Independent service auditor's assurance report on compliance with the Data Protection Regulation (GDPR) and attached Data Protection Law as data processor covering their general services for the period of 01-04-2019 to 31-03-2020.

ISAE 3000

VISMA Consulting A/S

CVR-no.: 29 97 33 34

June 2020

Table of contents

Section 1: Visma Consulting A/S' statement

This description has been prepared for data controllers who have made use of Visma Consulting A/S' general processing in the role of data processor, and have sufficient understanding to consider the description along with other information, including information about controls operated by data controllers themselves, when assessing whether the demands stated in the EU Regulation covering "Protection of natural persons with regard to the processing of personal data and on the free movement of such data" have been met.

Visma Consulting A/S confirms that:

a) The accompanying description in Section 2 fairly presents Visma Consulting A/S' general processing of personal data on behalf of data controllers covered by the General Data Protection Regulation during the entire period of 01-04-2019 to 31-03-2020. The criteria for this statement were that the included description:

(i) Presents how Visma Consulting A/S' general processing in the role of data processor was designed and implemented, including:

- The type of services provided, hereunder the type of personal data processed.
- The procedures, within both the information technology and manual systems, by which transactions are initiated, recorded, processed, and if necessary, corrected, deleted and restricted processing of personal data.
- The processes used, to ensure that the data processing has been performed according to contract, instructions, or agreement with the data controller.
- The processes used to ensure that individuals authorised to process personal data, has committed themselves to confidentiality or are subject to a suitable statutory professional secrecy.
- The processes that upon termination of data processing ensures, that by choice of the data controller, deleting or return of all personal data to the data controller is carried out, unless law or regulations requires for storage of the personal data.
- The processes, that in case of breach of personal data security, ensures that the data controller can file a report with the controlling authorities and notify the data subjects.
- The processes, that ensures suitable technical and organizational security measures, including consideration for the risks that are connected with processing, particularly in case of accidental or fraudulent destruction of data, loss, altering, unauthorised passing of or access to personal data, being transmitted or otherwise processed.
- Controls, that we with reference to Visma Consulting A/S' general processing in the role of data processor delimitation, have assumed would be implemented by the data controller, and that, if necessary to reach the control objectives stated in the description, has been identified in the description.

- Other aspects concerning our control environment, risk evaluation process, information system (including the attached procedures) and communication, control activities and surveillance controls that have been relevant for the processing of personal data.

(ii) Contains relevant information about changes in the data processor's general processing of personal data in the role of data processor for processing personal data performed during the period of 01-04-2019 to 31-03-2020.

(iii) Does not omit or distort information relevant to the scope of the described general processing in the role of data processor for processing personal data, while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore include every aspect of the general processing in the role of data processor, that each individual data controller may consider important to their particular environment.

b) The controls, attached to the control objectives, were suitable designed and functioning efficiently during throughout the entire period 01-04-2019 to 31-03-2020. The criteria used for this statement was:

(i) The risks that threatened achievement of the control objectives stated in the description were identified.

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period 01-04-2019 to 31-03-2020.

c) Suitable technical and organisational measures have been established and maintained, in order to meet the agreements with the data controllers, good data processor practice and relevant requirements to data processors according to the General Data Protection Regulation.

Lyngby, 15 June 2020

Visma Consulting A/S

Lars Engell Berthelsen
CEO

Section 2: Visma Consulting A/S' control description

The company and our performance

Custom Solutions deliver bespoke software and software as a service to the public sector and private enterprises.

Visma provides both packaged software including software as a service (SaaS) and bespoke software solutions for public sector and large regulated private companies. For customers who need more than the packaged software can provide, we deliver custom-designed solutions.

Our mission is to expand our position as the preferred partner of software solutions to enable the continuous development of the Digital Society and eGovernment in the Nordic countries. Our Governments in the Nordics have supported the Digital Society since the early 2000s. They firmly believe that digitalization is a cornerstone in up keeping our welfare society and meet the challenges of the growing elderly population and competition from the developing countries in the future. We must simply become more efficient and digitization of the public sector is one important answer.

We digitize the Nordics

Throughout the year, we work to digitalize the Nordics. We help both public and private companies to design, develop, modernize, and maintain software. We provide both bespoke solutions and commercial off-the-shelf solutions. Together with our customers, we create increased productivity and growth in the Nordics for the benefit of all of us.

In close collaboration with customers, we develop end-to-end business software and self-service solutions that help customers to improve productivity by digitization, automation, and integration of business processes. Subsequently we maintain and further develop the solutions as part of the application lifecycle management service to keep the software updated and efficient over time.

Cooperation with our customers

We work according to agile principles and in very close cooperation with our customers. Part of our DNA is to strive for customer value. We do this through professional skills using state of the art methods and tools as well as insights to challenges in the market. As a result, our solutions make an important impact in society and value for our customers' businesses.

With technically advanced expertise and knowledge of our clients, we are analysing, designing, developing, and testing new innovative software solutions to enhance competitiveness. Through implementation and integrations, we can capture, organize, store, analyse, and visualize large amounts of information. We also reduce bureaucracy through improved online collaboration and self-service solutions. Our software solutions help large organizations to automate and manage straight-through processing enabling enterprises to become more efficient and profitable.

High degree of rules and regulation

The division is handling some of the largest ICT contracts in the public sector with values exceeding 400 MNOK each. Many of the contracts are long-term contracts (4-6 years) and include mission critical solutions with high degree of rules and regulation. Consequently, we have established long-term relations with our customers, and we invest in building value creating domain knowledge to ensure continuous satisfied customers. Some of our customers have a track record of more than 25 years.

Solutions and Services from Visma Custom Solutions

- Bespoke solutions and services
- Systems development and project delivery
- Application Lifecycle Management
- Business intelligence
- Big Data
- Machine Learning
- Predictive analytics
- Case & Document Management
- Business Process Management & straight-through processing
- Electronic signature
- Signing as a Service
- E-government solutions
- Self-service solutions
- E-commerce solutions
- Content Management solutions

Nature of processing

The purpose of the data processor processing of personal identifiable information (PII) is based on the clients' needs and instructions as stated in the Data Processing Agreement (DPA) with each client. The nature of the processing and the data differs from client to client. Visma Consulting does not store data of any EU citizen themselves - all infrastructure related to processing of EU PII is presently located with Itadel - an external hosting partner.

Personal information

Visma has stored:

- Personal information (Name, Address, email, phone etc.)
- Sensitive information (Health)
- Classified information (CPR, Income)

Categories of data subjects that are used in a DPA

- Pension takers
- Unemployed workers in Denmark (at one time or another)
- Digital Signers
- Pension Brokers
- People in Fishery (employees, ship owners, fishermen)

Practical deployments

Management in Visma or Visma Consulting A/S has approved all procedures (access control, development and acquisition, security incidents, data subject requests and risk management), controls, internal tools, and instructions to sub data processors.

Organizationally all employees have been informed about personal identifiable data and information security, including security incident procedures - what to do in case of an incident. This happens through an e-learning course and an hour meeting where security awareness is presented.

Access to VC requires access card and code, except the main entrance inside working hours where there is a manned reception.

Risk Management

As a part of each project that handles PII, the project management does a risk analysis wrt. data risk and data subject rights according to the general Visma Risk Management Process. Furthermore, VC performs every year an analysis and documents all the data where VC is a data controller. This is followed by a management review, where all the findings are approved by management or an approved mitigation is formulated.

Control measures

Processing - instructions

We always do what the DPA says. We act on behalf of the data owner, who gives the instructions on what and how to process the data.

Procedure control

There is a yearly review of all procedures based on incidents, risk assessments etc. It is carried out by the Data Protection Manager and the Security Officer.

Procedure for access control

Access to individual projects are given based on the respective Team Leads authorization. Team Lead initially presents a list of employees that need access to resources and support grants the access. Subsequent access can only be given if Team Lead approves. Access is also revoked on Team Lead request and all access (except support) is revoked upon termination of project.

Procedure for development

Most of Visma Consulting's projects are performed at client site where Visma has little influence on how the development should be performed. For in house development, the data protection manager visits each project twice a year and inspects if data subjects rights are handled within the project – i.e. can the project support the data subjects rights (Can they delete data, find data on request etc.).

Procedure for data subject Requests

The is a meeting scheduled each month, where incoming data subject requests are handled. So far, the only requests have come from Addo customers, wishing to be deleted. For other Visma products requests, this is handled by Eloqua – the marketing tool applied in the Visma group. Visma Consulting's Sales department has been developing new areas and next year, this is expected to have influence on this.

Procedure for security incidents

Security (and privacy) incidents are handled through CSIRT in Visma Group. They are available 24/7/365 and they are contacted in case of breach. From there they follow a strict procedure to contain, collect information and remedy the situation.

Sub processors

VC is a fully owned daughter company of Visma Group and a number of employee data is shared with Visma Group. No customer data is shared as such, but some data will be available to Visma Group through administration of common services.

Customer data for EU citizens are all hosted with Itadel A/S, a Danish hosting provider. Each year the reports (ISAE 3402, ISAE 3000) is evaluated by the projects using Itadel as well as an onsite inspection is performed. The latter is though only performed by one project – it is the same rack everything is stored in.

Third party

We do not currently have any data we are data processor for in a third-party country. Almost all of VC's clients are public in some way, Government, Municipality, Secretaries etc. They all frown when talking about anything else than hosting within the kingdom of Denmark. It is not so much that you cannot do it, it is merely that an acceptable DPA is not offered by any of the big players (AWS, Azure, Google).

Employees

It is stated in each employee contract that the employee is obligated to hold each client's data private.

Complementary controls

For all our projects, where data is stored outside VC's control – e.g. public projects where data is stored with Statens IT – this is almost all of our public projects, the agreement to store data is between the customer and Statens IT. Thus, it is Statens IT that is responsible for maintaining the security and privacy for all data stored. It is also Statens IT that controls the access to data – gives access, audits, and revokes access again. VC follows the procedures given to gain access and follows the DPA that Visma has with the customer – VC is still responsible for how its employees act within the systems hosted at Statens IT when access has been granted.

For a number of projects, VC works together with a third party for the customer. The contract with the third party is with the customer, but VC will exchange data with the third party. How the third party fulfils the requirements for security and privacy is agreed between the customer and the third party and it is also the customer that audits that these requirements are fulfilled.

Changes in the period

VC have received a number of contracts in the period, where a subcontractor has been used to fulfil the contract. A DPA has been made with all subcontractors where it has been relevant (some projects did not involve processing personal data).

Section 3: Independent service auditor's report of compliance with the General Data Protection Regulation (GDPR) and associated Danish Protection Act for the period 01-04-2019 to 31-03-2020

To the management of Visma Consulting A/S, their customers, and their auditors.

We have been engaged to report on Visma Consulting A/S 'compliance with the General Data Protection Regulation (GDPR) and associated Danish Protection Act for the period 01-04-2019 to 31-03-2020 in the role of data processor.

This assurance report is intended only for Visma Consulting A/S, their management, their customers and the auditors of these customers, who have sufficient understanding to consider the description of the established procedures, and must not be used for other purposes.

Visma Consulting A/S' responsibility

The management of Visma Consulting A/S is responsible for implementing and maintaining business procedures as required in the General Data Protection Regulation (GDPR) and associated Danish Protection Act.

Service auditor's responsibility

On the basis of the conducted work, it is our responsibility to express an opinion on whether the company complies with the requirements stated in the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act.

We have conducted our work in accordance with ISAE 3000, Assurance engagements other than audits or reviews of historical financial information and additional requirements under Danish audit regulation in order to obtain reasonable assurance for our opinion.

REVI-IT A/S applies International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Our work comprised enquiries, observations as well as assessments and examination in spot checks of the information we have been provided.

Due to limitations in all control systems, errors or fraud may occur, which might not be uncovered by our work. Also, the projection of our opinion on transactions in subsequent periods is subject to the risk of changes to systems or controls, changes to the requirements in relation to the processing of data or to the company's compliance with the described policies and procedures, whereby our opinion may not be applicable anymore.

Limitations in controls at a data processor

Visma Consulting A/S' description has been prepared to meet the common needs at a broad range of data controllers and may not, therefore, include every aspect of the services provided by Lessor Group, that each individual data controller may consider for important according to their specific circumstances. Also, because of their nature, controls at a processor may not prevent or detect all personal data breaches. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a controller may become inadequate or fail.

Opinion

This opinion is formed on the basis of the understanding of the criteria accounted for in the assurance report's introductory section, and which are based on the requirements in the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act.

It is our opinion that Visma Consulting A/S, in all material aspects has met the criteria mentioned for the period 01-04-2019 to 31-03-2020.

Description of tests of controls

The specific controls tested, and the nature, timing and results of these tests are listed in the subsequent main section.

Intended users and purpose

This assurance report is intended only for customers who have used Visma Consulting A/S' services in the role of data controller, and their auditors, who have sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves.

Copenhagen, 15 June 2020

REVI-IT A/S
State authorised public accounting firm

Henrik Paaske
State Authorised Public Accountant

Basel Rimon Obari
It-Auditor, (CISA, CISM), Director, Partner

Section 4: Control objectives, controls, tests, and related test controls

The following overview is provided to facilitate an understanding of the effectiveness of the controls implemented by Visma Consulting A/S according to compliance with the EU General Data Protection Regulation (GDPR) and associated Danish Data Protection Act. Our testing of functionality comprised the controls that we considered necessary to provide reasonable assurance for compliance with the mentioned articles during the period 01-04-2019 to 31-03-2020.

The requirements evident directly from the EU General Data Protection Regulation (GDPR) or the Danish Data Protection Act cannot be derogated from. However, it can be adjusted how the security is implemented, as the security requirements in GDPR in several respects are of more general and overall character that i.e. must consider purpose, nature of processing, category of personal data etc. In addition, there may be specific requirements in each customer contract that may have a scope extending beyond the general requirements of the Data Protection Act. If this is the case, these are not covered by the following.

Moreover, our assurance report does not apply to any controls performed at Visma Consulting A/S' customers, as the customers' own auditors should perform this review and assessment.

We performed our tests of controls at Visma Consulting A/S by taking the following actions:

Method	General description
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls.
Observation	Observing how controls are performed.
Inquiries	Interview, inquiry with appropriate personnel concerning the performance of controls.
Re-performance	We have performed - or observed – re-performance of controls in order to verify that the control is working as assumed.

Control objective A – Instruction regarding the processing of personal data

Procedures and controls are observed that ensure that instruction regarding the processing of personal data is complied with in accordance with the entered processor agreement.

No.	Processor's control activity	REVI-IT's performed test	Test result
A.1	There are written procedures containing requirements that processing of personal data may only occur on the basis of an instruction. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inquired whether formalised procedures have been established, to ensure that personal data are only processed on the basis of instructions from the company. We have inspected that procedures have been updated during the audit period. We have inspected calendar documentation and verified that the procedure is being evaluated on a yearly basis.	No deviations noted.
A.2	The processor only performs the processing of personal data evident from the instruction from the controller.	We have by spot check inspected 1 processing of personal data, and inspected that this is performed according to the instruction.	No deviations noted.
A.3	The processor immediately notifies the controller if an instruction according to the processor is contrary to the General Data Protection Regulation or data protection provisions in other EU law or the Member States' national legislation.	We have inspected, that formalized procedures have been established, in order to make sure that the control of processing of personal data is not contrary to the General Data Protection Regulation or other legislations.	No deviations noted.

Control objective B – Technical measures

Procedures and controls are observed that ensure that the processor has implemented technical measures for ensuring relevant security of data processing.

No.	Processor's control activity	REVI-IT's performed test	Test result
B.1	There are written procedures containing requirements on the establishment of agreed security measures for the processing of personal data in accordance with the agreement with the controller. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inquired whether formalized procedures have been established, securing compliance with agreed security measures. We have by spot check inspected 1 data processing agreement inspected that agreed security measures are established. We have inspected calendar documentation and verified that the procedure is being evaluated on a yearly basis.	No deviations noted.
B.2	The processor has performed a risk assessment and on the basis of this, has implemented the technical measures assessed to be relevant in order to achieve adequate security, including establishing the security measures agreed with the controller.	We have inquired about the performed risk assessment and inspected that risks for data subjects have been decided upon. We have inspected a control and ensured that an ongoing control of the risk log is performed. We have inspected management approval of the most recent risk log.	No deviations noted.
B.3	Antivirus is installed on the systems and databases that are used for the processing of personal data, and the antivirus is updated regularly.	We have inquired about statement from operations supplier and inspected that servers and databases are efficiently protected against malware.	No deviations noted.
B.4	External access to systems and databases used for the processing of personal data occurs through a secured firewall.	We have inquired whether external access to systems and databases, used for processing of personal data, only can be performed through established firewall. We have inspected, that firewall is configured according to relevant internal policy.	No deviations noted.
B.5	Internal networks are segregated in order to ensure restriction of access to systems and databases used for the processing of personal data.	We have inquired about a list of the network, including IP-summary, and inspected that internal networks have been segregated. We have inquired about overview of servers and inspected that these are segregated.	No deviations noted.

No.	Processor's control activity	REVI-IT's performed test	Test result
B.6	Access to personal data is isolated to users with a work-related need for this.	We have inspected the procedures for granting access and registration of new user and we have ensured that access rights are being evaluated based on a work-related need. We have by spot check inquired about accesses and inspected that they are work-related.	No deviations noted.
B.7	System monitoring with alarming has been established for the systems and databases used for the processing of personal data.	We have by spot check inspected monitoring of capacity and logging.	No deviations noted.
B.8	Effective cryptography is used at the transmission of confidential and sensitive personal data via the Internet and via email.	We have inquired VPN protocol by access to internal networks and inspected that they are configured. We have inquired about monitoring of TLS. We have by spot check inspected implementation of certificates.	No deviations noted.
B.9	Logging has been established in systems, databases, and networks.	We have by spot check inspected logging of transactions, service windows and access requests. We have inquired about statement from operation providers and inspected that logging of server access has been established.	No deviations noted.
B.10	Personal information used for development, test or similar, are always in pseudonymised or anonymised form. Usage is only in order to perform the controller's purpose according to agreement and on its behalf.	We have inquired whether the data processor is using personal data for testing.	We have been informed, that the data processor is not using personal data during test, without instruction. No further deviations noted.
B.11	The established technical measures are regularly tested by means of vulnerability scans and penetration tests.	We have by spot check, inspected vulnerability scans of portals.	No deviations noted.
B.12	Changes to systems, databases, and networks are made in accordance with established procedures that ensure maintenance by means of relevant updates and patches, including security patches.	We have inspected the procedure for changes and patch management. We have by spot check inspected changes during the period, and we have ensured that these have been made according to the procedures.	No deviations noted.

No.	Processor's control activity	REVI-IT's performed test	Test result
B.13	There is a formal procedure for allocating and revoking user accesses to personal data. Users' accesses are regularly reviewed, including that rights still can be justified by a work-related need.	We have inquired about the procedure for access management, and we have inspected that procedures for granting and termination of access has been decided upon. We have by random test, inspected review of system access.	No deviations noted.
B.14	Access to systems and databases, in which personal data is processed, which entails a high risk for the data subjects, occurs as a minimum by means of two factor authentication.	We have inquired about implementing of VPN connection of remote workplace.	No deviations noted.
B.15	Physical access security has been established such that only authorised persons can gain physical access to premises and data centres in which personal data are stored and processed.	We have inquired about operations supplier and inspected, that physical security of servers has been established.	No deviations noted.

Control objective C – Organisational measures

Procedures and controls are observed that ensure that the processor has implemented organisational measures for ensuring relevant security of data processing.

No.	Processor's control activity	REVI-IT's performed test	Test result
C.1	The processor's management has approved a written information security policy, which has been communicated to all relevant stakeholders, including the processor's employees. The information security policy is based on the performed risk assessment. Regularly – and at least annually – an assessment is made of whether the information security policy should be updated.	We have inquired about information security policy, and we have inspected that is has been communicated to the processor's employees. We have inquired about list of roles, and we have inspected that responsibilities have been assigned. We have inspected documentation, that the policy has been updated during the period.	No deviations noted.
C.2	The processor's management has ensured that the information security policy is not contrary to entered processor agreements.	We have inquired about information security policy and we have by spot check inspected data processor agreements, and ensured that there is one available in accordance with data processor agreements.	No deviations noted.
C.3	The processor's employees are checked in connection with employment.	We have inquired about the procedure for onboarding employees. We have by random test inspected that recruitment procedures have been followed.	No deviations noted.

No.	Processor's control activity	REVI-IT's performed test	Test result
C.4	At employment, employees sign a confidentiality agreement. In addition, the employee is introduced to the information security and procedures regarding data processing as well as other relevant information in connection with the employee's processing of personal data.	We have by spot check inquired about employment agreement, and we have inspected that a confidentiality agreement is included. We have by spot check inspected notice of intro meetings, and we have ensured that new employees are being introduced to information security.	No deviations noted.
C.5	At the termination of employment, a procedure has been implemented at the processor ensuring that the user's rights are deactivated or terminated, including that assets are returned.	We have inquired about procedures that ensures, that terminated employees' access rights are deactivated or removed upon resignation, and that assets such as key cards, PCs, mobile units etc. are returned. We have inspected, by spot check of 5 terminated employees, during the period, that access rights have been deactivated or removed. We have inspected a list of mobile units. We have by spot check inspected documentation that assets have been returned upon resignation.	No deviations noted.
C.6	At termination of employment the employee is informed that the signed confidentiality agreement still is applicable, and that the employee is subject to a general duty of non-disclosure in relation to the processing of personal data that the processor performs for the controllers.	We have inquired whether the processor when offboarding employees, informs the employee of the confidentiality agreement.	We have been informed, that the processor does not inform employees about the confidentiality agreement, in connection with them leaving. No further deviations noted.
C.7	There is periodic awareness training of the processor's employees in relation to information security in general as well as security of data processing in relation to personal data.	We have inquired about information security policy and inspected that the processor has decided upon awareness training of the employees. We have by spot check inspected that the processor is offering awareness training to the employees, which includes general it-security and processing security in relation to personal data.	No deviations noted.
C.8	The processor has assessed the need for a DPO and has ensured that the DPO has the adequate professional competence to perform their tasks and are involved in relevant areas.	We have by spot check, inquired about awareness training and we have inspected that the DPO is monitoring the company.	No deviations noted.

Control objective D – Return and deletion of personal data

Procedures and controls are observed, that ensure that personal data can be deleted or returned if agreed with the controller.

No.	Processor's control activity	REVI-IT's performed test	Test result
D.1	There are written procedures containing requirements that storage and deletion of personal data occurs in accordance with the agreement with the controller. Regularly – and at least annually – an assessment has been made, whether the procedures should be updated.	We have inquired about policies for returning and deletion of personal information, and we have inspected that returning and deletion is being performed according to agreements. We have inquired about the policy for returning and deleting of data, and inspected that storage and deletion is performed according to agreement. We have inquired about regular control of the policies and inspected that they are assessed on a regular basis.	No deviations noted.
D.2	Specific requirements to the processor's storage period and deletion routines have been agreed.	We have by spot check inquired about data processor agreements, and we have inspected that return and storage have been agreed upon.	No deviations noted.
D.3	At the end of the processing of personal data for the controller, data is according to the agreement with the controller: • Returned to the controller, and/or • Deleted, where not in conflict with other legislation	We have inquired whether there has been terminated projects during the period.	We have been informed, that there have been no terminated projects during the period, where the company has stored personal data, wherefore we couldn't test the control. No further deviations noted.

Control objective E – Storage of personal data

Procedures and controls are observed that ensure, that the processor only stores personal data in accordance with the agreement with the controller.

No.	Processor's control activity	REVI-IT's performed test	Test result
E.1	There are written procedures, containing requirements that storage of personal data only occurs in accordance with the agreement with the controller. Regularly – and at least annually – an assessment has been made, whether the procedures should be updated.	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. We have inquired about the policy and inspected that is has been updated during the period. We have inquired about regular control of the policy and inspected that it has been assessed on a regular basis.	No deviations noted.
E.2	The processor's processing including storage must only take place at the locations, in the countries, or the territories approved by the controller.	We have by spot check inquired about data processing agreement and we have inspected that the processing of data is performed on the agreed locations.	No deviations noted.

Control objective F – Use of sub-processors

Procedures and controls are observed that ensure, that only approved sub-processors are used and that the processor when following up on their technical and organisational measures for protection of the rights of the data subjects and the processing of personal data ensures adequate security of data processing.

No.	Processor's control activity	REVI-IT's performed test	Test result
F.1	There are written procedures containing requirements to the processor at the use of sub-processors, including requirements on sub-processor agreements and instruction. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	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. We have inspected that the procedure has been updated during the period.	No deviations noted.
F.2	The processor solely uses sub-processors for the use of processing of personal data that are specifically or generally approved by the controller.	We have inspected a list of new data processing agreements entered during the period. We have by spot check inquired about data processing agreements and inspected that there has either been granted a general or a specific permission to use sub-processors.	No deviations noted.
F.3	In case of changes to the use of generally approved sub-processors, the controller is informed in a timely manner in order to be able to raise objections and/or withdraw personal data from the processor. In case of changes to the use of specifically approved sub-processors, this is approved by the controller.	We have inquired whether there has been changes to sub-processors.	We have been informed that there have been no changes to sub-processors during the period. No further deviations noted.
F.4	The processor has subjected the sub-processor to the same data protection obligations as those stated in the processor agreement or the like with the controller.	We have by spot check 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.	No deviations noted.
F.5	The processor has a list of approved sub-processors.	We have inquired that the data processor has a complete and updated list of used and approved sub-processors.	No deviations noted.

No.	Processor's control activity	REVI-IT's performed test	Test result
F.6	On the basis of an updated risk assessment of each sub-processor and the activity taking place at this sub-processor, the processor performs periodic follow-up on this at meetings, inspections, review of assurance report, or similar. The data controller is being regularly informed about the follow-up at the sub-processor.	We have inquired about the procedure for supervision of the sub-processors. We have inquired about the most recent inspection report and obtained declarations from sub-processors, and we have inspected that sub-processors have been inspected during the period.	No deviations noted.

Control objective G – Transfer of personal data to third countries

Procedures and controls are observed that ensure, that the processor only transfers personal data to third countries or international organisations in accordance with the agreement with the controller on the basis of a valid ground for transfer.

No.	Processor's control activity	REVI-IT's performed test	Test result
G.1	There are written procedures containing requirements that the processor only transfers personal data to third countries or international organisations in accordance with the agreement with the controller on the basis of a valid ground for transfer.	We have inquired whether data is being transferred to third countries.	We have been informed, that the data processor does not transfer data to third countries, wherefore this point is not relevant. No deviations noted.
G.2	The processor may only transfer personal data to third countries or international organizations after instructions from the data controller.	We have inquired whether processor transfers data to third countries.	We have been informed, that the data processor does not transfer data to third countries, wherefore this point is not relevant. No deviations noted.
G.3	In connection with transfer of personal data or personal information to third countries or international organizations, the data processor has assessed and documented that a valid transfer basis has been established.	We have inquired whether the processor transfers data to third countries.	We have been informed, that the data processor does not transfer data to third countries, wherefore this point is not relevant. No deviations noted.

Control objective H – Rights of the data subjects

Procedures and controls are observed that ensure, that the processor can assist the controller with handing over, correcting, erasing, or the restriction of, and providing information about, the processing of personal data to the data subject.

No.	Processor's control activity	REVI-IT's performed test	Test result
H.1	There are written procedures containing requirements that the processor must assist the controller in relation to the rights of the data subjects. Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inquired about the procedure for handling the subjects' rights, and we have inspected that the processor is being able to assist the data controller. We have inspected documentation, that the procedure has been updated during the period.	No deviations noted.
H.2	The processor has established procedures that to the extent agreed permits timely assistance to the controller in relation to handing over, correcting, erasing, or the restriction of and providing information about the processing of personal data to the data subject.	We have inquired about the procedure for handling of requests. We have inquired whether there has been requests for assistance from data controller during the period. We have by spot check inspected the erasing of users.	We have been informed, that the data processor has not received requests from the data controller during the period. No further deviations noted.

Control objective I – Managing personal data breaches

Procedures and controls are observed that ensure, that any personal data breaches can be managed in accordance with the entered processor agreement.

No.	Processor's control activity	REVI-IT's performed test	Test result
I.1	There are written procedures containing requirements that the processor must inform the controller in case of personal data breaches.	We have inquired about the procedure and we have inspected, that the procedure considers requirements for informing the data controllers in case of personal data breach.	No deviations noted.
I.2	The processor has established the controls for identification of any personal data breaches.	We have – by spot check - inspected that awareness training of employees has been established.	No deviations noted.
I.3	In case of a personal data breach the processor has informed the controller without undue delay after finding out that the personal data breach has occurred at the processor or a sub-processor.	We have inquired about personal data breaches.	We have been informed, that there have been no personal data breaches during the period. No further deviations noted
I.4	The processor has established procedures for assisting the controller when filing a complaint with the Danish Data Protection Agency.	We have inquired about the procedure for personal data security breach and inspected that the procedures include measures for assisting the controllers.	No deviations noted.

Control objective J - Terms of consent and duty of disclosure

Procedures and protocols are observed that ensure, that the data subjects have given written consent to personal data being processed, and where it has been made sure the data subject has received controller's contact information necessary to fulfil the duty of disclosure.

No.	Processor's control activity	REVI-IT's performed test	Test result
J.1	Written procedures for obtaining written consent of personal data being processed, is available.	We have inquired whether the processor is obtaining consent on behalf of the controller.	We have been informed that the processor does not obtain consent on behalf of the controller. No further deviations noted.
J.2	Technical measures have been implemented to ensure that it can be documented which information has been given in connection with consent.	We have inquired whether the processor is obtaining consent on behalf of the controller.	We have been informed that the processor does not obtain consent on behalf of the controller. No further deviations noted.
J.3	Written procedures are available, describing measures to ensure that the data subject is informed about the purpose of processing personal data including information about transfer of personal data to recipients, third countries or international organizations, or how the processor can assist the controller herewith.	We have inquired whether the processor is responsible for fulfilling the duty of disclosure.	We have been informed that the controller is not responsible for the duty of disclosure. No further deviations noted.
J.4	Regularly - and at least annually – it is inspected whether every data subject has received the description of the subjects' right to insight in, correction of, or deletion of personal data.	We have inquired whether the processor is responsible for fulfilling the duty of disclosure.	We have been informed that the controller is not responsible for the duty of disclosure. No further deviations noted.

Control objective K – Record of processing activities

Procedures and controls are observed, that ensure that the processor maintains a record of categories of processing activities performed on behalf of the controller.

No.	Processor's control activity	REVI-IT's performed test	Test result
K.1	The processor keeps a record of categories of processing activities for each controller.	We have inspected documentation that a record of categories of processing activities for each controller, including the necessary information, is available.	No deviations noted.
K.2	Regularly – and at least annually – an assessment is made of whether the record of categories of processing activities for each controller should be updated.	We have inspected documentation that the record of categories of processing activities for each controller is updated and correct.	No deviations noted.
K.3	Management has ensured that the record of categories of processing activities for each controller is adequate, updated, and correct.	We have inspected documentation for the record being approved by the management.	No deviations noted.