for a suitable sample inspected workstation. We observed that local users do not have access to install software. We inspected procedure for installation of workstation. We observed that this procedure includes a list of software approved for installation on workstations without Management's approval.	We have found that users are granted privileged access on workstations. No further exceptions noted.

A.13 - Communications security

Control objectives

- *To ensure protection of network information and supportive information processing facilities. GDPR Art. 28 (3) (c).*
- *To maintain information security when transferring internally in an organisation and to an external entity. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
Policy for communication security ▶ A policy for communication security has been laid down and documented. ▶ The policy for communication security is audited annually.	We interviewed relevant personnel and inspected material received. We received and inspected policies for communication security. We observed policies and procedures, and the requirements for communication security are laid down. We also inspected the plan for recurring controls. We observed that a review and assessment of policies for communication security have been performed in September 2021.	No exceptions noted.
Network management ▶ Access to the configuration of network units is granted only to employees with a work-related need.	We interviewed relevant personnel and inspected system configuration. We inspected system configuration for network units. We observed that access is granted only to employees with a work-related need. We observed that passwords are stored in a system for storage of secret authentication data. We inspected the plan for recurring controls. We observed that an annual review of accesses granted was performed in the period.	No exceptions noted.
Securing network services ▶ Access to the company's operating network is protected with encryption and two-factor authentication.	We interviewed relevant personnel and inspected material received. We have verified access to operating network. We observed two-factor authentication is used.	No exceptions noted.

A.13 - Communications security

Control objectives

- *To ensure protection of network information and supportive information processing facilities. GDPR Art. 28 (3) (c).*
- *To maintain information security when transferring internally in an organisation and to an external entity. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
Divided network ▶ The network is divided into several security zones depending on the required security level. ▶ Security zones are separated by firewall. ▶ Services exposed towards the internet are placed in DMZ and protected by firewall.	We interviewed relevant personnel and inspected system configuration and data center. We inspected system configuration for firewall and Hyper-V servers. We observed that LAN and DMZ are configured on firewall. We inspected network adapters and vSwitch configuration for Hyper-V in LAN and DMZ. We observed that security zones are separated. We inspected the rules set up in firewall. We observed that there is a limitation of the services that can be accessed from WAN.	No exceptions noted.
Electronic messages ▶ EG SafetyNet - EG A/S uses e-mail to communicate with external parties. The e-mail communication is encrypted in the transmission.	We interviewed relevant personnel. We inspected system for e-mail communication in EG SafetyNet. We observed that the system is configured with encryption of communication. We were informed that personal data are not sent to customers. If it is required to assist customers retrieving information, this is done in the customer's own system and with the rights that the relevant customer's employee has been granted in the customer's system. The employees' understanding for the control was confirmed by inquiry of relevant personnel.	No exceptions noted.
Non-disclosure and secrecy agreements ▶ Data processing agreements are made or signed NDA, if supplier has access to or processes personal data, confidential information or sensitive data.	We interviewed relevant personnel and inspected material received. We received sub-processor agreements. We observed that sub-processor agreements are made with hosting providers.	No exceptions noted.

A.13 – Communications security

Control objectives

- *To ensure protection of network information and supportive information processing facilities. GDPR Art. 28 (3) (c).*
- *To maintain information security when transferring internally in an organisation and to an external entity. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
Import of customer basic data (department hierarchy and employees): ▶ Customer data are transferred via encrypted traffic either via an HTTPS Web service call or via FTPS/SFTP transferred csv/xml files. ▶ Imported basic data files are deleted after end of use.	We interviewed relevant personnel and made observations. We inspected for a sample system configuration for FTP-server. We observed that communication is TLS encrypted. We inspected for a sample the data folder for SFTP server. We observed that data are deleted.	No exceptions noted.

A.14 - Development and maintenance of systems

Control objectives

- *To ensure that information security is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems that provide public network services. GDPR Art. 25.*
- *To ensure that information security is organised and implemented within the information systems development life cycle. GDPR Art. 25.*
- *To ensure protection of data used for testing. GDPR Art. 25.*

Control activity	Test performed by BDO	Result of test
Policy for acquisition, development and maintenance of systems ▶ A policy for acquisition, development and maintenance of systems has been laid down and documented. ▶ The policy for acquisition, development and maintenance of systems is audited annually.	We interviewed relevant personnel and inspected material received. We received and inspected policies for acquisition, development and maintenance of systems. We observed policies have been designed and that procedures for acquisition, development and maintenance of systems are laid down. We inspected the year wheel and observed that a review and assessment of policies for acquisition, development and maintenance of systems is planned. We observed that a review of the policy was carried out in the period.	No exceptions noted.
Analysis and specification of information security requirements ▶ All projects relating to development or changes of information systems are covered by EG SafetyNet - EG A/S' project model according to which information security requirements are an obligatory area. ▶ Information security requirements are documented in the project documentation. ▶ In connection with new acquisitions, change of outsourcing partner, entering of agreements with a new outsourcing partner or the like, a risk assessment is carried out.	We interviewed relevant personnel, inspected material received and made observations. We observed that there is a specification requests for changes. We inspected overview of changes for the period. We observed that for all changes it is assessed whether the change will impact processing of personal data. We observed that the assessment is included in the project documentation. We were informed that there were no major new acquisitions or changes of sub-processors and, thus, there were no incidents to be used to test the control for risk assessment when entering into new agreements. We inspected procedures and policies. The employees' understanding for the control was confirmed by inquiry of relevant personnel.	No exceptions noted.

A.14 - Development and maintenance of systems

Control objectives

- *To ensure that information security is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems that provide public network services. GDPR Art. 25.*
- *To ensure that information security is organised and implemented within the information systems development life cycle. GDPR Art. 25.*
- *To ensure protection of data used for testing. GDPR Art. 25.*

Control activity	Test performed by BDO	Result of test
Secure development policy ▶ All projects are documented. ▶ OWASP is used as framework for secure development.	We interviewed relevant personnel, inspected material received and made observations. We inspected the case system and observed that changes are documented in the customer's requests for changes and in change cases. We inspected policies and procedures. We observed that procedures have been designed for development according to the OWASP framework. The employees' understanding for the control was confirmed by inquiry of relevant personnel. We have inspected an overview of implemented changes during the period. We have inspected documentation for changes for an appropriate sample.	No exceptions noted.
Principles for development of secure systems ▶ All tasks or changes in EG SafetyNet are assessed for impact on processing of personal data. ▶ Privacy by design and privacy by default are ensured when making changes relating to personal data. ▶ The company performs system approval test of components and integrated systems before commissioning.	We interviewed relevant personnel, inspected documentation and made observations. We inspected Jira which is used to register all changes and development tasks. We observed that, to create a task, it must be assessed if the change impacts or includes personal data. We observed for a sample that data protection is included in design and operating effectiveness. We inspected for a sample the documentation for test of changes. We observed that system approval tests are carried out and documented for the change.	No exceptions noted.

A.14 - Development and maintenance of systems

Control objectives

- *To ensure that information security is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems that provide public network services. GDPR Art. 25.*
- *To ensure that information security is organised and implemented within the information systems development life cycle. GDPR Art. 25.*
- *To ensure protection of data used for testing. GDPR Art. 25.*

Control activity	Test performed by BDO	Result of test
Segregation of development, test and operating environments ▶ Rules for transfer of software from development to operation are described in the policy for change management. ▶ Development, test and operating environments for mission-critical systems are segregated. ▶ Changes are tested in a separate environment before commissioning. ▶ All data in development and test environment are anonymised and masked. ▶ If customers require ”Live-data” in test, a separate environment is created for this purpose. This environment is secured at the same level as operating environments.	We interviewed relevant personnel, inspected system configuration and made observations. We observed by sampling that tests are carried out in a separate environment before roll-out in production environment. We inspected test environment for a randomly selected customer and observed that data are anonymized. We observed that masking routine for test environment is monitored, and that a follow-up action plan is prepared and that corrective procedures are performed in case of any deviations. There is no available test environment with live-data. The relevant employees understanding for the control for creation of test environments including personal data was confirmed by interviews.	No exceptions noted.

A.15 – Supplier relationships

Control objectives

- *To ensure protection of the organisation's assets that suppliers have access to. GDPR Art. 28 (2) and (3) (d), and Art. 28 (4).*
- *To maintain an agreed level of information security and delivery of services under the supplier agreements. GDPR Art. 28 (2) and (3) (d), and Art 28 (4).*

Control activity	Test performed by BDO	Result of test
Compliance with agreements/management of security in supplier agreements ▶ It is required that the suppliers' information security level complies with the requirements of EG SafetyNet - EG A/S' information security policy. This is ensured by contracts, NDA or data processing agreements. ▶ Service suppliers have an obligation to prove their compliance with EG SafetyNet - EG A/S' information security policy. ▶ Service suppliers have an obligation to allow Front-Avenue A/S to audit processes and controls relating to the agreement. ▶ Service suppliers have an obligation to inform EG SafetyNet - EG A/S of information security incidents. ▶ EG SafetyNet - EG A/S obtains and reviews annually ISAE 3000, ISAE 3402 or SOC-2 auditor's reports for suppliers of mission-critical services.	We interviewed relevant personnel, and inspected material received and made observations. We received data processing agreements, appendices and report for Sentia. We inspected the data processing agreement and observed that this is appropriately drawn up and is adequate in relation to the data processor's compliance with the General Data Protection Regulation and the obligations in relation to the data controller and the data subject. We observed that the data processor has access to perform audit of processes and controls relating to the agreement. We observed also that the sub-processor has an obligation to inform the data processor of information security incidents. We inspected the data processor's documentation for controls completed. We observed that reports from sub-processors have been obtained, reviewed and assessed. We inspected ISAE 3000 report for Sentia Denmark A/S' hosting activities for the period from 1st January 2021 to 31st December 2021. We observed that no qualifications and material comments are noted by the issuing auditor for the report. We received and inspected SOC-2 report for Microsoft Azure for the period from 1st October 2020 to 30th September 2021. We observed that no qualifications and material comments are noted by the issuing auditor for the report. We observed also that a Bridge Letter was obtained for the period from 1st October 2021 to 31st December 2021. We inspected Microsoft Azure library for reports.	No exceptions noted.

A.15 – Supplier relationships

Control objectives

- *To ensure protection of the organisation's assets that suppliers have access to. GDPR Art. 28 (2) and (3) (d), and Art. 28 (4).*
- *To maintain an agreed level of information security and delivery of services under the supplier agreements. GDPR Art. 28 (2) and (3) (d), and Art 28 (4).*

Control activity	Test performed by BDO	Result of test
Monitoring and review of supplier services ▶ EG SafetyNet - EG A/S performs an annual evaluation of service supplier's fulfilment of deliveries. If exceptions occur, these are followed up with the supplier.	We interviewed relevant personnel and inspected material received. The employee's understanding for the control was confirmed by interviews of relevant personnel. We inspected incident log. We observed that there were no incidents to be used for testing of the control for monitoring and review of supplier services and, therefore, we have no comments in this respect. We were informed that an informal evaluation is made of service sub-suppliers in connection with change of the contract with the individual service sub-suppliers.	No exceptions noted.
Management of changes in supplier services ▶ When material changes are made to delivery, ownership, economic, organisational and other security conditions at the supplier, the service must be subject to a new risk assessment by EG SafetyNet - EG A/S.	We interviewed relevant personnel and inspected policies relating to suppliers. We received and inspected policy for suppliers. We observed that a policy was designed for change of supplier services. We inspected the documentation for the most recent risk assessment. We observed that the sub-processors' controls are included in the risk assessment. The employee's understanding for the control was confirmed by interviews of relevant personnel. There were no incidents to be used for testing of the control for monitoring and review of supplier services and, therefore, we have no comments in this respect.	No exceptions noted.

A.16 – Information security incident management

Control objective

- *To ensure a uniform and effective method of managing information security breaches, including communication on security incidents and weaknesses. GDPR Art. 33 (2).*

Control activity	Test performed by BDO	Result of test
Reporting of information security incidents ▶ All Information security incidents, weaknesses and breaches are reported to Management. ▶ All Information security incidents, weaknesses and breaches are registered by Management in an incident log. ▶ All Information security incidents are assessed in relation to confidentiality, integrity and accessibility.	We interviewed relevant personnel, inspected documentation received and system for registration of incidents, and made observations. The employees' awareness of the procedure for information security breaches and incidents was confirmed. We inspected policies and procedure for management of information security incidents. We observed by sampling that incidents are registered in an incident log. We inspected registered incidents for a sample. We observed that the incident was assessed and that suitable corrective measures were taken.	No exceptions noted.
Management of information security breaches ▶ Information security breaches are managed according to a specified procedure.	We interviewed relevant personnel, inspected documentation received and system for registration of incidents, and made observations. The employees' awareness of the procedure for management of information security breaches was confirmed. We inspected policies and procedure for management of information security breaches. The employee's understanding for the control was confirmed by interviews of relevant personnel. We inspected system for registration of information security breaches. We observed that there were no incidents to be used for testing of the control for management of information security incidents and, therefore, we have no comments in this respect.	No exceptions noted.

A.16 – Information security incident management

Control objective

- *To ensure a uniform and effective method of managing information security breaches, including communication on security incidents and weaknesses. GDPR Art. 33 (2).*

Control activity	Test performed by BDO	Result of test
Experience from information security breaches ▶ EG SafetyNet – EG A/S reviews monthly the incident log and take measures to improve the information security.	We interviewed relevant personnel and inspected material received. We inspected system for registration of information security breaches. We observed that action plans have been implemented to currently improve the information security. We have observed that monthly reporting and review of incidents is carried out.	No exceptions noted.

A.17 – Information security aspects

Control objectives

- *To ensure that information security continuity is rooted in the organisation's management systems for contingency, emergency and restore management. GDPR Art. 28 (3) (c).*
- *To ensure accessibility of information processing facilities. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
Planning of information security continuity ▶ A plan for information security continuity is established based on a risk assessment.	We interviewed relevant personnel and inspected material received. We inspected policy for information security continuity and IT emergency response plan. We observed that procedures are designed for establishment and organisation of emergency response in connection with information security breaches.	No exceptions noted.
Implementation of information security continuity ▶ The organisational and management structure during emergency response is specified in the procedure for contingency, emergency and restore management. ▶ An overall emergency plan is prepared which describes the overall procedure for initiating emergency response and organisation of emergency response. ▶ Roles and responsibilities relating to activation of emergency response is communicated to relevant persons, including information on placing of required descriptions and information. ▶ A procedure and work descriptions are prepared for restore of mission-critical systems.	We interviewed relevant personnel and inspected material received. We observed that descriptions are prepared for management structure, roles and responsibilities relating to establishment of emergency response. We observed also that the organisation is informed of their roles and that emergency response plans are made available to relevant personnel. We inspected procedures and work descriptions for restore of mission-critical systems. We observed that work descriptions are prepared for restore of operating infrastructure and services relating to operation of EG SafetyNet.	No exceptions noted.
Verification, review and evaluation of information security continuity ▶ As regards critical systems, the emergency response plan must be tested in connection with implementation of the system. ▶ Emergency response plans are audited once a year, in connection with implementation of new systems or changes in the risk assessment. ▶ Emergency response plans are tested out according to a specified rotation plan. Test of emergency response plans is planned in the year wheel.	We interviewed relevant personnel and inspected system logging. There were no incidents to be used for testing that the control for test of emergency response plans in connection with implementation of systems is performed and, therefore, we have no comments in this respect. We inspected documentation for annual controls. We observed that emergency response plans are audited in connection with the annual controls. We observed that the performance of annual controls was completed in the period.	No exceptions noted.

A.17 – Information security aspects

Control objectives

- *To ensure that information security continuity is rooted in the organisation's management systems for contingency, emergency and restore management. GDPR Art. 28 (3) (c).*
- *To ensure accessibility of information processing facilities. GDPR Art. 28 (3) (c).*

Control activity	Test performed by BDO	Result of test
	We inspected logging for system restore. We observed that a testing was made monthly of a partial system restore for servers in the production environment, monthly in the period. We observed that a systematic testing of system restore is planned in the plan for recurring controls.	
Accessibility of information processing facilities. - Mission-critical systems are virtualised and redundant hardware is available in the server room for critical hardware. - Emergency response plans are stored electronically in several physical locations.	We interviewed relevant personnel and inspected hardware in data center We inspected system configuration. We observed that servers are virtualised and that there is redundant hardware. We inspected system for storing of emergency response plans We observed that these are stored in an internal system and that a copy is stored in an alternative location.	No exceptions noted.

A.18 – Compliance

Control objectives

- *To prevent violations of statutory, public authority or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28 (2), Art. 28 (3) (a), Art. 28 (3) (e), Art. 28 (3) (g), Art. 28 (3) (h), Art. 28 (3) (f), Art. 28 (10), Art. 29, Art. 32 (4), Art. 33 (2).*
- *To ensure that information security is implemented and operated in accordance with the organisation's policies and procedures. GDPR Art. 28 (1).*

Control activity	Test performed by BDO	Result of test
Compliance with applicable legislation and contractual requirements ▶ EG SafetyNet - EG A/S' day-to-day Management is responsible for compliance with relevant legislative, public authority and contractual requirements. ▶ All relevant legislative, public authority and contractual requirements and method to comply with these requirements are identified, documented and updated. ▶ Guidelines for retention, storing, management and disposal of registrations and information are described in the business procedure descriptions. ▶ Confidential and sensitive personal data are protected in accordance with relevant legislation, including the General Data Protection Regulation. ▶ Personal data are retained in Denmark and are not transferred to third countries or organisations that are not covered by EU-US Privacy Shield.	We interviewed relevant personnel and inspected relevant policies and procedures. We inspected policies and procedures for compliance with legislative and contractual requirements. We observed that relevant legislation is identified, and that procedures and instructions are prepared for compliance with legislation and assistance to the data controller. We inspected record of information assets. We observed that information assets are classified in accordance with policies for management of assets. We observed also that guidelines for storing, management and disposal are described in the business procedure descriptions. The employee's understanding for the protection of personal data was confirmed by interviews of relevant personnel. We inspected system configuration. We observed that data are stored on servers placed in Denmark. We observed also that encrypted backup copy is transferred to Microsoft Azure. We have reviewed the data processor agreement and data processor agreement with Microsoft regarding the use of Microsoft Azure. We have observed that according to the agreement, only data centers in the EU may be used, and we have inspected documentation for this.	EG SafetyNet - EG A/S has stated that there is no transfer of personal data to third countries and that they have configured security measures to protect personal data using Microsoft Azure as a sub-data processor. However, there is a risk of potential unintentional transfer of data from the sub-processor Microsoft Azure to the third country of the United States, as Microsoft Azure as a US-owned company is subject to US law. Based on the Data Inspectorate's Cloud guidelines, an unintentional transfer will have to be considered as a personal data breach for the data processor. No further exceptions noted.

A.18 – Compliance

Control objectives

- *To prevent violations of statutory, public authority or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28 (2), Art. 28 (3) (a), Art. 28 (3) (e), Art. 28 (3) (g), Art. 28 (3) (h), Art. 28 (3) (f), Art. 28 (10), Art. 29, Art. 32 (4), Art. 33 (2).*
- *To ensure that information security is implemented and operated in accordance with the organisation's policies and procedures. GDPR Art. 28 (1).*

Control activity	Test performed by BDO	Result of test
Procedure for making written, electronic data processing agreements and audit ▶ A procedure for obtaining and assessing data processing agreements has been designed and implemented. ▶ All relevant personnel are informed of the procedure for obtaining and assessing data processing agreement. ▶ EG SafetyNet - EG A/S performs annually an internal audit to ensure that information security controls are effective. ▶ Assistance to support the data controller in relation to the obligations to the data subject, including deletion, audit and inspection and demonstration of processing security is described in data processing agreements.	We interviewed relevant personnel and inspected documentation. We inspected procedure for obtaining data processing agreement with suppliers. We received and inspected a standard data processing agreement. The employee's understanding of the procedure for making the data processing agreement with the data controller was confirmed by interview of an employee. We inspected overview of data processing agreements with customers, including securing instructions, assessing instructions, and notifying in case of illegal instructions. We observed that a standard data processing agreement is drawn up which is sent to customers. In a few cases a diverging agreement has been made. It is described in the overview which modifications are made in the applicable agreement if it differs from the standard agreement. We inspected support system. We observed that there is for all customers a reference to the placing of the data processing agreement a memo on who is the customer's data controller contact person. The employees' understanding for the control was confirmed by inquiry of relevant personnel. We were informed that current control is made of the compliance of information security. We observed that a follow-up is made on the system owner's controls. We inspected record of data controllers. We inspected data processing agreements for a sample.	No exceptions noted.

A.18 – Compliance

Control objectives

- *To prevent violations of statutory, public authority or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28 (2), Art. 28 (3) (a), Art. 28 (3) (e), Art. 28 (3) (g), Art. 28 (3) (h), Art. 28 (3) (f), Art. 28 (10), Art. 29, Art. 32 (4), Art. 33 (2).*
- *To ensure that information security is implemented and operated in accordance with the organisation's policies and procedures. GDPR Art. 28 (1).*

Control activity	Test performed by BDO	Result of test
	We inspected data processing agreement and procedures for assistance to the data controller and procedure for deletion. We observed that assistance is described.	
Review of information security - EG SafetyNet - EG A/S' Management is responsible for taking steps to review the information security, including control objectives, policies and procedures, to ensure that relevant IT security policies are complied with and in order to prepare statements.	We interviewed relevant personnel and inspected relevant policies and procedures. We inspected policy for review of information security. We observed that the responsibility for an annual review of the information security is determined. By interview of relevant employees, the employee's understanding for the control was confirmed by interview of relevant personnel. We inspected documentation for the data processor's controls. We observed that a review of the information security and of own controls has been made. We were informed that a current control is carried out of the compliance with the information security. We observed that a follow-up is made on the system owner's controls.	No exceptions noted.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR NO. 20 22 26 80