



ISAE 3000 REPORT AT 15 APRIL 2018 ON THE DESCRIPTION OF TECHNICAL AND ORGANISATIONAL MEASURES AND THEIR DESIGN RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION

GOT ETHICS A/S

# CONTENT

Auditor's Report	2
Statement by Got Ethics A/S	4
Got Ethics A/S' Description	6
Control Objectives, Controls, Tests and Result of Tests	10
A.5: Security Policies - Management direction for information security	11
A.6: Organisation of Information Security - Internal organisation, mobile devices and teleworking	12
A.7: Human Resource Security - Prior to, during and termination and change of employment	15
A.8: Responsibility for Assets - Information classification and media handling	17
A.9: Access Control	21
A.10: Cryptography	27
A.11: Physical and Environmental Security	28
A.12: Operations Security	31
A.13: Communications security	38
A.14: System acquisition, development and maintenance	40
A.15: Supplier relationships	44
A.16: Information security incident management	46
A.17: Information security aspects of business continuity management	49
A.18: Compliance	51
App Reporting Channel	54
Phone Hotline	55
Translation Service	56

## AUDITOR'S REPORT

### INDEPENDENT AUDITOR'S ISAE 3000 REPORT AT 15 APRIL 2018 ON DESCRIPTION OF TECHNICAL AND ORGANISATIONAL MEASURES AND THEIR DESIGN RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION

To: The Management of Got Ethics A/S  
Got Ethics A/S' Customers

#### Scope

We have been engaged to report on Got Ethics A/S' (the Processor) description at pages 6-9 of the Whistleblower system and related technical and organisational measures (controls) for processing of personal data on behalf of controllers subject to the EU regulation on protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation) at 15 April 2018 (the Description) and on the design of technical and organisational measures (controls) at 15 April 2018 related to the described control objectives.

We have not performed any procedures in relation to the operating effectiveness of the controls included in the description and, accordingly, we do not express any opinion hereon.

#### The Processor's Responsibilities

At page 4 of this report, the Processor has made a statement on the suitability of the overall presentation of the description.

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

#### Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the FSR - "Code of Ethics for Danish Professional Accountants" which is based on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct.

We are subject to the international standard on quality control, ISQC 1, and apply and maintain a comprehensive system for quality control, including documented policies and procedures for complying with rules of ethics, professional standards and applicable requirements according to legislation and other regulation.

#### Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Processor's description and on the design of the controls related to the control objectives stated in the description. We conducted our engagement in accordance with ISAE 3000, Assurance Reports Other Than Audits or Reviews of Historical Financial Information and additional requirements according to relevant Danish legislation. 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 suitably designed.

An assurance engagement to report on the description and design of controls at a Processor involves performing procedures to obtain evidence about the disclosures in the Processor's description of its system, and the design of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the Processor and described at page 4.

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

As described above, we have not performed any procedures in relation to the operating effectiveness of the controls included in the description and, accordingly, we do not express any opinion hereon.

#### **Limitations of Controls at a Data Processor**

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

#### **Opinion**

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described at page 4. In our opinion, in all material respects:

- (a) The description presents fairly the Whistleblower system and related technical and organisational measures (controls) as designed and implemented at 15 April 2018; and
- (b) The technical and organisational measures (controls) related to the control objectives stated in the description were suitably designed at 15 April 2018.

#### **Description of Tests of Controls**

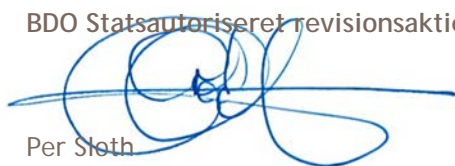
The specific controls tested and the nature, timing and results of those tests are listed at pages 11 - 56.

#### **Intended Users and Purpose**

This report, including the description of tests of controls at pages 11 - 56, is intended only for the Controllers, who have used the Processor's Whistleblower system, and who have a sufficient understanding to consider it, along with other information including information about controls operated by the Controllers themselves, when assessing whether the requirements of the General Data Protection Regulation are fulfilled.

Copenhagen 18 April 2018

**BDO Statsautoriseret revisionsaktieselskab**



Per Sloth  
Partner, Head of Risk Assurance  
Registered Public Accountant



## STATEMENT BY GOT ETHICS A/S

Got Ethics A/S is responsible for processing of personal data of our customers, who are controllers according to the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "General Data Protection Regulation").

The following description is intended for controllers using the Whistleblower system, and who have a sufficient understanding to consider the description along with other information, including information about controls operated by the controllers themselves, when assessing whether the requirements of the General Data Protection Regulation are fulfilled.

Got Ethics A/S confirms that the accompanying description at pages 6-9 presents fairly the Whistleblower system, which has processed personal data for controllers subject to the General Data Protection Regulation, and the related technical and organisational measures (controls) at 15 April 2018. The criteria we used in making this statement were that we:

1. Account for the design and implementation of the Whistleblower system and the related technical and organisational measures (controls), including:
  - The type of services provided, including the type of personal data processed.
  - The processes of both IT and manual systems used to process personal data, such as collection, recording, structuring, storage, adaption or alteration, retrieval, restriction, erasure or destruction.
  - The processes used to ensure data processing in accordance with contract, instruction or agreement with the controller.
  - The processes ensuring that the persons authorised to process personal data have a duty of confidentiality.
  - The processes ensuring at the completion of the data processing that all personal data are, as elected by the controller, erased or returned to the controller unless legislation or regulation prescribes retention of the personal data.
  - The processes that in case of breach of the personal data security ensure that the controller can file a report to the supervisory authority and assist the controller to inform the data subjects.
  - The processes ensuring appropriate technical and organisational measures for the processing of personal data with due regard to the risks that the processing involves, especially as regards accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data that are transmitted, stored or otherwise are processed.
  - Technical and organisational measures (controls) that we have assumed, with reference to the design of the Whistleblower system, to be implemented by the controllers and which, if necessary to achieve the control objectives described, are identified in the description.
  - Other aspects of our control environment, risk assessment process, and communication, control activities and monitoring controls that have been relevant to the processing of personal data.
2. Base our control objectives and the implemented controls and processes on the framework set out in ISO 27001.
3. Do not omit or distort information relevant to the scope of the described Whistleblower system and the related technical and organisational measures (controls) for processing of personal data considering that the description is prepared to meet the general needs of a wide range of controllers and therefore cannot include every aspect of the Whistleblower system that the individual controller may consider of importance to their special environment.

Got Ethics A/S confirms that the technical and organisational measures (controls) related to the control objectives stated in the accompanying description were suitably designed at 15 April 2018. The criteria we used in making this statement were that:

1. The risks threatening achievement of the described control objectives 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.

Got Ethics A/S confirms that appropriate technical and organisational measures are implemented and maintained to fulfil the agreements with the controllers, good practices for the processing of data, and relevant requirements in relation to processors in accordance with the General Data Processing Regulation.

Yours sincerely

Got Ethics A/S

  
Jesper Dannemann  
COO

## GOT ETHICS A/S' DESCRIPTION

### INTRODUCTION

Got Ethics A/S is a company providing software products to our customers.

Got Ethics A/S has 2 offices. The general management and the consulting/implementation function reside in the Copenhagen office. The IT development/operating department reside in the office in Holstebro.

Got Ethics A/S' main product is a whistleblower solution. The whistleblower solution is a platform where whistleblowers can submit incidents to a web-based case management system where the incidents are handled by case investigators appointed by Got Ethics A/S' customers. It is possible for the case investigators to engage into a dialogue with the whistleblowers in a way where the identity of the whistleblower is not revealed to the case investigators.

Got Ethics A/S has been providing whistleblower solutions to our customers since 2011.

The basic version of the whistleblower system contains a web-based reporting portal and a web-based case management system. Furthermore, the customers can purchase the following add-on products:

- Smart phone apps as a separate reporting channel.
- Phone hotline as a separate reporting channel.
- Translation service where reported incidents and uploaded documents can be translated by an independent translation company.

It is essential to Got Ethics A/S' management to maintain full focus on information security to ensure that the implemented controls are effective and meets generally accepted standards for information security. The implemented information security measures are assessed regularly, and it is evaluated whether they need to be adjusted.

To emphasize that information security is an important matter to Got Ethics A/S, it has been decided to obtain an assurance report from an independent auditor.

### THE SYSTEM

The system is a SaaS (Software as a Service) - which is an internet-based application hosted by Got Ethics A/S.

The system consists of several reporting interfaces and an administrator portal. Furthermore, a translation service can be acquired as an add-on service.

Below, the following terms are used:

- "Customers" are Got Ethics A/S customers who have purchased a license to use the system.
- "Informants" are whistleblowers etc. submitting incidents to the Customers through the system.
- "Incidents" are knowledge or suspicion about unethical or criminal behavior submitted in the system by Informants. Incidents are submitted to the case management system (administrator portal) by the Customers' employees and/or business relations/business partners.
- "Case Investigators" are persons appointed the Customer (typically employees) who receive the Incidents, investigate the Incident and communicates with the Informant if necessary.

### Reporting Interfaces

#### *Web Portal*

Incidents can anonymously (or not anonymously) be reported on a SSL encrypted web form. The Incidents (HTML) are sent to the case management system in the administrator portal where they are stored encrypted.

Logging of IP addresses has been disabled on the web server to protect the identity of the Informant.

The communication between the Informant and the Case Investigators is done anonymously (or not anonymously) via the web portal on a SSL encrypted web form.

#### *Smartphone Apps for iPhone and Android*

Incidents can anonymously (or not anonymously) be reported via an app.

The Incidents (text/voice/movie) are sent encrypted to the case management system in the administrator portal where it is stored encrypted.

Voice messages sent through the app are obfuscated irreversibly to protect the identity of the Informant.

The communication between the Informant and the Case Investigators is done (encrypted) anonymously (or not anonymously) via the app.

The app is an add-on product that can be purchased separately and is tailor made to each Customer.

#### *Phone Hotline*

Incidents can be reported through a phone hotline (recording of voice messages).

Voice messages recorded via the phone hotline are obfuscated irreversibly to protect the identity of the Informant and stored encrypted in the case management system in the administrator portal.

The communication between the Informant and the Case Investigators is done via an interface between the administrator portal (Case Investigators) and a telephone number (Informant) with an IVR menu system. Questions from the Case Investigators are read aloud to the informant via speech synthesis. Answers and further comments are recorded as a voice message by the Informant.

The phone hotline is an add-on product that can be purchased separately by each Customer.

#### **Administrator Portal**

In the system's administrator portal, the customer's Case Investigators/administrator users can perform the case management.

Furthermore, the system settings (including the security settings) can be configured in the administrator portal.

All sensitive personal data in the customers' whistleblower systems is encrypted while in transit and at rest with a customer-specific encryption key that is kept by the Customer. None of Got Ethics A/S' employees (even the systems developers) can decrypt the encrypted sensitive personal data stored in the Customers' systems.

#### **Translation Service**

Customers can include a translation service where reported Incidents and uploaded documents are translated to other languages.

The translation is performed in an interface in the system by an independent translation company. The translation service is carried out by translators who are approved by the Danish police authorities.

Translations are performed in Got Ethics A/S' IT infrastructure via remote desktop connections. This way it can be ensured that all sensitive information is stored in a protected environment at all times where the appropriate security measures have been implemented. It is not possible for the translators to copy information from the remote desktop.



### The Customers' Responsibility

It is set out in the service contract between the customer and Got Ethics A/S that it is the responsibility of the customer to:

- Review the transaction log regularly,
- Ensure that the password policy configured in the system complies with the requirements of the regulation of processing of personal data relating to complexity, periodic password change, and temporary suspension of logins in case of unsuccessful login attempts (brute force settings),
- Implement procedures for deletion of transaction log and sensitive personal data in accordance with the guidelines of the regulation of processing of personal data,
- Cancel systems access for leaving employees and, in the situation where an employee changes to a job where the relevant person is not to have access to the system.

### IDENTIFICATION AND ASSESSMENT OF RISKS AND IMPLEMENTATION OF CONTROLS

Got Ethics A/S' management has analyzed the risks relating to the system. A business continuity risk assessment as well as a data protection impact assessment has been conducted.

The business continuity risk assessment is based on identification of the risks, how likely the situations generating the risks are to occur and what the impact would be for Got Ethics A/S if the situations should occur.

The data protection impact assessment is based on the article 29 data protection working party's guidelines. The assessment identifies the processes where personal data are being processed and assesses what the consequences would be for the affected data subjects if the processed personal data should be compromised.

The risk assessments are being conducted (reassessed) with regular intervals and furthermore if an event should occur that would make it appropriate to conduct a reassessment.

Based on the risk analysis, the management has defined the relevant control objectives and implemented the necessary and sufficient controls to ensure that the system complies with the requirements set out in the general data protection regulation and follows the framework set out in ISO 27001.

The main areas and control objectives are described below. A full list of control objectives and selected controls are amended as an appendix to the audit report.

### MAIN AREAS ISO 27001 AND CONTROL OBJECTIVES

Main areas ISO 27001	Control Objectives
A.5: Security Policies	<ul style="list-style-type: none"> <li>• To provide guidelines for and supporting information security in accordance with business requirements and relevant laws and regulations. GDPR art. 28, section 1, art. 28, section 3, letter c.</li> </ul>
A.6: Organisation of information security	<ul style="list-style-type: none"> <li>• To establish a management basis for initiating and managing the implementation and operation of information security in the organization. GDPR art. 37, section 1.</li> <li>• To secure remote workplaces and the use of mobile equipment. GDPR art. 28, section 3, letter c.</li> </ul>
A.7: Human resource security	<ul style="list-style-type: none"> <li>• To ensure that employees understand their responsibilities and are suitable for the roles they are intended. GDPR art. 28, section 1, art. 28, section 3, art. 37, section 1.</li> <li>• To protect the organization's interests as part of the change or termination of the employment relationship.</li> </ul>
A.8: Responsibility for assets	<ul style="list-style-type: none"> <li>• To identify the organization's assets and define appropriate responsibilities for its protection.</li> <li>• To ensure adequate protection of information that is in relation to the importance of the information for the organization (GDPR Article 30, section 3, Article 30, section 4).</li> <li>• To prevent unauthorized disclosure, modification, removal or destruction of information stored on media (GDPR Article 28, section 3, letter c).</li> </ul>

Main areas ISO 27001	Control Objectives
A.9: Access control	<ul style="list-style-type: none"> <li>To restrict access to information and information processing facilities (GDPR Article 28, section 3, letter c).</li> <li>To ensure access for authorized users and prevent unauthorized access to systems and services (GDPR Article 28, section 3, letter c).</li> <li>To make users responsible for securing their authentication information (GDPR Article 28, section 3, letter c).</li> <li>To prevent unauthorized access to systems and applications (GDPR Article 28, section 3, letter c).</li> </ul>
A.10: Cryptography	<ul style="list-style-type: none"> <li>To ensure the correct and effective use of cryptography to protect the confidentiality, authenticity and / or integrity of information (GDPR Article 28, section 3, letter c).</li> </ul>
A.11: Physical and Environmental security	<ul style="list-style-type: none"> <li>To prevent unauthorized physical access to, and damage/disruption of the organization's information and information processing facilities (GDPR Article 28, section 3, letter c).</li> <li>To avoid loss, damage, theft or compromise of assets and disruptions in the organization.</li> </ul>
A.12: Operations security	<ul style="list-style-type: none"> <li>To ensure proper and safe operation of information processing facilities (GDPR Article 25, Article 28, section 3, letter c).</li> <li>To ensure that information and information processing facilities are protected against malware (GDPR Article 28, section 3, letter c).</li> <li>To protect against data loss (GDPR Article 28, section 3, letter c).</li> <li>To record events and provide evidence (GDPR Article 33, section 2).</li> <li>To ensure the integrity of operating systems (GDPR Article 28, section 3, letter c).</li> <li>To prevent technical vulnerabilities being exploited (GDPR Article 28, section 3, letter c).</li> <li>To minimize the impact of audit activities on operating systems.</li> </ul>
A.13: Communications security	<ul style="list-style-type: none"> <li>To ensure protection of network information and supportive information processing facilities (GDPR Article 28, section 3, letter c).</li> <li>To maintain information security when transferring internally in an organization and to an external entity (GDPR Article 28, section 3, letter c).</li> </ul>
A.14: System acquisition, development and maintenance	<ul style="list-style-type: none"> <li>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 Article 25).</li> <li>To ensure that information security is organized and implemented within the information systems development life cycle (GDPR Article 25).</li> <li>To ensure the protection of data used for testing (GDPR Article 25).</li> </ul>
A.15: Supplier relationships	<ul style="list-style-type: none"> <li>To ensure protection of the organization's assets that suppliers have access to (GDPR Article 28, section 2, Article 28, section 3, letter d, Article 28, section 4).</li> <li>To maintain an agreed level of information security and delivery of services under the supplier agreements (GDPR Article 28, section 2, Article 28, section 3, letter d, Article 28, section 4).</li> </ul>
A.16: Information security incident management	<ul style="list-style-type: none"> <li>To ensure a uniform and effective method of managing information security breaches, including communication on security incidents and weaknesses (GDPR Article 33, section 2).</li> </ul>
A.17: Information security aspects of business continuity	<ul style="list-style-type: none"> <li>To ensure that information security continuity is rooted in the organization's management systems for emergency and re-establishment (GDPR Article 28, section 3, letter c).</li> <li>To ensure accessibility of information processing facilities (GDPR Article 28, section 3, letter c).</li> </ul>
A.18: Compliance	<ul style="list-style-type: none"> <li>To prevent violations of statutory, regulatory or contractual requirements in relation to information security and other security requirements (GDPR Article 25, Article 28, section 2, Article 28, section 3, letter a, Article 28, section 3, letter e, Article 28, section 3, letter g, Article 28, section 3, letter h, Article 28, section 3, letter f, Article 28, section 10, Article 29, Article 32, section 4, Article 33, section 2).</li> <li>To ensure that information security is implemented and run in accordance with the organization's policies and procedures.</li> </ul>
App reporting channel	<ul style="list-style-type: none"> <li>To ensure secure capture, storage and processing of incidents via the smartphone apps for iPhone and Android (GDPR Article 28, section 3, letter c).</li> </ul>
Phone hotline	<ul style="list-style-type: none"> <li>To ensure secure capture, storage and processing of incidents (voice messages) via the phone hotline solution (GDPR Article 28, section 3, letter c).</li> </ul>
Translation service	<ul style="list-style-type: none"> <li>To ensure that all information processed by translators are processed in a secure manner (GDPR Article 28, section 3, letter c).</li> </ul>

## CONTROL OBJECTIVES, CONTROLS, TESTS AND RESULT OF TESTS

In the following, the relevant control objectives and implemented control activities, designed to achieve the control objectives, are described and selected by Got Ethics A/S.

We have described the tests performed that were considered necessary to obtain reasonable assurance that the described control objectives were achieved, and that the relevant controls were implemented at 15 April 2018.

The tests of the design and implementation of controls were performed by inquiries, inspection and observation.

Type	Description
Inquiry	<p>Inquiries of relevant personnel at Got Ethics A/S have been performed for all significant control activities.</p> <p>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.</p>
Inspection	<p>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, ie 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.</p> <p>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.</p>
Observation	<p>The use and existence of specific controls has been observed, including tests to ensure that the control has been implemented.</p>

With respect to the services provided by Microsoft Corporation - Microsoft Azure (Germany), we have received a SOC 2 report from independent auditor on controls related to the operation and hosting services for the period from 1 October 2016 to 30 September 2017 and an ISO 27001:2013 certificate for Microsoft Deutschland MCIO GmbH for the following areas: Infrastructure, Development, Security and engineering services/systems, Operations, Data trustee controls and Support for the following Azure Services in accordance with Microsoft Germany Azure ISMS Statement of Applicability 2017.02, dated 1 June 2017 and valid from 19 January 2017 to 18 January 2020 and certified by TÜV NORD CERT GmbH.

With respect to the services provided by Cogeco Peer 1 in Canada, we have received a SOC 1 / SSAE 18 report from independent auditor on IT general controls related to the operation and hosting services for the period from 1 July 2016 to 30 June 2017.

With respect to the services provided by Supertel A/S, we have received an ISAE 3402 type II report from independent auditor on IT general controls related to the operation and hosting services for the period from 1 January to 31 December 2017.

The relevant control objectives and controls of these service sub-organisations are not included in Got Ethics A/S' description of services and controls related to the operation of the whistleblower system. Thus, we have solely considered the report and tested the controls at Got Ethics A/S which monitor the functionality of the service sub-organisations' controls.

A.5: Security Policies - Management direction for information security		
<b>Control Objective</b> ▪ To provide guidelines for and supporting information security in accordance with business requirements and relevant laws and regulations. GDPR art. 28, section 1, art. 28, section 3, letter c.		
Control Activity	Test performed by BDO	Result of test
<b>Establish policies for information security</b> • An Information Security Policy has been implemented.	We have made inquiries of relevant personnel and inspected the "Information Security Policy" and "Code of Good Information Security Behavior".  We have observed that "Code of Good Information Security Behavior" is signed by all employees with access to the IT infrastructure in March 2018.	No deviations identified.
<b>Periodical review of the policies for information security</b> • Procedures have been implemented to ensure periodic reviews of the Information Security Policy.	We have made inquiries of relevant personnel.  We have inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Business Continuity Risk Assessment", "Data Protection Impact Assessment" and "Code of Good Information Security Behavior".  We have inspected the latest periodic review of policies for information security from 3 April 2018 carried out by the Information Security Committee.  We have observed that the "Information Security Policy", "Business Continuity Risk Assessment" and "Data Protection Impact Assessment" are reviewed and approved at 23 March 2018.	No deviations identified.



**A.6: Organisation of Information Security - Internal organisation, mobile devices and teleworking****Control Objective**

- To establish a management basis for initiating and managing the implementation and operation of information security in the organization. GDPR art. 37, section 1.
- To secure remote workplaces and the use of mobile equipment. GDPR art. 28, section 3, letter c.

Control Activity	Test performed by BDO	Result of test
<b>Establish information security roles and responsibilities</b> <ul style="list-style-type: none"> <li>Procedures have been implemented to ensure that the roles and responsibilities are defined and communicated to the employees.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls and "Code of Good Information Security Behavior".</p> <p>We have observed that "Code of Good Information Security Behavior" is signed by all employees with access to the IT infrastructure in March 2018.</p>	No deviations identified.
<b>Segregation of duties</b> <ul style="list-style-type: none"> <li>Segregation of the groups working with the test, development and production environment have been implemented to the extent possible.</li> <li>Actions performed by employees in the production environment are logged.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls and "Information Security Policy" and "Information Security in Project Management".</p> <p>We have observed that segregation of duties is managed by using groups and that the test, development and production environments are placed at different servers in different environments.</p> <p>We have observed that there are logging of actions performed by employees in the production environment.</p>	No deviations identified.
<b>Contact with special interest groups</b> <ul style="list-style-type: none"> <li>Periodic contact with information security specialists to exchange ideas and get input regarding information security.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls and "Report Review Report".</p> <p>We have observed that the security specialists at the Processor periodically exchange ideas and input regarding the information security.</p>	No deviations identified.
<b>Implement information security in project management</b> <ul style="list-style-type: none"> <li>Procedures have been implemented to ensure that information security implications are considered in project management.</li> <li>Periodic discussions related to information security implications.</li> <li>Addressing information security risks are integrated in the programming assignments.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Information Security in Project Management".</p> <p>We have inspected the documentation for the recent project and Build. We have made inquiries of relevant development personnel regarding projects and Builds.</p> <p>We have observed that the security specialists at the Processor periodically discuss related information security implications.</p>	No deviations identified.

**A.6: Organisation of Information Security - Internal organisation, mobile devices and teleworking****Control Objective**

- To establish a management basis for initiating and managing the implementation and operation of information security in the organization. GDPR art. 37, section 1.
- To secure remote workplaces and the use of mobile equipment. GDPR art. 28, section 3, letter c.

Control Activity	Test performed by BDO	Result of test
	We have observed that addressed information security risks are an integrated part of the programming assignments.	
<b>Mobile device policy</b> <ul style="list-style-type: none"> <li>• A policy for the use of mobile devices have been implemented.</li> <li>• Access restriction requirements.</li> <li>• Installation of anti-virus, anti-malware programs and software firewall.</li> <li>• Updating of operating systems.</li> <li>• Internet access via secure lines.</li> <li>• Encryption when transferring sensitive data.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Policy for use of Mobile devices".</p> <p>We have observed that the Processor has a policy for use of mobile devices and remote access and that these are known by the employees. We have observed that all employees have signed the "Code of Good Information Security Behavior"</p> <p>We have by interviews and walk-through of mobile devices and configuration observed that:</p> <ul style="list-style-type: none"> <li>• There are access restrictions to mobile devices by passwords and the devices are locked after inactivity laptop after 10 minutes and mobile phones after 1 minute.</li> <li>• Anti-virus and malware programs and software firewall are installed.</li> <li>• The software must at all times be updated at mobile devices. This is the employees' responsibility.</li> <li>• USB-mobile devices must be encrypted by using 7-zip using AES-256 encryption.</li> <li>• The Processor uses secure lines by using RDS.</li> </ul> <p>We have selected laptops and mobile phones and observed that they were updated and that the employees use internal encryption keys when transferring sensitive data.</p>	No deviations identified.
<b>Teleworking</b> <ul style="list-style-type: none"> <li>• A policy for teleworking and remote access have been implemented.</li> <li>• No storing of sensitive data on remote workplaces.</li> <li>• Secure access to files.</li> <li>• Secure remote access for developers.</li> <li>• Requirements to install anti-virus, anti-malware programs and software firewall.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Policy for Teleworking and Remote Access".</p> <p>We have observed that the Processor has a policy for use of teleworking and remote access and that these are known by the employees. We have observed that all employees have signed the "Code of Good Information Security Behavior".</p>	No deviations identified.

## A.6: Organisation of Information Security - Internal organisation, mobile devices and teleworking

### Control Objective

- To establish a management basis for initiating and managing the implementation and operation of information security in the organization. GDPR art. 37, section 1.
- To secure remote workplaces and the use of mobile equipment. GDPR art. 28, section 3, letter c.

Control Activity	Test performed by BDO	Result of test
<ul style="list-style-type: none"> <li>• Secure remote access to the production environment.</li> <li>• Commitment to the Code of Good Information Security Behavior.</li> </ul>	<p>We have by interviews and walk-through of teleworking and configuration observed the following:</p> <ul style="list-style-type: none"> <li>• The Processor has a policy for not storing sensitive data on remote workplaces; we have observed that employees are aware of that.</li> <li>• For access to company files the employees have to use Remote Desktop (RDS) to access data, which are hosted on Office 365 SharePoint.</li> <li>• The Processor uses secure lines by using VPN and RDS. We have observed that the remote connection has to be established from a dedicated work computer, and that a certificate has to be installed on that computer.</li> <li>• We have inspected the configuration of RDS for selected employees and observed that they only have the access rights needed.</li> <li>• Anti-virus and malware programs and software firewall are installed. The software must at all times be updated. The "Production Environment Access Group" is responsible for managing these updates.</li> </ul>	

A.7: Human Resource Security - Prior to, during and termination and change of employment		
<b>Control Objective</b> <ul style="list-style-type: none"> <li>To ensure that employees understand their responsibilities and are suitable for the roles they are intended. GDPR art. 28, section 1, art. 28, section 3, art. 37, section 1.</li> <li>To protect the organization's interests as part of the change or termination of the employment relationship.</li> </ul>		
Control activity	Test performed by BDO	Result of test
<b>Screening</b> <ul style="list-style-type: none"> <li>Personal interview.</li> <li>Investigation of criminal records.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and criminal records for employees.</p> <p>According to the procedures, the Processor interviews the employee to be and check the background e.g. with former employer and asks for a copy of criminal records.</p> <p>We have observed that the Processor has received criminal records from their employees.</p>	No deviations identified.
<b>Terms and conditions of employment</b> <ul style="list-style-type: none"> <li>The terms and the conditions of the employment are set out in: <ul style="list-style-type: none"> <li>An employment contract.</li> <li>A non-disclosure undertaking.</li> <li>A Code of Good Information Security Behavior.</li> <li>The Information Security Policy.</li> </ul> </li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior", "Non-disclosure Undertaking" and "Employment Contract".</p> <p>We have inspected:</p> <ul style="list-style-type: none"> <li>The terms and conditions of employment.</li> <li>The standard employment contract and the contract for an employee</li> </ul> <p>We have observed that:</p> <ul style="list-style-type: none"> <li>Non-disclosure undertaking is signed by all employees.</li> <li>Code of Good Information Security Behavior are signed by all employees.</li> <li>All employees must read and agree to the Information Security Policy.</li> </ul>	No deviations identified.
<b>Management responsibilities</b> <ul style="list-style-type: none"> <li>Implemented a policy for communication and management of information security responsibilities involving the general management and the managers.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls and "Information Security Policy".</p> <p>We have observed that the information Security Policy is signed by the Information Security Committee.</p>	No deviations identified.



**A.7: Human Resource Security - Prior to, during and termination and change of employment****Control Objective**

- To ensure that employees understand their responsibilities and are suitable for the roles they are intended. GDPR art. 28, section 1, art. 28, section 3, art. 37, section 1.
- To protect the organization's interests as part of the change or termination of the employment relationship.

Control activity	Test performed by BDO	Result of test
<b>Disciplinary process</b> <ul style="list-style-type: none"> <li>• The consequences of violating the employment contract and the information security policies are set out in the employment contract and the Code of Good Information Security Behavior.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls and "Information Security Policy".</p> <p>We have observed that:</p> <ul style="list-style-type: none"> <li>• Consequences of violation of the employment contract and the "Information Security Policy" are set out in the Employment contract and the "Code of Good Information Security Behavior"</li> <li>• "Code of Good Information Security Behavior" is signed by all employees yearly.</li> </ul>	No deviations identified.
<b>Termination or change of employment responsibilities</b> <ul style="list-style-type: none"> <li>• Employees are bound by the non-disclosure undertaking after the termination.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior", "Non-disclosure Undertaking", "Employment Contract" and documentation for dismissed employees.</p> <p>We have inspected the master for revocation of access to IT systems and revocation of assets and keys.</p> <p>We have inspected the documentation for returning assets and keys and for revocation of access to IT systems for recent employee who left the Processor on 31 January 2018.</p>	No deviations identified.

**A.8: Responsibility for Assets - Information classification and media handling****Control Objective**

- To identify the organization's assets and define appropriate responsibilities for its protection.
- To ensure adequate protection of information that is in relation to the importance of the information for the organization (GDPR Article 30, section 3, Article 30, section 4).
- To prevent unauthorized disclosure, modification, removal or destruction of information stored on media (GDPR Article 28, section 3, letter c).

Control Activity	Test performed by BDO	Result of test
<b>Inventory of assets</b> <ul style="list-style-type: none"> <li>• An inventory of information assets has been established.</li> <li>• The responsibility to maintain the inventory have been defined.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Inventory of Information Assets".</p> <p>We have observed that the Processor has established an inventory of information assets and it is updated in March 2018.</p> <p>We have observed that it is the "Information Asset Group" that has the responsibility for maintaining the list of inventory.</p>	No deviations identified.
<b>Ownership of assets</b> <ul style="list-style-type: none"> <li>• The ownership (responsibility to manage and maintain) of information assets have been identified for all information assets.</li> <li>• The responsibility to maintain the list of information asset ownership has been appointed.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Inventory of Information Assets".</p> <p>We have observed that the "Information Asset Group" has the responsibility for maintaining the list of inventory and we have been informed that it contains all the information assets of the Processor.</p>	No deviations identified.
<b>Acceptable use of assets</b> <ul style="list-style-type: none"> <li>• An acceptable use of assets policy has been incorporated in the Code of Good Information Security Behavior.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that "Code of Good Information Security Behavior" contains acceptable use of assets policy and that all employees have signed this document in March 2018.</p>	No deviations identified.
<b>Return of assets</b> <ul style="list-style-type: none"> <li>• A procedure has been implemented for retrieving information assets from employees in case of termination of the employment.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Revocation of Assets" and "Inventory of Information Assets".</p> <p>We have observed the procedure for retrieving information assets from employees in connection with termination of the employment.</p>	No deviations identified.

**A.8: Responsibility for Assets - Information classification and media handling****Control Objective**

- To identify the organization's assets and define appropriate responsibilities for its protection.
- To ensure adequate protection of information that is in relation to the importance of the information for the organization (GDPR Article 30, section 3, Article 30, section 4).
- To prevent unauthorized disclosure, modification, removal or destruction of information stored on media (GDPR Article 28, section 3, letter c).

Control Activity	Test performed by BDO	Result of test
	We have inspected the documentation for returning assets and keys for recent employee who left the Processor on 31 January 2018.	
<b>Classification of information</b> <ul style="list-style-type: none"> <li>• The different information handled and managed by the organization have been identified and separated in categories reflecting the consequences if the information was compromised.</li> <li>• Appropriate measures have been implemented to protect the information taking into account the classification of the information.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Inventory of Information Assets".</p> <p>We have observed that the Processor has established an inventory of information assets form which it follows who is responsible.</p> <p>We have been informed that the Processor has divided breaches of information as follows:</p> <ol style="list-style-type: none"> <li>1. Information that has no or little consequences.</li> <li>2. Information that would not be critical to the company, but would have some impact.</li> <li>3. Information that would have critical business impact - short term.</li> <li>4. Information that would be critical to survival of the company - long term.</li> </ol> <p>We have observed that the data in classification categories 2-4 are encrypted and most of the data in classification category 1 are encrypted as well.</p>	No deviations identified.
<b>Labeling of information</b> <ul style="list-style-type: none"> <li>• Procedures have been implemented to ensure appropriate labelling of information assets during transfer.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Inventory of Information Assets".</p> <p>We have observed that the data in classification categories 2-4 are encrypted and most of the data in classification category 1 are encrypted as well - during transfer.</p> <p>We have observed when the employees are sharing sensitive data by using internal key passes and passwords.</p>	No deviations identified.

**A.8: Responsibility for Assets - Information classification and media handling****Control Objective**

- To identify the organization's assets and define appropriate responsibilities for its protection.
- To ensure adequate protection of information that is in relation to the importance of the information for the organization (GDPR Article 30, section 3, Article 30, section 4).
- To prevent unauthorized disclosure, modification, removal or destruction of information stored on media (GDPR Article 28, section 3, letter c).

Control Activity	Test performed by BDO	Result of test
<b>Handling of assets</b> <ul style="list-style-type: none"> <li>• A procedure for handling assets have been implemented to ensure correct classification of the information, compliance with the access control policy, correct registration and appropriate storage.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Inventory of Information Assets".</p> <p>We have observed that to ensure segregation of duties the Processor has implemented a strong password policy by using 2-factor authentication, complexity and ensured that the employee only has access to what is necessary to fulfil his/hers work.</p>	No deviations identified.
<b>Management of removable media</b> <ul style="list-style-type: none"> <li>• A procedure for storing information on removable media have been implemented to ensure that sensitive information is not compromised.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Inventory of Information Assets".</p> <p>We have observed that the Processor has a procedure for storing of information on removable media to ensure that sensitive data are saved.</p>	No deviations identified.
<b>Disposal of media</b> <ul style="list-style-type: none"> <li>• A procedure has been implemented for deleting sensitive information on media in connection of the disposal of the media.</li> <li>• The responsibility for secure disposal of media has been appointed.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Inventory of Information Assets".</p> <p>We have observed that the Processor has a procedure for deleting sensitive information on media before disposal.</p>	No deviations identified.
<b>Physical media transfer</b> <ul style="list-style-type: none"> <li>• A procedure has been implemented to ensure secure transfer of physical media.</li> <li>• Only use of recognized and professional couriers.</li> <li>• Appropriate labelling of the media.</li> <li>• Securing sensitive data during the transfer of the media.</li> <li>• Secure storing during the transfer to avoid destruction of the media.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Inventory of Information Assets".</p> <p>We have observed that the Processor has a procedure for physical media transfer. We have observed encrypted customer data.</p>	No deviations identified.



**A.8: Responsibility for Assets - Information classification and media handling****Control Objective**

- To identify the organization's assets and define appropriate responsibilities for its protection.
- To ensure adequate protection of information that is in relation to the importance of the information for the organization (GDPR Article 30, section 3, Article 30, section 4).
- To prevent unauthorized disclosure, modification, removal or destruction of information stored on media (GDPR Article 28, section 3, letter c).

Control Activity	Test performed by BDO	Result of test
	<p>We have observed that "Cryptographic Key Management Group" has checked and found that the Cryptographic Technologies were adequate and appropriate at 12 March 2018 for:</p> <ul style="list-style-type: none"><li>• Passwords</li><li>• Encryption of sensitive data in transit</li><li>• Encryption of sensitive data at rest</li></ul> <p>We have observed that the procedure for physical media transfer is known by the employees.</p>	

**A.9: Access Control****Control Objective**

- To restrict access to information and information processing facilities (GDPR Article 28, section 3, letter c).
- To ensure access for authorized users and prevent unauthorized access to systems and services (GDPR Article 28, section 3, letter c).
- To make users responsible for securing their authentication information (GDPR Article 28, section 3, letter c).
- To prevent unauthorized access to systems and applications (GDPR Article 28, section 3, letter c).

Control Activity	Test performed by BDO	Result of test
<b>Access control policy</b> <ul style="list-style-type: none"> <li>• A policy for access control and access to networks has been implemented.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that the Processor has implemented access control policy for access to networks.</p>	No deviations identified.
<b>Access to networks and network services</b> <ul style="list-style-type: none"> <li>• Employees only have access to the systems and networks they need to fulfil their job (need to know principle).</li> <li>• Approval procedure implemented determining who is authorized to grant/revoke access to networks and network services.</li> <li>• Use of VPN, 2 factor authentication and similar authorization mechanisms where appropriate.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that the Processor has implemented different roles and accesses to the IT infrastructure and systems and the employees have only the access they need to fulfil their job.</p> <p>We have observed that the "Production Environment Access Group" has admin rights to give access in the network and network services.</p> <p>We have observed that the Processor uses VPN/RDS with 2-factor authentication for remote access.</p>	No deviations identified.
<b>User registration and de-registration</b> <ul style="list-style-type: none"> <li>• Procedure for creation of new used IDs has been implemented.</li> <li>• Use of unique user IDs.</li> <li>• Reuse of deleted user IDs requires reconfiguring of all access rights etc.</li> <li>• User IDs for employees leaving the organization are revoked immediately (regarding user IDs in the whistleblower system, this obligation lies with the customer).</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Non-disclosure Undertaking".</p> <p>We have observed that the Processor has procedures for creating new users with unique user IDs and that it is not allowed to reuse deleted users' IDs.</p> <p>We have inspected the documentation for revocation of access to IT systems for the recent employee who left the Processor on 31 January 2018.</p>	No deviations identified.

## A.9: Access Control

### Control Objective

- To restrict access to information and information processing facilities (GDPR Article 28, section 3, letter c).
- To ensure access for authorized users and prevent unauthorized access to systems and services (GDPR Article 28, section 3, letter c).
- To make users responsible for securing their authentication information (GDPR Article 28, section 3, letter c).
- To prevent unauthorized access to systems and applications (GDPR Article 28, section 3, letter c).

Control Activity	Test performed by BDO	Result of test
<b>User access provisioning</b>  <i>Got Ethics</i> <ul style="list-style-type: none"> <li>• Procedure for provisioning and revocation of user IDs has been implemented.</li> <li>• Responsibility for the appointment of user IDs has been allocated.</li> <li>• Central registration of access rights.</li> <li>• Periodic review.</li> </ul> <i>The whistleblower system</i> <ul style="list-style-type: none"> <li>• The user access provisioning is solely conducted by the customer.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Non-disclosure Undertaking".</p> <p>We have observed that procedures for user access provisioning have been implemented.</p> <p>We have received documentation for the recent periodic review carried out by the IT Security Committee at 3 April 2018.</p> <p>We have observed that the Processor has verification of employees' identities.</p> <p>We have observed that the user access provisioning in the Whistleblower system is conducted by the customer.</p>	No deviations identified.
<b>Management of privileged access rights</b> <ul style="list-style-type: none"> <li>• The number of users with privileged access rights in production systems has been reduced to the extent possible.</li> <li>• The possibility of using privileged access rights in production systems has been reduced to the extent possible.</li> <li>• Logging of actions performed by users with privileged access rights in production systems have been implemented to the extent possible.</li> <li>• Users with privileged access rights to production systems are registered and must be approved to the management.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Non-disclosure Undertaking".</p> <p>We have observed that it is only the "Production Access Group" who has admin rights in the production environment</p> <p>We have observed that, to get access to the production environment, the access has to be done by special workstations with certificates.</p> <p>We have observed that actions performed by users with privileged access rights in the production systems are logged.</p> <p>We have observed that users with privileged access are approved by the Processor's management.</p>	No deviations identified.

## A.9: Access Control

### Control Objective

- To restrict access to information and information processing facilities (GDPR Article 28, section 3, letter c).
- To ensure access for authorized users and prevent unauthorized access to systems and services (GDPR Article 28, section 3, letter c).
- To make users responsible for securing their authentication information (GDPR Article 28, section 3, letter c).
- To prevent unauthorized access to systems and applications (GDPR Article 28, section 3, letter c).

Control Activity	Test performed by BDO	Result of test
<b>Management of secret authentication information of users</b>  <i>Got Ethics</i> <ul style="list-style-type: none"> <li>• Each user is responsible of managing own passwords.</li> <li>• Passwords to networks and services are managed by a special employee using an encrypted password manager tool.</li> </ul> <i>The whistleblower system</i> <ul style="list-style-type: none"> <li>• Temporary passwords for administrator user accounts are time limited and must be changed at the first login.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that each user is responsible for managing own passwords and that passwords to networks and services are managed by the "Access Granting Group" using an encrypted password manager tool.</p> <p>We have inspected "Code of Good Information Security Behavior" and observed the Processor's password policy length, complexity, and 2-factor authentication.</p> <p>We have observed configuration and, by testing, that temporary administrator user accounts in the whistleblower system are time limited and must be changed at the first login.</p>	No deviations identified.
<b>Review of user access rights</b>  <i>Got Ethics</i> <ul style="list-style-type: none"> <li>• The employees access rights are reviewed 4 times annually to ensure that all changes/revocations have been registered correctly.</li> </ul> <i>The whistleblower system</i> <ul style="list-style-type: none"> <li>• The responsibility for periodic review of the administrator user's access rights lies with the customers.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have received documentation for the recent periodic review done by the IT Security Committee at 3 April 2018.</p> <p>We were informed that it is the customer's responsibility to review the administrator access in the whistleblower system.</p>	No deviations identified.
<b>Removal or adjustment of access rights</b>  <i>Got Ethics</i> <ul style="list-style-type: none"> <li>• Procedures have been implemented to ensure that access rights are revoked or changed when employees leave the organization, or their job contents change.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have inspected the documentation for revocation of access to IT systems for the recent employee who left the Processor on 31 January 2018.</p>	No deviations identified.



## A.9: Access Control

### Control Objective

- To restrict access to information and information processing facilities (GDPR Article 28, section 3, letter c).
- To ensure access for authorized users and prevent unauthorized access to systems and services (GDPR Article 28, section 3, letter c).
- To make users responsible for securing their authentication information (GDPR Article 28, section 3, letter c).
- To prevent unauthorized access to systems and applications (GDPR Article 28, section 3, letter c).

Control Activity	Test performed by BDO	Result of test
<i>The whistleblower system</i> <ul style="list-style-type: none"> <li>• The responsibility for changing/revoking access rights when employees leave the organization, or their job contents change lies with the customers.</li> </ul>	We were informed that it is the customer's responsibility to change/revoke access rights when employees leave the organization or their job contents change.	
<b>Use of secret authentication information</b> <ul style="list-style-type: none"> <li>• Guidelines for use of secret authentication information is implemented in the code of good information security behavior that have been signed by all employees.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that "Code of Good Information Security Behavior" contains acceptable use of assets policy and that all employees have signed this document in 2018.</p>	No deviations identified.
<b>Information access restriction</b> <p><i>Got Ethics</i></p> <ul style="list-style-type: none"> <li>• The employees only have access to the networks, servers and services that are required for them to fulfil their jobs (need to know principle).</li> </ul> <p><i>The whistleblower system</i></p> <ul style="list-style-type: none"> <li>• The administrator user accounts can be configured individually to only grant access to the specific system functionalities that are required in order to fulfil their jobs.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Non-disclosure Undertaking".</p> <p>We have observed that the Processor has implemented different roles and accesses to the IT infrastructure and systems and the employees have only the access they need to fulfil their job.</p> <p>We have for the Whistleblower system observed that the administrator user accounts can be configured individually to only grant access to the specific system functionalities that are required in order to fulfil their jobs.</p>	No deviations identified.
<b>Secure log-on procedures</b> <p><i>Got Ethics</i></p> <ul style="list-style-type: none"> <li>• Guidelines for secure login have been implemented in the code of good information security behavior that have been signed by all employees.</li> <li>• Logging of actions performed in production environments.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Non-disclosure Undertaking".</p> <p>We have observed that "Code of Good Information Security Behavior" contains guidelines for secure login and that all employees have signed this document in 2018.</p> <p>We have observed that logging of actions is performed in the production environment.</p>	No deviations identified.

## A.9: Access Control

### Control Objective

- To restrict access to information and information processing facilities (GDPR Article 28, section 3, letter c).
- To ensure access for authorized users and prevent unauthorized access to systems and services (GDPR Article 28, section 3, letter c).
- To make users responsible for securing their authentication information (GDPR Article 28, section 3, letter c).
- To prevent unauthorized access to systems and applications (GDPR Article 28, section 3, letter c).

Control Activity	Test performed by BDO	Result of test
<p><i>The whistleblower system</i></p> <ul style="list-style-type: none"> <li>• The administrator user accounts can be configured individually to only grant access to the specific system functionalities that are required in order to fulfil their jobs.</li> <li>• Logging of failed login attempts.</li> <li>• Configurable brute force protection.</li> <li>• Each administrator user can see the login history.</li> <li>• Passwords are shown as dots on login screen.</li> <li>• Possibility of 2 factor authentication (add-on product).</li> <li>• Transmission of credentials are SSL encrypted.</li> <li>• Automatic session timeout.</li> </ul>	<p>We have for the Whistleblower system observed:</p> <ul style="list-style-type: none"> <li>• That the administrator user accounts can be configured individually to only grant access to the specific system functionalities that are required in order to fulfil their jobs.</li> <li>• Failed login attempts are logged.</li> <li>• Configuration for brute force protection.</li> <li>• That each administrator user can see the login history.</li> <li>• Passwords are shown as dots on login screen.</li> <li>• That it is possible for 2-factor authentication if the customer wants it (add-on product).</li> <li>• That transmission and credentials are SSL encrypted.</li> <li>• Automatic session timeout.</li> </ul>	
<p><b>Password management system</b></p> <p><i>Got Ethics</i></p> <ul style="list-style-type: none"> <li>• Guidelines for using secure passwords been implemented in the code of good information security behavior that have been signed by all employees.</li> </ul> <p><i>The whistleblower system</i></p> <ul style="list-style-type: none"> <li>• Configurable password policy (complexity requirements).</li> <li>• Configurable password mandatory change cycle.</li> <li>• Administrator users can change their passwords at any time.</li> <li>• The password must be changed at first login.</li> <li>• Passwords are stored as salted hash values.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Non-disclosure Undertaking".</p> <p>We have observed that "Code of Good Information Security Behavior" contains guidelines for using secure passwords and that all employees have signed this document in 2018.</p> <p>We have for the Whistleblower system observed the following:</p> <ul style="list-style-type: none"> <li>• Configurable password policy (complexity).</li> <li>• Configurable password mandatory change cycle.</li> <li>• Administrator users can change their passwords at any time.</li> <li>• The password must be changed at first login.</li> <li>• Passwords are stored as salted hash values.</li> </ul>	No deviations identified.
<p><b>Use of privileged utility programs</b></p> <ul style="list-style-type: none"> <li>• The use and number of users with privileged system access to the production environment is reduced to the extent possible.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Non-disclosure Undertaking".</p>	No deviations identified.

**A.9: Access Control****Control Objective**

- To restrict access to information and information processing facilities (GDPR Article 28, section 3, letter c).
- To ensure access for authorized users and prevent unauthorized access to systems and services (GDPR Article 28, section 3, letter c).
- To make users responsible for securing their authentication information (GDPR Article 28, section 3, letter c).
- To prevent unauthorized access to systems and applications (GDPR Article 28, section 3, letter c).

Control Activity	Test performed by BDO	Result of test
<ul style="list-style-type: none"> <li>• Logging of actions performed by users with privileged system access to the production environment is implemented to the extent possible.</li> </ul>	<p>We have observed that it is only the "Production Access Group" who has admin rights in the production environment.</p> <p>We have observed that logging of actions is performed in the production environment.</p>	
<b>Access control to program source code</b> <ul style="list-style-type: none"> <li>• Source code is kept separate from the production environment.</li> <li>• Only a small number of employees have access to the source code versioning server.</li> <li>• Logging is enabled on the source code versioning server.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Non-disclosure Undertaking".</p> <p>We have observed that:</p> <ul style="list-style-type: none"> <li>• Source code is kept separate from the production environment.</li> <li>• It is developers who have access to the source code versioning server.</li> <li>• Logging is enabled on the source code versioning server.</li> </ul>	No deviations identified.

**A.10: Cryptography****Control Objective**

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

Control Activity	Test performed by BDO	Result of test
<b>Policy on the use of cryptographic controls</b> <ul style="list-style-type: none"> <li>A policy for use of cryptographic controls have been implemented.</li> <li>Passwords are stored as salted hash values.</li> <li>Encryption of personal data in transit.</li> <li>Encryption of personal data at rest.</li> <li>The encryption algorithms meet generally accepted standard requirements.</li> <li>Periodic assessment if the encryption algorithms comply with best practice.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls and "Information Security Policy".</p> <p>We have observed that:</p> <ul style="list-style-type: none"> <li>A policy for use of cryptographic controls is implemented by logon to the Whistleblower system and observed that the connection is SSL encrypted.</li> <li>Passwords are stored as salted hash values.</li> <li>Personal data in transit, data internal between servers, and at rest are encrypted.</li> <li>The encryption algorithms meet generally accepted standard requirement.</li> <li>There is a periodic assessment that the encryption algorithms comply with best practice - recent in March 2018.</li> </ul>	No deviations identified.
<b>Key management</b> <ul style="list-style-type: none"> <li>Unique encryption key for each customer.</li> <li>Encryption keys are kept by the customers.</li> <li>Got Ethics A/S does not have access to the private key and therefore cannot decrypt the customers' encrypted personal data.</li> <li>A procedure for management of compromised encryption keys have been implemented.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls and "Information Security Policy".</p> <p>We have observed that each customer has a unique encryption key.</p> <p>We have been informed that the encryption keys are kept by the customers when the Whistleblower system is set in production at the customer, then it is not possible the Processor to see the data. If the customers lose their encryption key, it is not possible for the Processor to help other than by making a new database with a new encryption key.</p> <p>We have observed that a procedure has been implemented for management of compromised encryption keys.</p>	No deviations identified.

## A.11: Physical and Environmental Security

### Control Objective

- To prevent unauthorized physical access to, and damage/disruption of the organization's information and information processing facilities (GDPR Article 28, section 3, letter c).
- To avoid loss, damage, theft or compromise of assets and disruptions in the organization.

Control Activity	Test performed by BDO	Result of test
<p><b>Physical security perimeter</b></p> <p><i>Got Ethics A/S</i></p> <ul style="list-style-type: none"> <li>No personal data is stored in Got Ethics A/S' offices, only in the hosting providers' data centers.</li> <li>Appropriate physical security perimeter measures implemented.</li> </ul> <p><i>Data centers</i></p> <ul style="list-style-type: none"> <li>Appropriate physical security perimeter measures implemented.</li> <li>The hosting partners prepare audit reports to document the security level.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have performed walk-through of local computers at the Processor's office together with employees and observed that no personal data are stored in the Processor's offices, but all data are stored on the servers in the datacenters in Germany (for the Danish and European customers) and in Canada (for Non-European customers).</p> <p>We have observed that the Processor has implemented appropriate physical security perimeter measures.</p> <p>We have received and inspected a statement from Nupark regarding physical and environment security. We assess that this is sufficient as there are no personal data in the Nupark server room and that the Processor has their own monitoring at the equipment and server rack.</p> <p>We have received and inspected the agreement between the Processor and Microsoft Azure in Germany.</p> <p>We have received and inspected a SOC 2 audit report from Microsoft Corporation - Microsoft Azure (Azure Germany) for the period 1 October 2016 - 30 September 2017 submitted by Deloitte &amp; Touche LLP dated 31 October 2017. The audit report is without qualification.</p> <p>We have received and inspected the agreement between the Processor and Cogeco Peer 1 in Canada.</p> <p>We have received and inspected a SOC 1 - SSAE 18 audit report from COGECO Peer 1 for the period 1 July 2016 to 30 June 2017 submitted by PriceWaterhouseCoopers LLP dated 10 November 2017. The audit report is without qualification.</p>	No deviations identified.

**A.11: Physical and Environmental Security****Control Objective**

- To prevent unauthorized physical access to, and damage/disruption of the organization's information and information processing facilities (GDPR Article 28, section 3, letter c).
- To avoid loss, damage, theft or compromise of assets and disruptions in the organization.

Control Activity	Test performed by BDO	Result of test
<b>Physical entry controls</b>  <i>Got Ethics A/S</i> <ul style="list-style-type: none"> <li>• No personal data is stored in Got Ethics A/S' offices, only in the hosting providers' data centers.</li> <li>• Appropriate entry control measures implemented.</li> </ul> <i>Data centers</i> <ul style="list-style-type: none"> <li>• Appropriate entry control measures implemented.</li> <li>• The hosting partners prepare audit reports to document the security level.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We refer to the section of "Physical security perimeter".</p>	No deviations identified.
<b>Securing office, room and facilities</b> <ul style="list-style-type: none"> <li>• No personal data is stored in Got Ethics A/S' offices.</li> <li>• Offices are locked when left unattended by key or keycard.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have performed walk-through of local computers at the Processor's office together with employees and observed that no personal data are stored in the Processor's offices, but all data are stored on the servers in the datacenters in Germany (for the Danish and European customers) and in Canada (for Non-European customers).</p> <p>We have inspected the physical security when we arrived at our visit to the office, and the employees observed us as guests and the Clean Desk Policy is observed.</p> <p>We have observed that the Processor's office premises in Copenhagen and in Holstebro (Nupark) are locked outside normal work hours and when the office is unattended.</p>	No deviations identified.
<b>Protecting against external and environmental threats</b> <ul style="list-style-type: none"> <li>• Appropriate measures have been implemented where sensitive/important data is stored.</li> </ul>	We refer to the section of "Physical security perimeter".	No deviations identified.
<b>Equipment siting and protection</b> <ul style="list-style-type: none"> <li>• Appropriate measures have been implemented where sensitive/important data is stored.</li> </ul>	We refer to the section of "Physical security perimeter".	No deviations identified.



## A.11: Physical and Environmental Security

### Control Objective

- To prevent unauthorized physical access to, and damage/disruption of the organization's information and information processing facilities (GDPR Article 28, section 3, letter c).
- To avoid loss, damage, theft or compromise of assets and disruptions in the organization.

Control Activity	Test performed by BDO	Result of test
<b>Supporting utilities</b> <ul style="list-style-type: none"> <li>The below measures are implemented in as well Got Ethics A/S' server room and in the data centers where the production servers are located: <ul style="list-style-type: none"> <li>Fire suppression system.</li> <li>HVAC Systems.</li> <li>UPS.</li> <li>Generators.</li> </ul> </li> </ul>	We refer to the section of "Physical security perimeter".	No deviations identified.
<b>Cabling security</b> <ul style="list-style-type: none"> <li>Cabling is performed according to industry standards.</li> </ul>	We refer to the section of "Physical security perimeter".	No deviations identified.
<b>Equipment maintenance</b> <ul style="list-style-type: none"> <li>A procedure has been implemented to ensure protection of personal data in case the equipment on which the data is stored, shall be maintained.</li> </ul>	We refer to the section of "Organisation of information security mobile devices and teleworking".	No deviations identified.
<b>Removal of assets</b> <ul style="list-style-type: none"> <li>A procedure has been implemented to ensure that removal of information assets from the offices are registered.</li> </ul>	We refer to the section of "Organisation of information security mobile devices and teleworking".	No deviations identified.
<b>Security of equipment and assets off-premises</b> <ul style="list-style-type: none"> <li>A procedure has been implemented to ensure securing of assets removed from the office.</li> </ul>	We refer to the section of "Organisation of information security mobile devices and teleworking".	No deviations identified.
<b>Secure disposal or re-use of equipment</b> <ul style="list-style-type: none"> <li>A procedure has been implemented to ensure deletion of sensitive data in case the media on which the information is stored shall be disposed of or reused for other purposes.</li> </ul>	We refer to the section of "Physical security perimeter".	No deviations identified.
<b>Unattended user equipment</b> <ul style="list-style-type: none"> <li>A locked computer policy has been implemented.</li> </ul>	See the above area: Organisation of information security mobile devices and teleworking.	No deviations identified.
<b>Clear desk and clear screen policy</b> <ul style="list-style-type: none"> <li>A clear desk and clear screen policy has been implemented.</li> </ul>	See the above area: Physical and environmental security	No deviations identified.

## A.12: Operations Security

### Control Objective

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

Control Activity	Test performed by BDO	Result of test
<b>Documented operating procedures</b> <ul style="list-style-type: none"> <li>• The operating procedures have been formalized and communicated to the relevant employees.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that the Processor has a formalized operating procedure and by interview observed that it is communicated to the relevant employees.</p>	No deviations identified.
<b>Change management</b> <ul style="list-style-type: none"> <li>• Change management procedures have been implemented to ensure that all changes are documented and tested thoroughly before migrated to the production environment.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that:</p> <ul style="list-style-type: none"> <li>• The Processor has an implemented Change Management procedure.</li> <li>• The changes are documented in the project management system where you can see who has requested the change, the assigned developer, tester and approver for migration to the production environment.</li> <li>• Each change is documented in the version control system</li> <li>• After each build migrated to the production environment, the Processor runs a penetration test.</li> <li>• The result are stored in a folder for each build.</li> </ul> <p>We have observed that after each build that contains substantial changes, a newsletter is sent to the customers. We have received and inspected the newsletters from June and December 2017 with system changes and migrating to Microsoft Azure.</p>	No deviations identified.

**A.12: Operations Security****Control Objective**

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

Control Activity	Test performed by BDO	Result of test
<b>Capacity management</b> <ul style="list-style-type: none"> <li>• The ongoing capacity consumption, availability, patch management status, SSL certificate expiry and backup functionality in the production environment is being monitored by a technical solution that sends alerts if failures are encountered.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that the on-going capacity, availability, patch management status, SSL certificate expiry and backups in the production environment is being monitored by a diagnostic system.</p> <p>We have observed that an incident is raised in the diagnostic system; the diagnostic system sends a notification to the incident management system.</p>	No deviations identified.
<b>Separation of development, testing and operational environments</b> <ul style="list-style-type: none"> <li>• Development, testing and operation of production system has been separated to different environments to the extent possible.</li> <li>• Logging of actions performed in the production environment.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that the Processor has separated the development, testing and operation of production system in different environments to the extent possible and that logging of actions are performed in the production environment.</p>	No deviations identified.
<b>Controls against malware</b> <ul style="list-style-type: none"> <li>• Procedures have been implemented to ensure installation of anti-virus and anti-malware on work computers.</li> <li>• Files uploaded to the whistleblower servers in the production environment are cleaned from malware by an internally developed tool "File Detox", which creates a cleaned version of the file. However, the original file is saved in case it is needed for forensic purposes.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that the Processor has a procedure to ensure installation of anti-virus and anti-malware on work computers.</p>	No deviations identified.

## A.12: Operations Security

### Control Objective

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

Control Activity	Test performed by BDO	Result of test
	<p>We have observed the configuration of Anti-virus Windows Defender and observed that it is configured in real-time to ensure that it is updated with the recent version. We have observed an employee's workstation and that it was up-to-date.</p> <p>We have observed that files uploaded to the Whistleblower system in the production environment are cleaned from malware by a file detox system, which makes a cleaned version of the file, but keeps the original file saved as well, so the customer has access to both files. We have observed the configuration together with the administrator of the production environment.</p>	
<p><b>Information backup</b></p> <p><i>Got Ethics A/S</i></p> <ul style="list-style-type: none"> <li>• Internal files and source code is backed up.</li> <li>• Restore tests are performed with appropriate intervals to ensure the validity of the backup sets.</li> </ul> <p><i>Whistleblower System</i></p> <ul style="list-style-type: none"> <li>• Daily backups are made every day. The daily backup is kept for 30 days.</li> <li>• At the end of each calendar month a monthly backup is made. The monthly backup is kept for 5 years whereupon it is deleted.</li> <li>• Restore tests are performed with appropriate intervals to ensure the validity of the backup sets.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>As to Information backup, we have been informed and observed that:</p> <ul style="list-style-type: none"> <li>• The internal files and source code are backed up.</li> <li>• Restore test is done at appropriate intervals to ensure the validity of the backup - latest restore test of backup of source code is done 9 March 2018.</li> </ul> <p>As to Whistleblower System, we have been informed and observed that:</p> <ul style="list-style-type: none"> <li>• Daily backups are made for the production systems and are kept for 30 days.</li> <li>• A monthly backup is made which is kept for 5 years.</li> <li>• Restore test is done with appropriate intervals to ensure the validity of the backup - latest restore test of backup of production environment is done 13 March 2018.</li> </ul>	No deviations identified.

## A.12: Operations Security

### Control Objective

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

Control Activity	Test performed by BDO	Result of test
	We have together with the administrator of the production environment made a walk-through of the configuration of backup for internal development environment and for the production environment - dashboards etc.	
<b>Event logging</b> <ul style="list-style-type: none"> <li>• The Windows Server and SQL server logs on the whistleblower system's production servers are enabled.</li> <li>• The significant actions performed by the administrator users created in the whistleblower system are logged.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have by walk-through of the logging and monitoring tools observed the procedures and controls for logging and monitoring.</p> <p>We have observed that the Windows and SQL server logs on the Whistleblower systems are enabled.</p> <p>We have observed that significant changes performed by the administrator user in the Whistleblower system are logged in Active Directory Event log and in Microsoft Azure.</p>	No deviations identified.
<b>Protection of log information</b> <ul style="list-style-type: none"> <li>• The audit log in the whistleblower system, the Windows Server log and the SQL Server log are backed up.</li> <li>• The disk space consumption is monitored to ensure that log information is not lost due to running out of disk space.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that logs for the Whistleblower system, Window Server logs and the SQL server logs are backed up.</p> <p>We have observed that space consumption is monitored to ensure that log information is not lost due to running out of disk space.</p>	No deviations identified.

**A.12: Operations Security****Control Objective**

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

Control Activity	Test performed by BDO	Result of test
<b>Administrator and operator logs</b> <ul style="list-style-type: none"> <li>• The windows and database server logs on the servers in the production environment are backed up.</li> <li>• All actions performed by the employees who is performing the work on the servers in the production environment are logged and the logs cannot be accessed by this employee as well as the logging functionality cannot be disabled by this employee.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that Windows and database server logs on the server in the production environment are backup up.</p> <p>We have observed that action performed by employees are logged and that they cannot access, change or delete the logs and they do not have access to disable the logging.</p>	No deviations identified.
<b>Clock synchronization</b> <ul style="list-style-type: none"> <li>• Where relevant, systems/services are synchronized with a NTP time server.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have together with the "Infrastructure Group" and the "Production Environment Access Group" made a walk-through of the operating system.</p> <p>We have observed that updating the systems with operational software is done Clock synchronized with NTP timeserver, if possible.</p> <p>We have observed that the Processor is updating the systems (NTP time) in windows between 23:00 and 7:00, so it will be the most convenient time for the customers.</p>	No deviations identified.
<b>Installation of software on operational systems</b> <ul style="list-style-type: none"> <li>• Installation of software on servers in the production environment is restricted to specific employees.</li> <li>• The main software (Windows and database server) used on the servers in the production environment must always be supported by the manufacturer.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p>	No deviations identified.



## A.12: Operations Security

### Control Objective

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

Control Activity	Test performed by BDO	Result of test
	<p>We have observed that it is only the "Production Environment Access Group" who has access to maintain the production environment.</p> <p>We have observed that the main software is standard software that is supported by the manufacturers.</p>	
<b>Management of technical vulnerabilities</b> <ul style="list-style-type: none"> <li>• Restriction on which software that is allowed installed on employees' work computers. The list is reviewed with appropriate intervals.</li> <li>• Requirement to install anti-virus and anti-malware programs and keep the definition databases updated.</li> <li>• Automatic patch management of the servers in the production environment.</li> <li>• Anti-virus and anti-malware software installed on the servers in the production environment.</li> <li>• Periodic security assessment of the plugins used by the whistleblower system.</li> <li>• Periodic review to ensure that the plugins used by the whistleblower system are updated.</li> <li>• Procedure implemented to ensure that new threats are identified, and any security implications are remedied in due time.</li> <li>• Periodic review if the implemented security measures in the whistleblower system are still effective and meets relevant standards.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that:</p> <ul style="list-style-type: none"> <li>• In the Code of Good Information Security Behavior is instruction and a "whitelist" for allowed software and all employees have signed this document.</li> <li>• The IT security group reviews the list of allowed software in the Code of Good Information Security Behavior 4 times a year.</li> <li>• The employees weekly make sure that the anti-virus and anti-malware programs are updated, we have observed that the diagnostic system is monitoring this as well and we have checked two employees' laptop.</li> <li>• There is automatic patch management of the servers in the production environment.</li> <li>• Anti-virus and anti-malware software are installed on servers in the production environment, we have observed the configuration together with the "Production Environment Access Group".</li> <li>• The "IT Security Committee" is assessing the plugins and have a periodic review to ensure that the plugins used by the Whistleblower system are updated minimum 4 times a year.</li> </ul>	No deviations identified.

**A.12: Operations Security****Control Objective**

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

Control Activity	Test performed by BDO	Result of test
	<ul style="list-style-type: none"> <li>• There is a procedure to ensure that new threats are identified and security implications are remedied in due time.</li> <li>• A periodic review is conducted of security measures in the Whistleblower system to ensure they are effective and meet relevant standards.</li> </ul>	
<b>Restrictions on software installation</b> <ul style="list-style-type: none"> <li>• Restriction on which software that is allowed installed on employees' work computers. The list is reviewed with appropriate intervals.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that the "IT security Committee" is assessing the software that it is allowed to install on employees' work computers and the list is reviewed at appropriate intervals and minimum 4 times a year.</p>	No deviations identified.
<b>Information systems audit controls</b> <ul style="list-style-type: none"> <li>• Procedures have been implemented to ensure that audit activities and monitoring are conducted in a way that reduce impact on performance of the production system as much as possible</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We were informed that the Processor's "IT Security Committee" is going through: The "Information Security Policy", access rights, encryption algorithms, restore tests, the list over allowed software, third party components on servers, whistleblower vulnerability, incidents and changes, the emergency procedure, technical compliance to their Information security policy and a review of the "Data Protection Impact Assessment" 4 times a year.</p> <p>We have observed that the Processor makes a penetration test after each build in production and that they monitor the production system 24/7/365.</p>	No deviations identified.

**A.13: Communications security****Control Objective**

- To ensure protection of network information and supportive information processing facilities (GDPR Article 28, section 3, letter c).
- To maintain information security when transferring internally in an organization and to an external entity (GDPR Article 28, section 3, letter c).

Control Activity	Test performed by BDO	Result of test
<b>Network controls</b> <ul style="list-style-type: none"> <li>• Appropriate measures have been implemented to secure the networks.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have together with the administrator of the production environment conducted walk-through of the networks (internal and production networks).</p> <p>We have together with the administrator of the production environment observed the configuration of the firewalls for:</p> <ul style="list-style-type: none"> <li>• Microsoft Azure in Germany.</li> <li>• The datacenters in Cogeco Montreal and Toronto</li> <li>• Nupark in Holstebro.</li> </ul> <p>We have together with the administrator of the production environment observed the network infrastructure.</p>	No deviations identified.
<b>Security of network services</b> <ul style="list-style-type: none"> <li>• The network services that the production environment depend on are monitored.</li> <li>• The network services that the production environment depend on have been assessed and found secure.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that the production environment is monitored by Microsoft Azure in Germany and by the Processor using the diagnostic system.</p> <p>We have observed the quarterly reviews by the "IT Security Committee" where they assess the security in the production environment.</p>	No deviations identified.
<b>Segregation in networks</b> <ul style="list-style-type: none"> <li>• The networks have been segregated so employees can access only those networks they are required to in order to be able to perform their duties.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed the segregation of duties in the network together with the administrator in the production environment and the administrator in the development and test environment.</p>	No deviations identified.

**A.13: Communications security****Control Objective**

- To ensure protection of network information and supportive information processing facilities (GDPR Article 28, section 3, letter c).
- To maintain information security when transferring internally in an organization and to an external entity (GDPR Article 28, section 3, letter c).

Control Activity	Test performed by BDO	Result of test
<b>Information transfer policies and procedures</b> <ul style="list-style-type: none"> <li>• Policies have been implemented to ensure protection of transfer of information.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Non-disclosure Undertaking".</p> <p>We have observed that a policy has been implemented to ensure protection of transfer of information.</p>	No deviations identified.
<b>Agreements on information transfer</b> <ul style="list-style-type: none"> <li>• Transfer of the encryption key to the customers are regulated in the service contract.</li> <li>• Procedures have been implemented to secure transfer of sensitive information.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Non-disclosure Undertaking".</p> <p>We have observed that the Processor has data processing agreements with the customers and that access to information is handled by encryption keys. When the customer's Whistleblower system is in production, it is only the customer who can see the data. We have tested access from the Processor to selected customers.</p> <p>We have observed that procedures are implemented to secure transfer of sensitive information.</p>	No deviations identified.
<b>Electronic messaging</b> <ul style="list-style-type: none"> <li>• Procedures have been implemented that restrict the use of electronic messaging to specific messaging software and ensure that sensitive data is transferred securely.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Non-disclosure Undertaking".</p> <p>We have observed that the Processor is using internal encryption keys to ensure that data are transferred securely.</p>	No deviations identified.
<b>Confidentiality or non-disclosure agreements</b> <ul style="list-style-type: none"> <li>• The employees are bound by non-disclosure undertakings.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Code of Good Information Security Behavior" and "Non-disclosure Undertaking".</p> <p>We have observed that all employees have signed the "Non-disclosure Undertaking" document.</p>	No deviations identified.

**A.14: System acquisition, development and maintenance****Control Objective**

- 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 Article 25).
- To ensure that information security is organized and implemented within the information systems development life cycle (GDPR Article 25).
- To ensure the protection of data used for testing (GDPR Article 25).

Control Activity	Test performed by BDO	Result of test
<b>Information security requirements analysis and specification</b> <ul style="list-style-type: none"> <li>• Procedures have been implemented to ensure that information security requirements are assessed when acquiring new systems or upgrading existing systems with information security implications.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have been informed that after implementing the procedure the Processor has not implemented new systems, so we have not been able to verify documentation for this procedure.</p> <p>We have observed that the "IT Security Committee" reviews systems before upgrading existing systems for information security implications and that the group reviews the important software etc. We refer to section "Operations security - Information systems audit considerations".</p>	<p>As the Processor has not implemented new information systems, we have not been able to verify the procedure for ensuring that information security requirements are assessed when acquiring new information systems.</p> <p>No deviations identified.</p>
<b>Securing applications services on public networks</b> <ul style="list-style-type: none"> <li>• Only secure application services on public networks are used regarding operations with information security impact.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have inspected the Inventory of Information Assets together with the "Infrastructure Group" and observed that the Processor only use secure application services on public networks.</p>	No deviations identified.
<b>Secure development policy</b> <ul style="list-style-type: none"> <li>• A secure development policy has been implemented.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that a secure development policy and change management procedure have been implemented. We have observed that each development project is documented in the project management system.</p>	No deviations identified.
<b>System change control procedures</b> <ul style="list-style-type: none"> <li>• Change management procedures have been implemented.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that all changes are documented in the version control system where you can see what have been changed, by whom and when, so it will be possible to roll back in case of bugs etc.</p>	No deviations identified.

**A.14: System acquisition, development and maintenance****Control Objective**

- 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 Article 25).
- To ensure that information security is organized and implemented within the information systems development life cycle (GDPR Article 25).
- To ensure the protection of data used for testing (GDPR Article 25).

Control Activity	Test performed by BDO	Result of test
<b>Technical review of applications after operating platform changes</b> <ul style="list-style-type: none"> <li>• Procedures have been implemented to ensure a technical review after operating platform changes.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that a procedure has been implemented for technical review after operating platform changes and the technical review is controlled and documented in the project management system. After each build release, a penetration test is done - recently for version 1.39.</p>	No deviations identified.
<b>Restrictions on changes to software packages</b> <ul style="list-style-type: none"> <li>• No changes are made in third party software packages.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that no changes are made in third party software packages. We have inspected the Inventory of Information Assets.</p>	No deviations identified.
<b>Secure system engineering principles</b> <ul style="list-style-type: none"> <li>• A policy for secure system engineering principles have been implemented and communicated to the relevant employees.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that a policy for secure system engineering principles is implemented and communicated to the relevant employees by interview of an employee.</p>	No deviations identified.
<b>Secure development environment</b> <ul style="list-style-type: none"> <li>• Confidential data is not used in the development and test environments.</li> <li>• Appropriate measures implemented to protect source code.</li> <li>• Source code versioning tool implemented.</li> <li>• Back up of source code.</li> <li>• Least privilege principle implemented.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed, that:</p> <ul style="list-style-type: none"> <li>• The Processor does not use confidential data in the development and test environments.</li> <li>• Appropriate measures are implemented to protect the source code.</li> <li>• A source code versioning tool is implemented.</li> </ul>	No deviations identified.



**A.14: System acquisition, development and maintenance****Control Objective**

- 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 Article 25).
- To ensure that information security is organized and implemented within the information systems development life cycle (GDPR Article 25).
- To ensure the protection of data used for testing (GDPR Article 25).

Control Activity	Test performed by BDO	Result of test
	<ul style="list-style-type: none"> <li>• The source code is backed up.</li> <li>• Least Privilege principle for the employees is implemented, we have seen the difference for Remote Desktop Access for a developer and for access to the production environment.</li> </ul>	
<b>System security testing</b> <ul style="list-style-type: none"> <li>• Before deploying a new version to the production environment, system changes are tested thoroughly.</li> <li>• After each deployment of a new build in the production environment, an internal penetration test is conducted and documented.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that before deploying of a new version (build) to the production environment, the system changes are tested thoroughly first by the developer. Then the developer commits the changes to the version control system and updates the status in the project management system. Then the change is committed to the test server and the tester(s). After approval, the tester registers the approval in the project management system.</p>	No deviations identified.
<b>System acceptance testing</b> <ul style="list-style-type: none"> <li>• Before deploying a new build to the production environment, a system acceptance test is conducted and documented.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that:</p> <ul style="list-style-type: none"> <li>• When a tester has approved the change, then the next step is to perform an acceptance test. If the acceptance test is ok, the test is stored in the build folder.</li> <li>• Before the build is ready to deploy in the production environment, the change must be reviewed and approved by a reviewing developer.</li> </ul> <p>We have observed that after deployment of a new build in the production environment an internal penetration test is conducted and documented in the recent builds 1.39 and 1.39.1.</p>	No deviations identified.

**A.14: System acquisition, development and maintenance****Control Objective**

- 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 Article 25).
- To ensure that information security is organized and implemented within the information systems development life cycle (GDPR Article 25).
- To ensure the protection of data used for testing (GDPR Article 25).

Control Activity	Test performed by BDO	Result of test
<b>Protection of test data</b> <ul style="list-style-type: none"> <li>• No sensitive data (including data from the production environment) are used in the test environment, hence no special requirements to protect the data. However, only employees required to access the test environment have access to test data.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that no sensitive data are used in the test environment, and that it is only employees requiring access that have access to the test environment, Remote Desktop Access manages access to the test environment.</p>	No deviations identified.

A.15: Supplier relationships		
<b>Control Objective</b> <ul style="list-style-type: none"> <li>To ensure protection of the organization's assets that suppliers have access to (GDPR Article 28, section 2, Article 28, section 3, letter d, Article 28, section 4).</li> <li>To maintain an agreed level of information security and delivery of services under the supplier agreements (GDPR Article 28, section 2, Article 28, section 3, letter d, Article 28, section 4).</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Information security policy for supplier relationships</b> <ul style="list-style-type: none"> <li>An information security policy for supplier services have been implemented.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that the Processor has an implemented security policy for supplier services.</p>	No deviations identified.
<b>Addressing security within supplier agreements</b> <ul style="list-style-type: none"> <li>Policy implemented to ensure information security assessments of new suppliers where information security implications are conducted and the implications are handled in the contract.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that the Processor has an implemented security assessment policy for new suppliers where information security implications are conducted and the implications are handled in the contract.</p> <p>We have inspected the agreement between the Processor and the following hosting providers: Cogeco Peer 1, Microsoft Azure, ComText A/S, and Supertel A/S.</p>	No deviations identified.
<b>Information and communication technology supply chain</b> <ul style="list-style-type: none"> <li>The audit reports from the hosting providers have been reviewed.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have inspected that the Processor has reviewed the audit reports from the above-mentioned hosting providers.</p>	No deviations identified.
<b>Monitoring and review of supplier services</b> <ul style="list-style-type: none"> <li>Review of audit reports of suppliers that supply services with information security implications.</li> <li>Monitoring of relevant delivered services.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have inspected that the Processor has reviewed the audit report from the hosting providers.</p>	No deviations identified.

**A.15: Supplier relationships****Control Objective**

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

Control Activity	Test performed by BDO	Result of test
	<p>We have been informed that following suppliers are allowed access to the Processor's IT systems and infrastructure regarding the Whistleblower system:</p> <ul style="list-style-type: none"> <li>• Microsoft Azure Germany - hosting whistleblower system in Europe (data encrypted).</li> <li>• Cogeco Peer 1 - hosting whistleblower system in Canada (data encrypted).</li> <li>• ComText A/S - provider of translation services.</li> </ul> <p>We have observed the Processor's monitoring of delivered services in the diagnostic system. Further we have observed that a loud alert alarm informs the employees if there is a service they have to take care of.</p>	
<b>Managing changes to supplier services</b> <ul style="list-style-type: none"> <li>• Policy implemented to ensure information security assessments are conducted when changes are made in supplier contracts with suppliers with information security implications and any implications are handled in the contract.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that the Processor has implemented a policy to ensure information security assessment are conducted when changes are made in supplier contracts with suppliers with Information security implications and any implications are handled in the contract.</p> <p>We have inspected the agreements with addendums between the suppliers and observed that they have non-disclosure agreements in place.</p>	No deviations identified.

**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 Article 33, section 2).

Control Activity	Test performed by BDO	Result of test
<b>Responsibilities and procedures</b> <ul style="list-style-type: none"> <li>Procedures have been implemented to ensure fast, efficient handling of information security incidents.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that the Processor has an implemented a procedure to handle information security incidents.</p>	No deviations identified.
<b>Reporting information security events</b> <ul style="list-style-type: none"> <li>Guidelines to reporting information security incidents have been implemented and communicated to the employees.</li> <li>It is part of the standards data processing agreement that customers shall inform Got Ethics A/S in case they suspect an information security incident has occurred.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that:</p> <ul style="list-style-type: none"> <li>In "Code of Good information Security Behavior" is a guideline for reporting information security incidents; we have observed that all employees have signed this document.</li> <li>It is a part of the standard data processing agreement with the customers that the customers shall inform the Processor if any suspect information security incidents occur.</li> </ul>	No deviations identified.
<b>Reporting information security weaknesses</b> <ul style="list-style-type: none"> <li>Guidelines to reporting information weaknesses have been implemented and communicated to the employees.</li> <li>It is part of the standards data processing agreement that customers shall inform Got Ethics A/S in case they suspect an information security weakness.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that:</p> <ul style="list-style-type: none"> <li>In "Code of Good information Security Behavior" is a guideline for reporting information security weaknesses; we have observed that all employees has signed this document.</li> <li>It is a part of the standard data processing agreement with the customers that the customers shall inform the Processor if any suspect information security weaknesses occur.</li> </ul>	No deviations identified.

A.16: Information security incident management		
<b>Control Objective</b> <ul style="list-style-type: none"> <li>To ensure a uniform and effective method of managing information security breaches, including communication on security incidents and weaknesses (GDPR Article 33, section 2).</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Assessment of and decision on information security events</b> <ul style="list-style-type: none"> <li>Procedures have been implemented to ensure that security incidents are assessed, including an evaluation of whether the incident can be categorized as a security breach.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that the Processor has a procedure to ensure that security incidents will be assessed, evaluated and categorized as well as responded to, learning from and collection of evidence but we cannot verify that it is implemented, as there have been no security incidents.</p>	<p>As there have not been any security incidents, we are not able to verify that the procedure for handling security incidents is implemented.</p> <p>No deviations identified.</p>
<b>Response to information security incidents</b> <ul style="list-style-type: none"> <li>Procedures have been implemented to ensure that information security incidents are responded to.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that In "Code of Good information Security Behavior" is a guideline for reporting information security incidents and weaknesses; we have observed that all employees have signed this document.</p>	No deviations identified.
<b>Learning from information security incidents</b> <ul style="list-style-type: none"> <li>It is assessed if new measures need to be implemented to avoid future information security incidents.</li> <li>Information security incidents are registered.</li> <li>The information security incident registry is reviewed with appropriate intervals to assess if any patterns can be identified.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that the Processor has implemented a procedure to handle information security incidents.</p>	No deviations identified.
<b>Collection of evidence</b> <ul style="list-style-type: none"> <li>Procedures have been implemented to ensure appropriate collection of evidence in connection with occurred information security incidents, to ensure that the evidence is stored appropriately (and backed up if relevant) taking into consideration the classification of the information, and to ensure that the evidence cannot be tampered with.</li> <li>Procedures have been implemented to ensure that the Processor notify the customers without undue delay after becoming aware of a personal data breach.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that procedures are implemented to ensure appropriate collection of evidence in connection with occurred information security incidents, to ensure that the evidence is stored appropriately (and backed up if relevant) taking into consideration the classification of the information, and to ensure that the evidence cannot be tampered with.</p>	<p>As there have not been any security incidents, we are not able to verify that the procedure for handling security incidents is implemented.</p> <p>No deviations identified.</p>

**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 Article 33, section 2).*

Control Activity	Test performed by BDO	Result of test
	<p>We have observed that procedures have been implemented to ensure that the Processor notify the customers without undue delay after becoming aware of a personal data breach.</p> <p>We have observed that the Processor has a procedure to ensure that security incidents will be assessed, evaluated and categorized as well as responded to, learning from and collection of evidence but we cannot verify that it is implemented, as there have been no security incidents.</p>	



**A.17: Information security aspects of business continuity management****Control Objective**

- To ensure that information security continuity is rooted in the organization's management systems for emergency and re-establishment (GDPR Article 28, section 3, letter c).
- To ensure accessibility of information processing facilities (GDPR Article 28, section 3, letter c).

Control Activity	Test performed by BDO	Result of test
<b>Planning information security continuity</b> <ul style="list-style-type: none"> <li>• The requirements to ensure business continuity and operating continuity have been identified.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that the Processor has identified the requirements to ensure business continuity and operating continuity</p>	No deviations identified.
<b>Implementing information security continuity</b> <ul style="list-style-type: none"> <li>• Procedures have been implemented to ensure the business continuity and operating continuity of the whistleblower systems.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that the Processor has implemented procedures to ensure the business continuity and operating continuity of the Whistleblower systems by using redundancy sites for European Customers at Microsoft Azure in Germany. The servers at the 2 sites are in real time, so if the Whistleblower system fails in 1 site, the other will automatically take over. A message is sent to the Processor's technical contact person.</p> <p>We have observed that the Processor has implemented procedures to ensure the business continuity and operating continuity of the Whistleblower systems by using redundancy sites for Customers in Canada at Cogeco. At Cogeco in Canada they have to restore a backup at the redundant site.</p>	No deviations identified.
<b>Verify, review and evaluate information security continuity</b> <ul style="list-style-type: none"> <li>• The information security continuity procedures shall be tested to the extent possible and verified with appropriate intervals.</li> <li>• The information security continuity procedures are reviewed with appropriate intervals and updated if found necessary.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy", "Business Continuity Risk Assessment" and "Data Protection Impact Assessment".</p> <p>We have been informed that "IT Security Committee" ongoing and at least 2 times a year verifies the information security continuity by.</p> <p>We have observed that the Processor is testing their Business Continuity and operating continuity and operating Continuity of the Whistleblower systems by ongoing restore tests.</p>	No deviations identified.

**A.17: Information security aspects of business continuity management****Control Objective**

- *To ensure that information security continuity is rooted in the organization's management systems for emergency and re-establishment (GDPR Article 28, section 3, letter c).*
- *To ensure accessibility of information processing facilities (GDPR Article 28, section 3, letter c).*

Control Activity	Test performed by BDO	Result of test
<b>Availability of information processing facilities</b> <ul style="list-style-type: none"><li>• Full redundancy has been implemented regarding the instance of the whistleblower system hosted in Germany.</li><li>• A recovery plan has been implemented for the instance of the whistleblower system hosted in Canada to ensure the fast system recovery in case of critical failure.</li></ul>	We refer to the section "Implementing information security continuity".	No deviations identified.

**A.18: Compliance****Control Objective**

- To prevent violations of statutory, regulatory or contractual requirements in relation to information security and other security requirements (GDPR Article 25, Article 28, section 2, Article 28, section 3, letter a, Article 28, section 3, letter e, Article 28, section 3, letter g, Article 28, section 3, letter h, Article 28, section 3, letter f, Article 28, section 10, Article 29, Article 32, section 4, Article 33, section 2).
- To ensure that information security is implemented and run in accordance with the organization's policies and procedures.

Control Activity	Test performed by BDO	Result of test
<b>Identification of applicable legislation and contractual requirements</b> <ul style="list-style-type: none"> <li>• The requirements to the implementation of appropriate technical and organizational measures according to GDPR are monitored. Any changes are implemented when necessary.</li> <li>• Data processing agreements have been entered with the hosting providers and other sub-processors.</li> <li>• Data processing agreements are being entered with the customers.</li> <li>• Non-disclosure undertakings have been signed by employees.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Non-disclosure Undertaking".</p> <p>We have observed that the Processor has prepared a list of the processes for their own internal processes and for the processes regarding the Whistleblower system.</p> <p>We have observed that the processes are implemented to comply with the EU General Data Protection Regulation (GDPR).</p> <p>We have observed that Data Processing Agreements have been entered with the hosting providers and other sub-processors.</p> <p>We have observed that Data Processing Agreements have been entered with the Processor's customers.</p> <p>We have observed that the Processor has made an inventory of customers and sub-processors and descriptions.</p> <p>We have observed that all employees have signed the "Non-disclosure Undertaking" document.</p>	No deviations identified.
<b>Intellectual property rights</b> <ul style="list-style-type: none"> <li>• Procedures have been implemented and communicated to ensure awareness regarding compliance with the license terms of the software installed by the employees.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that employees are informed about software they may install by a list in the "Code of Good Information Security Behavior" and that all employees have signed this document.</p>	No deviations identified.

**A.18: Compliance****Control Objective**

- To prevent violations of statutory, regulatory or contractual requirements in relation to information security and other security requirements (GDPR Article 25, Article 28, section 2, Article 28, section 3, letter a, Article 28, section 3, letter e, Article 28, section 3, letter g, Article 28, section 3, letter h, Article 28, section 3, letter f, Article 28, section 10, Article 29, Article 32, section 4, Article 33, section 2).
- To ensure that information security is implemented and run in accordance with the organization's policies and procedures.

Control Activity	Test performed by BDO	Result of test
<b>Protection of records</b> <ul style="list-style-type: none"> <li>Procedures have been implemented to ensure that registrations, logs information etc. is stored on suitable media (and backed up if relevant) to avoid destruction. The media chosen for each registration etc. and the implemented security measures shall be chosen depending on the classification of the information.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that the Processor has implemented procedures to ensure that registrations, logs information and media is chosen for each registration - depending on the classification of the information stored on suitable media and backup up to avoid destruction.</p>	No deviations identified.
<b>Privacy and protection of personally identifiable information</b> <ul style="list-style-type: none"> <li>Compliance with the EU General Data Protection Regulation (GDPR) is verified by obtaining an annual audit report from an independent auditor demonstrating compliance.</li> </ul>	We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".	No deviations identified.
<b>Regulation of cryptographic controls</b> <ul style="list-style-type: none"> <li>A policy on use of cryptographic controls have been implemented to ensure that sensitive data are being encrypted while in transit and at rest.</li> <li>The implemented encryption algorithms are reviewed with appropriate intervals to ensure they always meet general accepted standards and the requirements in GDPR.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that the Processor has implemented a policy for use of cryptographic controls in transit and at rest. We refer to section "Cryptographic - Cryptographic controls".</p>	No deviations identified.
<b>Independent review of information security</b> <ul style="list-style-type: none"> <li>Compliance with the EU General Data Protection Regulation (GDPR) is verified by obtaining an annual audit report from an independent auditor demonstrating compliance.</li> </ul>	We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".	No deviations identified.
<b>Compliance with security policies and standards</b> <ul style="list-style-type: none"> <li>Procedures are implemented and communicated to the employees to ensure registration of non-compliance with the Information security policy.</li> <li>Procedures implemented to ensure periodic review of occurrences of non-compliance with the Information Security Policy.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Code of Good Information Security Behavior".</p> <p>We have observed that the Processor has implemented procedures and communicated to the employees to ensure registration of non-compliance with the Information Security Policy by awareness meetings and that the employee has access to the document and signed the "Code of Good Information Security Behavior" once a year.</p>	No deviations identified.

**A.18: Compliance****Control Objective**

- To prevent violations of statutory, regulatory or contractual requirements in relation to information security and other security requirements (GDPR Article 25, Article 28, section 2, Article 28, section 3, letter a, Article 28, section 3, letter e, Article 28, section 3, letter g, Article 28, section 3, letter h, Article 28, section 3, letter f, Article 28, section 10, Article 29, Article 32, section 4, Article 33, section 2).
- To ensure that information security is implemented and run in accordance with the organization's policies and procedures.

Control Activity	Test performed by BDO	Result of test
	<p>We have observed that employees have signed the "Code of Good Information Security Behavior" in March 2018.</p> <p>We have observed that the "IT Security Committee" makes a periodic review 4 times a year to ensure occurrences of non-compliance with the Information Security Policy.</p>	
<b>Technical compliance review</b> <ul style="list-style-type: none"> <li>• Procedures implemented to ensure internal technical compliance reviews with appropriate intervals.</li> <li>• Internal penetration tests when new builds have been migrated to the production environment.</li> <li>• External penetration tests with appropriate intervals.</li> <li>• Annual audit report from an independent audit firm.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy".</p> <p>We have observed that the Technical employees have a procedure for ongoing assessment for compliance with the information security requirements - recently done 12 March 2018.</p> <p>We have observed that an internal penetration test is done when new builds are migrated to the production environment.</p> <p>We have observed that an external penetration test is done 10 May 2017 by HiSolutions AG.</p>	No deviations identified.

App Reporting Channel		
<b>Control Objective</b> <ul style="list-style-type: none"> <li>To ensure secure capture, storage and processing of incidents via the smartphone apps for iPhone and Android (GDPR Article 28, section 3, letter c).</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Implementation of appropriate security measures</b> <ul style="list-style-type: none"> <li>Incidents that have been sent to the case management system and are encrypted at rest in the same way as the incidents submitted from the web portal.</li> <li>Encryption of information in transit.</li> <li>Brute force protection to access the app.</li> <li>No information stored inside the app - only on the production server.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Inventory of Processing Operations".</p> <p>We have observed that the incident from the app reporting channel are submitted to the case management system and are encrypted in the same way as the incidents submitted from the web-portal on the server at Microsoft Azure in Germany or Cogeco in Canada.</p> <p>We have observed that the transfer of data between the client and the server is SSL encrypted. The data are encrypted while at rest in the database in the Whistleblower System and cannot be read/decrypted by the Processor.</p> <p>We have together with "Production Environment Access Group" observed the security for Brute force protection to access the App Reporting Channel.</p> <p>We have downloaded the app and used the app as a test.</p> <p>We have observed that no information is stored inside the app - only at the production servers in Germany or in Canada.</p>	No deviations identified.

Phone Hotline		
<b>Control Objective</b> <ul style="list-style-type: none"> <li>To ensure secure capture, storage and processing of incidents (voice messages) via the phone hotline solution (GDPR Article 28, section 3, letter c).</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Implementation of appropriate security measures</b> <ul style="list-style-type: none"> <li>Voice messages are recorded directly to the case management system and are encrypted in the same way as the incidents submitted from the web portal.</li> <li>Voice messages are obfuscated to hide the identity of the whistleblower.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Inventory of Processing Operations".</p> <p>We have observed that the Voice messages are recorded directly to the case management system and are encrypted in the same way as the incidents submitted from the web portal.</p> <p>We have observed that the voice messages are obfuscated to hide the identity of the whistleblower.</p> <p>We have reviewed the agreement between the Processor and Supertel A/S regarding hosting of Supertel SIP trunk inclusive Voice Traffic. The voice messages are handled at the Supertel Broad soft VoIP platform.</p> <p>We have received and inspected an ISAE 3402 type II Audit report from GlobalConnect A/S for the period 1 January to 31 December 2017 submitted by Ernst &amp; Young dated 13 February 2018. The audit report is without qualification.</p>	No deviations identified.



Translation Service		
<b>Control Objective</b> <ul style="list-style-type: none"> <li>To ensure that all information processed by translators are processed in a secure manner (GDPR Article 28, section 3, letter c).</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Implementation of appropriate security measures</b> <ul style="list-style-type: none"> <li>All processing is performed within Got Ethics A/S' IT infrastructure.</li> <li>Not possible to transfer information to outside Got Ethics' IT infrastructure.</li> <li>Information in transit is SSL encrypted.</li> <li>Information is encrypted while at rest.</li> <li>2-factor authentication with SMS code to access the translation web portal.</li> <li>Brute force protection to remote desktop connection (storing and translation of files).</li> <li>File deletion policy.</li> </ul>	<p>We have made inquiries of relevant personnel and inspected system descriptions of procedures, control objectives and controls, "Information Security Policy" and "Policy for use of Cryptographic Controls".</p> <p>We have inspected the agreement between the Processor and ComText A/S.</p> <p>We have tested the TranslationWeb functionalities by being created as a translator and assigned test translations of plain text and attachment and observed that:</p> <ul style="list-style-type: none"> <li>All the processing regarding the translation is performed within the Processor's IT infrastructure.</li> <li>It is not possible to transfer information to outside the Processor's IT infrastructure.</li> <li>The information is SSL encrypted in transit and while at rest.</li> <li>The Processor use 2-factor authentication with SMS code to access the translation Web Portal.</li> <li>There is Brute force protection to remote desktop connection in the process of translation.</li> <li>The translator has no access to the translated file after it is sent to client.</li> </ul> <p>We have together with the "Cryptographic Key management Group" observed the configuration.</p> <p>We have interviewed a developer regarding the TranslationWeb project - this project is documented as a case in the support system.</p>	No deviations identified.

## BDO Statsautoriseret revisionsaktieselskab

Havneholmen 29  
DK-1561 København V  
CVR-nr. 20 22 26 70

*BDO Statsautoriseret revisionsaktieselskab, en danskejet rådgivnings- og revisionsvirksomhed, er medlem af BDO International Limited - et UK-baseret selskab med begrænset hæftelse - og del af det internationale BDO netværk bestående af uafhængige medlemsfirmaer. BDO er varemærke for både BDO netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger godt 1.100 medarbejdere, mens det verdensomspændende BDO netværk har godt 64.000 medarbejdere i 154 lande.*

*Copyright - BDO Statsautoriseret revisionsaktieselskab, cvr.nr. 20 22 26 70.*