

*December 2022*

# Qampo ApS

ISAE 3000 TYPE 1 ASSURANCE REPORT

CVR 36430443

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



# Structure of the Assurance Report

## Chapter 1:

Letter of Representation.

## Chapter 2:

Independent Auditor's Assurance Report with description of the implemented controls.

## Chapter 3:

Description of the data processing environment.

## Chapter 4:

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

## Chapter 5:

Additional information from Qampo ApS.

# Letter of Representation

Qampo ApS processes personal data on behalf of Data Controllers according to signed Data Processor Agreement regarding Decision Science Solutions from Qampo ApS.

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

Qampo ApS hereby confirms that

(A) The accompanying description, Chapter 3, gives a true and fair description of Qampo ApS' control environment in relation to Decision Science Solutions, which has processed personal data covered by the General Data Protection Regulation as of 14<sup>th</sup> September 2022. The criteria for this assertion are that the following description:

- (i) Gives an account of how the controls were designed and implemented, including:
  - The types of services delivered, including the type of personal data processed
  - The processes in both IT and manual systems that are used to initiate, record, process and, if necessary, correct, erase and limit the processing of personal data
  - The processes utilized to secure that the performed data processing was conducted according to contract, directions or agreements with the customer i.e. the Data Controller
  - The processes securing that the persons authorized to process personal data have pledged themselves to secrecy or are subject to relevant statutory confidentiality
  - The processes securing that - at the Data Controller's discretion - all personal data are erased or returned to the Data Controller, when the data processing is finished, unless personal data must be stored according to law or regulation
  - The processes supporting the Data Controller's ability to report to the Supervisory Authority as well as inform the Data Subjects in the event of personal data security breaches
  - The processes ensuring appropriate technical and organizational security measures for processing personal data taking into consideration the risks connected to processing, in particular accidental or illegal actions causing destruction, loss, change, unauthorized forwarding of or access to personal data that is transmitted, stored or in other ways processed
  - Control procedures, which we assume - with reference to the limitations of the Decision Science Solutions - have been implemented by the Data Controllers and which, if necessary to fulfil the control objectives mentioned in the description, have been identified in the description
  - Other aspects of our control environment, risk assessment process, information system (including the accompanying work routines) and communication, control activities and monitoring controls relevant for processing of personal data
- (ii) Includes relevant information about changes in Qampo solution in relation to processing of personal data performed as of 14<sup>th</sup> September 2022
- (iii) Does not omit or misrepresent information relevant for the scope of the controls described, taking into consideration that the description has been prepared to meet the common needs of a broad range of customers and their auditors, and may not, therefore, include every aspect of

the control system that each individual customer may consider important in their own particular environment.

- (B) The controls related to the control objectives stated in the accompanying description were suitably designed as of 14<sup>th</sup> September 2022. The criteria for this assertion are that:
  - (i) The risks threatening the fulfilment of the control objectives mentioned in the description were identified
  - (ii) The identified controls would, if used as described, provide reasonable assurance that the risks in question would not prevent the fulfilment of the said control objectives
- (C) Appropriate technical and organizational security measures are established in order to honour the agreements with the Data Controllers, compliance with generally accepted data processor standards and relevant demands to Data Processors according to the General Data Processing Regulation.

Aarhus, 7<sup>th</sup> December 2022



**CEO, Ali Khatam**

Qampo ApS, Bredskifte Allé 11, DK-8210 Aarhus V, CVR number: 36430443

# Independent auditor's ISAE 3000 assurance report on information security and data protection measures in relation to Data Processor Agreement with Qampo ApS' customers

For Qampo ApS and relevant data controllers

## Scope

We have been engaged to report on Qampo ApS' description of their system Decision Science Solutions, see Chapter 3, in relation to Data Processor Agreement with Qampo ApS' customers as of 14<sup>th</sup> September 2022 and on the design of controls regarding the control objectives stated in the description.

We express our opinion with reasonable assurance.

## Qampo ApS' responsibility

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

## Beierholm's independence and quality management

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

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

## Auditor's responsibility

Our responsibility is to express an opinion, based on our procedures, on Qampo ApS's description and on the design and implementation of controls related to the control objectives stated in the said description.

We have conducted our engagement in accordance with ISAE 3000, Other assurance reports than audit or review of historical financial statements and additional requirements according to Danish audit regulation. The standard requires that we comply with ethical requirements and that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and whether the controls in all material aspects are appropriately designed.

An assurance engagement to report on the description, design and implementation of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of their system, and about the design of controls. The procedures selected depend on the judgement of the data processor's auditor, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or implemented.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified and described by Qampo ApS in Chapter 3. We have not performed procedures regarding the operating effectiveness of controls included in the description and express no opinion thereof.

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

### Limitations of controls at Qampo ApS

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

### Opinion

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

- a) The description fairly presents Qampo's Decision Science Solutions, such as this service was designed and implemented as of 14<sup>th</sup> September 2022 in all material respects; and
- b) The controls related to the control objectives stated in the description were in all material respects suitably designed as of 14<sup>th</sup> September 2022

### Description of tests of controls

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


### Intended users and purpose

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

Søborg, 9<sup>th</sup> December 2022

#### Beierholm

State Authorized Public Accountants  
CVR 32 89 54 68



Kim Larsen  
State-authorized Public Accountant



Palle Gregersen  
IT-auditor



# Description of control environment for the operation of Decision Science Solutions

## Introduction

The purpose of Qampo's processing of personal data on behalf of customers and partners is to calculate decision support plans and strategies on the basis of the data received.

These treatments go by a common name: **Decision Science**.

Qampo always processes data on behalf of customers and partners according to instructions. On the one hand, a main agreement has been entered into for each relationship, typically in the form of a license or project agreement that regulates the specific contractual matters. In the case of personally identifiable and / or business-critical data, an individual data processor agreement is also entered into, which describes Qampo's obligations during the specific processing.

The purpose of this description is to describe the technical and organizational measures that Qampo has implemented to ensure that the data processing at Qampo takes place in accordance with agreements entered into with customers and partners.

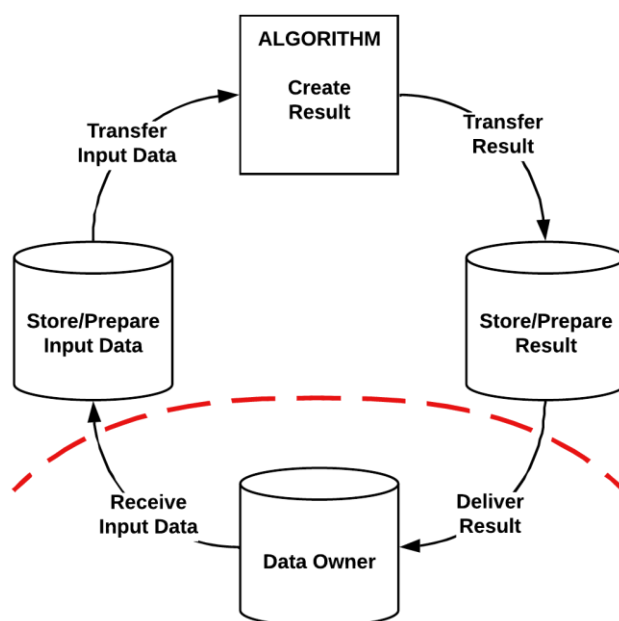
## The nature of data processing

Qampo develops Decision Science software that solves complex planning problems. Qampo's solutions are thus not targeted at specific industries, but rather industries with types of issues that are suitable for solving with Decision Science software. Examples of such types are planning tasks regarding staffing, distribution, services and situations where predictions can support a business process.

The core of any Decision Science solution is the algorithm that receives data from the customer as input, to calculate concrete action proposals in the form of plans, strategies, recommendations or actions.

Since Qampo does not make one specific product, this description is based on the general cycle by which data runs from the input data is delivered to Qampo, to the output and dissemination of the result.

## Description of data processing



### Receive input data:

Inputs to Qampo's algorithms must be handed over from the customer or partner to the Decision Science solution. This transfer can in practice take place with one or more of the following methods:

#### User interface / Manual entry:

In situations where inputs are required to be manually entered from the end user, a web-based user interface is used.

Qampo develops user interfaces according to the principle of data protection by design. Internal procedures ensure that data in Qampo's solutions comply with high standards of security.

In some situations, the user interface is owned by Qampo's customer or business partner, in such cases the data owner itself is responsible for the security of the processing in the user interface, and are thus outside the scope of this statement.

#### Rest API – (POST):

In cases when the inputs are prepared for loading directly into the algorithm in a specific agreed upon format, the Rest API (POST) is used.

This is the case when the algorithm is called from a user interface designed specifically for the purpose. Rest APIs always use HTTPS during transfer. Tokens are issued to ensure that the results cannot be released to unauthorized inquiries subsequently.

#### SFTP:

Are used when data must be pre-processed before the algorithm is called.

In such situations the data may be delivered in a somewhat more flexible or unstructured format. Prediction models ideally require the data that best describes the object being predicted. This may change over time, and thus require a more flexible handover of data. Qampo prepares data for the algorithm in a pre-process in such cases.

In proof of concepts when Qampo receive data from customers and a fixed data format has not yet been decided, data will also be transferred by SFTP.



## Store/prepare input data:

Qampo stores received input data for the following reasons:

- **Communication**  
In order to communicate results in a readable format after the algorithm has been run, certain elements of data needs to be stored. The output of the algorithm is typically not immediately readable, as it often consists mainly of numbers and ID's, and therefore requires a translation process to be made suitable for communication.
- **Support**  
If the algorithm gives an odd result, it is important to be able to recreate the result with the exact same inputs to adjust the algorithm. Without the possibility to do this, it is near impossible to explain the odd result, and to adjust the algorithm to prevent it from happening again.
- **Baseline**  
During improvements of algorithms, it is important to be able to compare results before and after committed changes, in order to verify whether the adjustments works as intended. For this, saved inputs from real queries are ideally used, to make sure further development is based on realistic and concrete situations.

Data is always stored according to instructions from the customer. The following types of storage can be used:

- **Database:**  
When data needs to be stored for the purpose of communicating the results later, a database is used. Preparation of data for the algorithm is also performed in the database. Such preparation might be: Translation of data into operational information, such as conversion of addresses into geographical coordinates, or district divisions. Or restructuring data into rules, such as transforming service codes into the competency requirements an employee must have in order to perform the service. Qampo's databases are physically located in the EU, and protected behind firewall. Access is granted only upon relevant needs by employees and in compliance with internally described procedures
- **REST API (POST):**  
Data sent via REST API in POST requests is stored in JSON format for support and baseline. This data is stored according to instructions from the customer, and is deleted accordingly.
- **SFTP:**  
Data transferred from the customer to the SFTP server managed by Qampo is stored according to instructions from the customer, and deleted accordingly. If data is stored on SFTP, it is for support and baseline reasons. Access to SFTP follows internal procedures regarding allocation of access.


## Transfer input data:

The inputs must be transferred from the stored state to the algorithm. Data is currently pseudonymized, hence additional data is required in order to attribute data back to individuals. In addition to the REST API (POST) described above, data can also be transferred to the algorithm via a database connection:

- **Database connection**  
Connections to Qampo's databases are always encrypted and via secure connection. In analysis processes or support cases where connection to databases may be required from home workplaces, this is achieved by VPN.

## Algorithm

The algorithm may be perceived as an advanced data processing. It receives an input in an agreed format, and returns a desired output as a result. Viewed this way, an algorithm is conceptually the same as any other method that calculates a result based on an input. No data is stored in the algorithm, and once the algorithm has returned its result, the algorithm is left unchanged, as it were prior to the call.



Algorithms are generally run on Qampo's servers, located in the EU and protected by firewalls. In proof of concepts, there may be cases where algorithms are run locally on employees' workstations. In both cases, the processing takes place according to instructions from the customer, and in compliance with Qampo's internal procedures for compliance with information security.

Algorithms can be developed according to 2 main principles:

- **Modelled algorithms:**  
Modeled algorithms are static. They are developed based on a specific problem the algorithm is designed to solve. New considerations such as rules or objectives require the algorithm to be maintained manually. Planning algorithms fall under this principle, the quality of a planning algorithm is inextricably linked to how well it supports the rules and considerations that it must comply to. A new consideration in the real world requires that the algorithm be adjusted accordingly, if the consideration has an influence on whether the proposed plans are good or not. Planning algorithms are designed to look for the best plans that meet all rules and considerations at the same time. This is done either by the algorithm simulating many valid plans to eventually select the best one. Alternatively, the algorithm can be designed to look for the best plan, so that when a plan is returned, it is guaranteed to be the best possible plan (Optimality).
- **Trained algorithms:**  
Trained algorithms are dynamic. They are developed in order to decode patterns and trends in data that can expose or explain the answer to a specific question (target). The starting point is to give the algorithm as much relevant data to process as possible, then the algorithm can find the patterns itself, and set the parameters in the final algorithm, this process is commonly known as "training" the algorithm. These algorithms can accept changes in input data as long as they are simply delivered in the same flexible format, they can therefore to some extent maintain themselves. Although they need to be closely monitored on an ongoing basis. Prediction models belong to this type of models. The algorithm can be said to indirectly carry elements of data in it, since the parameters are derived from input data, however, this information is never personally identifiable.

## Transfer result

The result of the algorithm now begins its journey back to the user.

- **Database connection**  
If the result is to be stored and communicated, it is returned to the database holding the previously collected master data via a database connection, the principles for which have already been described earlier.
- **Rest API – (GET):**  
When the inputs has been received by REST API - (POST) by the Algorithm, the result must be retrieved by REST API (GET). The enclosed token is compared with the token of the result, to make sure that it is not released to unauthorized parties.

## Store/prepare result

Results are saved for several reasons:

- **Operational implementation**  
Implementing the result at the customer site requires that it can be communicated and reported to the right stakeholders in the right format, in the time frame it takes to do so.
- **Measuring the impact**  
When results are released by the customer for compliance, it is important to be able to see the impact of the effort over time. This is often achieved through A/B testing or KPI reporting. To be able to perform this type of task, it is important that the result used, is saved as long as the reporting is relevant.
- **Support**  
As important it is to save input data in order to investigate inconveniences, saving proposed results are also necessary.

Having the option to adjust the algorithm, run it on the same input data, and finally compare the new result with the old result. Is a powerful way to maintain the algorithm

- **Baseline**

Especially in planning scenarios, a clear answer to whether one result is better than another is very rare. If a result is better at all conceivable measuring points than another result, the conclusion is of course obvious. But in the real world, goals are often contradictory, for example, cost and quality are often affected in opposite directions. Saving results to assess with human eyes whether one or the other proposed strategy is the most appropriate, is very valuable.

Results are always stored according to instructions from the customer.

Results are stored using the same methods as when storing input data: Database, SFTP and the raw result sent via REST API (GET) described earlier.

## Personal Data

Qampo potentially processes personal information from data controllers. Although Decision Science software takes on many different forms, there is still some consistent information that is typical when working with personal information.

- Identification – Relevant for communicating the results
  - Name
  - Contact Information
- Inputs – Relevant when describing the problem
  - Pseudomized ID (Employee ID, Citizen ID or similar)
  - Job title / Skills - Relevant in service planning
  - Address / Location – Relevant in route planning
  - Collective agreement / Planned working hours – Relevant for shift planning
  - Demand for services - Relevant for service planning
  - Complaints / Supports - Relevant for loyalty support
  - Subscription contents - Relevant for loyalty support

Categories of registered persons who may be covered by the data processing:

- Customers' employees - Those planned for
- Customers' customers / Stakeholders - Those who demand the service being planned

## Risk assessment

Risks are assessed and managed on an ongoing basis, and at least once a year. A risk assessment sheds light on the risks in relation to the data controllers' data.

Risk assessments are prepared with a focus on two scales:

- **Consequence** - How serious is it if a given incident occurs?
- **Likelihood** - How likely will the event occur?

Based on the analysis, QISB decides whether technical and / or organizational measures must be taken to address any identified challenges.



## Control measures

Qampo has implemented a number of control measures to ensure a uniformly high level of information security.

To ensure anchoring among Qampo employees, Information security is a fixed item on the agenda at Qampo's internal monthly meetings. In addition, the agreed frequency of controls is ensured via the calendars of those responsible. QISB is responsible for operation of the control measures, and thus ensures that all adopted reviews and controls are carried out in a timely and correct manner.

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

## CONTROL OBJECTIVE A:

Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.

Qampo ApS control procedures	Auditor's test of controls	Test findings
<p>A.1</p> <p>Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inspected the existence of formalized policies that ensures that the processing of personal data is carried out solely in accordance with instructions.</p> <p>Does the procedures contain the demand for at least manually revision?</p> <p>We have inspected that the policies are up to date.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>A.2</p> <p>The data processor only processes personal data stated in the instructions from the data controller.</p>	<p>We have – by sample test - inspected data processor agreements and ensured that the information security policy is compliant with the data processor agreements</p>	<p>We have not identified any essential deviations in our test.</p>
<p>A.3</p> <p>The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.</p>	<p>We have inspected the procedure for handling instructions from data controllers.</p> <p>We have inquired if there have been any instructions in the period that the processor has deemed unlawful.</p> <p>Inspected that the data controller is notified in cases where the processing of personal data is assessed to be in breach of the legislation.</p>	<p>We have not identified any essential deviations in our test.</p>

CONTROL OBJECTIVE B:

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

Qampo' control procedures	Auditor's test of controls	Test findings
<p>B.1</p> <p>Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Does formalized policies to ensure that personal data is required to be processed in accordance with data processing agreements exist?</p> <p>Are policies up to date ?</p> <p>Inspected by a sample of data processing agreements that the agreed security measures have been established.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>B.2</p> <p>The data processor has performed a risk assessment and based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller.</p>	<p>Inspected that there are formalized procedures that ensure that the data processor carries out a risk assessment in order to achieve adequate security.</p> <p>We have inspected that the risk assessment carried out has been updated and includes the current processing of personal data.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>B.3</p> <p>For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.</p>	<p>We have inquired about measures against malware</p> <p>We have inquired about the use of antivirus software, and we have inspected documentation of its use</p>	<p>We have not identified any essential deviations in our test.</p>
<p>B.4</p> <p>External access to systems and databases used in the processing of personal data takes place through a secured firewall.</p>	<p>We have inspected that external access to systems and databases used to process personal data is done only through a firewall.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>B.5</p> <p>Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.</p>	<p>We have requested whether internal networks are segmented to ensure limited access to systems and databases, used for the processing of personal data.</p> <p>We have inspected documentation to ensure proper segmentation</p>	<p>We have not identified any essential deviations in our test.</p>



<p>B.6</p> <p>Access to personal data is isolated to users with a work related need for such access.</p>	<p>We have inspected the existence of formalized procedures to restrict users' access to personal data</p> <p>We have – by sample test - inspected users, and – by sample test - ensured that users have work-related need for the access</p>	<p>We have not identified any essential deviations in our test.</p>
<p>B.7</p> <p>For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.</p>	<p>We have – by sample test - inspected capacity and logging monitoring</p>	<p>We have not identified any essential deviations in our test.</p>
<p>B.8</p> <p>Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.</p>	<p>We have inspected the existence of a formal policy on the use of encryption.</p> <p>We have – by sample test - inspected VPN-protocol and certificates, and by sample test ensured that transmission is done via secure connectivity</p>	<p>We have not identified any essential deviations in our test.</p>
<p>B.9</p> <p>Logging has been established in systems, databases, and networks. Logon data are protected against manipulation and technical errors and are reviewed regularly.</p>	<p>We have – by sample test - inspected the systems, and by sample test ensured that events are logged.</p> <p>We have – by sample test - inspected log storage and by sample test ensured that log files are protected.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>B.10</p> <p>Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.</p>	<p>We have inquired into whether the data processor is using personal data for testing</p>	<p>We have not identified any essential deviations in our test.</p>
<p>B.11</p> <p>The technical measures established are tested on a regular basis in vulnerability scans and penetration tests</p>	<p>We have – by sample test - inspected operational system monitoring, and by sample test ensured that the processor has carried out vulnerability scans</p>	<p>We have not identified any essential deviations in our test.</p>

<p>B.12</p> <p>Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.</p>	<p>We have inspected the existence of formalized procedures for handling changes to systems, databases, and networks, including handling relevant updates, patches, and security patches</p>	<p>We have not identified any essential deviations in our test.</p>
<p>B.13</p> <p>A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.</p>	<p>We have inspected the existence of formalized procedures for granting and disrupting users' access to systems and databases used for the processing of personal data.</p> <p>We have inspected the list of terminated employees on a random basis, and, on a random basis, we have determined that the terminated employees' admissions have been closed</p> <p>We have inspected that there is evidence of regular – at least annual – assessment and approval of assigned user access</p>	<p>We have not identified any essential deviations in our test.</p>
<p>B.14</p> <p>Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.</p>	<p>We have inspected the existence of formal policies for the application of two-factor authentication.</p> <p>We have – by sample test – inspected accesses, and we have by sample test ensured that this is done with two factor authentication</p>	<p>We have not identified any essential deviations in our test.</p>
<p>B.15</p> <p>Physical access safeguards have been established so as to only permit physical access by authorized persons to premises and data centres at which personal data are stored and processed.</p>	<p>We have inspected asset lists and ensured that keys have been identified.</p>	<p>We have not identified any essential deviations in our test.</p>

CONTROL OBJECTIVE C:

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

Qampos' control procedures	Auditor's test of controls	Test findings
<p>C.1</p> <p>Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.</p>	<p>We have inspected the information security policy and ensured that it has been updated during the period.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>C.2</p> <p>Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.</p>	<p>We have – by sample test - inspected data processor agreements and ensured that the information security policy is compliant with the data processor agreements.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>C.3</p> <p>The employees of the data processor are screened as part of the employment process.</p>	<p>We have inquired about the procedure for onboarding employees.</p> <p>We have – by sample test - inspected that recruitment procedures have been followed.</p> <p>We have inquired about screening of employees</p>	<p>We have not identified any essential deviations in our test.</p>
<p>C.4</p> <p>Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.</p>	<p>We have – by sample test - inquired about employment agreements, and we have inspected that a confidentiality agreement is included.</p> <p>We have – by sample test - inspected notice of introduction meetings, and we have ensured that new employees are being introduced to information security.</p>	<p>We have not identified any essential deviations in our test.</p>

<p>C.5</p> <p>For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.</p>	<p>We have inquired about procedures that ensures, that terminated employees' access rights are deactivated or removed upon resignation, and that assets such as keycards, PCs, mobile units etcetera, are returned.</p> <p>We have – by sample test - inspected terminated employees during the period, as to whether access rights have been deactivated or removed, and that assets have been returned.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>C.6</p> <p>Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.</p>	<p>We have inquired into whether the processor when offboarding employees, informs the employee of the confidentiality agreement.</p> <p>We have – by sample test - inspected employee contracts and by sample test ensured that confidentiality also applies after employment.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>C.7</p> <p>Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.</p>	<p>We have inquired about information security policy and inspected that the processor has decided upon awareness training of the employees.</p> <p>We have - by sample test - inspected that the processor is offering awareness training to the employees, which includes general IT-security and processing security in relation to personal data.</p>	<p>We have not identified any essential deviations in our test.</p>

CONTROL OBJECTIVE D:

Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.

Qampo' control procedures	Auditor's test of controls	Test findings
<p>D.1</p> <p>Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inquired about the policy for returning and deleting of data, and inspected that storage and deletion is performed according to agreement</p> <p>We have inquired about regular control of the policies and inspected that they are assessed on a regular basis.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>D.2</p> <p>Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.</p> <ul style="list-style-type: none"> <li>• Data is generally deleted at most 8-14 days after the end of the processing of the specific Data.</li> </ul> <p>However in special cases other rules may apply, in such cases these rules must be stated clearly in the signed DPA.</p>	<p>Inspected that the existing procedures for storage and deletion contain the specific requirements for the data processor's storage periods and deletion routines.</p> <p>Inspected by a sample of data processing from the data processor's overview of processing activities, that there is documentation that personal data is stored in accordance with the agreed storage periods.</p> <p>Inspected by a sample of data processing from the data processor's overview of processing activities, that there is documentation that personal data has been deleted as described.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>D.3</p> <p>Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been:</p> <ul style="list-style-type: none"> <li>• Returned to the data controller And/Or</li> <li>• Deleted if this is not in conflict with other legislation.</li> </ul>	<p>Inspected that there is formalization ready procedures for the processing of the data controller's data when the processing of personal data ceases.</p> <p>Inspected by a sample of discontinued data processing during the declaration period, that there is documentation that the agreed deletion or return of data has been carried out.</p> <p>Inspected the data processor's documentation to ensure that the data controller has received notification that the deletion has been carried out, cf. the data processor agreement section 12.3</p>	<p>We have not identified any essential deviations in our test.</p>

CONTROL OBJECTIVE E:

Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.

Qampo' control procedures	Auditor's test of controls	Test findings
<p>E.1</p> <p>Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inquired about the policy for storage of personal data and inspected that only the data processor is authorised to store personal data in accordance with the data processing agreement.</p> <p>We have inquired about the policy and inspected that it has been updated during the period.</p> <p>Inspected by random sampling of data processing from the data processor's overview of processing activities, that there is documentation that the data processing takes place in accordance with the data processing agreement.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>E.2</p> <p>Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.</p>	<p>Inspected that the data processor has a comprehensive and up-to-date overview of processing activities with an indication of localities, countries or land areas.</p> <p>Inspected by a sample of data processing from the data processor's overview of processing activities, that there is documentation that the data processing, including the storage of personal data, is only carried out in the locations that appear in the data processing agreement - or is otherwise approved by the data controller.</p>	<p>We have not identified any essential deviations in our test.</p>



CONTROL OBJECTIVE F:

Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

Qampo' control procedures	Auditor's test of controls	Test findings
<p>F.1</p> <p>Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-data processing agreements and instructions.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inquired about the procedure for monitoring the sub-processors and we have inspected that the processor is entering a data processing agreement with the sub-processor.</p> <p>We have inspected that the procedure has been updated during the period.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>F.2</p> <p>The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.</p>	<p>We have inspected a list of new data processing agreements entered during the period.</p> <p>Inspected that the data processor has an updated overview of sub-data processors used.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>F.3</p> <p>When changing the generally approved sub-data processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-data processors used, the data controller has approved this.</p>	<p>We have inquired whether there have been changes to sub-processors.</p> <p>Inspected that there are formalized procedures for notifying the data controller of changes in the use of sub-data processors.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>F.4</p> <p>The data processor has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.</p>	<p>We have – by sample test - inquired about data processing agreements and we have inspected that the sub-processor has been subject to the same or similar obligations as the controller</p>	<p>We have identified missing follow-up on data processing agreements for sub processor.</p>

<p>F.5</p> <p>The data processor has a list of approved sub-data processors. Holding the following information:</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• CVR</li> <li>• Address</li> <li>• Process description</li> </ul>	<p>We have inquired into whether the data processor has a complete and updated list of used and approved sub-processors.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>F.6</p> <p>Based on an updated risk assessment of each sub-data processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-data processor</p>	<p>We have inquired about the procedure for supervision of the sub-processors.</p> <p>We have inquired about the most recent inspection report and obtained declarations from sub-processor, and we have inspected that sub-processor has been inspected during the period.</p> <p>Inspected documentation that proper follow-up has been carried out on technical and organizational measures, the processing security of the sub-processors used.</p>	<p>We have not identified any essential deviations in our test.</p>

CONTROL OBJECTIVE G:

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

Qampo' control procedures	Auditor's test of controls	Test findings
<p>G.1</p> <p>Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>Inspected that there are formalized procedures that ensure that personal data is only transferred to third countries or international organizations in accordance with an agreement with the data controller on the basis of a valid transfer basis.</p> <p>We have inspected the procedures and ensured that it has been updated during the period.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>G.2</p> <p>The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.</p>	<p>Asked the data processor if it can confirm that no assistance has been provided to data controllers with the transfer of information to third countries during the control period.</p>	<p>We have not identified any essential deviations in our test.</p>

CONTROL OBJECTIVE H:

Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting or restricting information on the processing of personal data to the data subject.

Qampo' control procedures	Auditor's test of controls	Test findings
<p>H.1</p> <p>Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inquired about the procedure for handling of the subjects' rights, and we have inspected that the processor is being able to assist the data controller</p> <p>We have inspected documentation, that the procedure has been updated during the period.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>H.2</p> <p>The data processor has established procedures as far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting, or restricting or providing information about the processing of personal data to data subjects.</p>	<p>We have inquired about the procedure for handling of requests.</p> <p>We have inquired into whether there have been requests for assistance from data controllers during the period.</p>	<p>We have not identified any essential deviations in our test.</p>

CONTROL OBJECTIVE I:

Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processor agreement entered into.

Qampo' control procedures	Auditor's test of controls	Test finding
<p>I.1</p> <p>There are written procedures which contain requirements that the data processor must notify the data controllers in the event of a breach of personal data security. An ongoing – and at least once a year – assessment of whether the procedures need to be updated is carried out.</p>	<p>We have inspected that the procedure regarding data breach contains requirements about informing the data controllers, in case of personal data breach.</p> <p>Inspected that the procedure is up to date.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>I.2</p> <p>The data processor has established the following controls for the identification of possible breaches of personal data security:</p> <ul style="list-style-type: none"> <li>• Awareness among employees</li> <li>• Monitoring of network traffic</li> <li>• Follow-up on logging of access to personal data</li> </ul>	<p>Inspected that the data processor offers awareness training to employees in relation to the identification of possible breaches of personal data security.</p> <p>Inspected documentation that network traffic is monitored and that there is follow-up on abnormalities, surveillance alarms, etc.</p> <p>Inspected that there are procedures for follow-up on logging of access to personal data.</p>	<p>We have not identified any essential deviations in our test.</p>
<p>I.3</p> <p>In the event of any breach of personal data security, the data processor has notified the data controller without undue delay and no later than 24 hours after becoming aware that there has been a breach of personal data security at the data processor or a sub-processor.</p>	<p>Inspected that the data processor has an overview of security incidents indicating whether the individual incident has resulted in a breach of personal data security.</p> <p>Asked the data processor if it can confirm that no breach of personal data security has been detected at the sub-data processor during the declaration period.</p>	<p>We have not identified any essential deviations in our test.</p>

### **Additional information from Qampo ApS**

Regarding Control procedure F.4:

Follow-ups has been carried out to ensure that Qampo's sub processors are acting in compliance to the same security demands that Qampo is obligated to carry out towards customers and partners.

We have specifically received up-to-date copies of agreements and certificates relevant to ensure that policy is followed.

Internal procedures have also been modified to clarify how and when follow-ups towards our sub processors must be carried out correctly. These formulations and follow-ups will be available at the time of the next assurance report.