BEIERHOLM

DECEMBER 2022

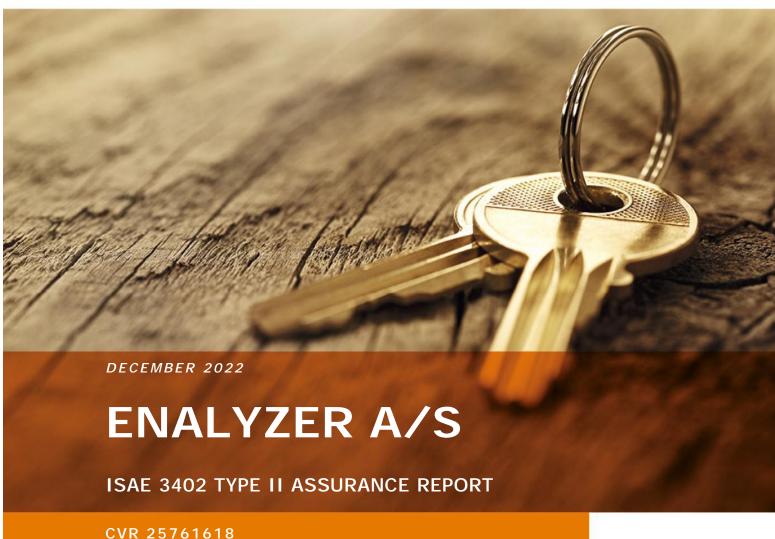# ENALYZER A/S

ISAE 3402 TYPE II ASSURANCE REPORT

CVR 25761618

Independent auditor's report on the control environment related to the operation of Enalyzer SaaS solutions for data collection and reporting.

In addition, a paragraph has been added to the description about the role as data processor in accordance with the General Data Protection Regulation.

Structure of the Assurance Report

Chapter 1:
Letter of Representation.

Chapter 2:
Description of the control environment for the operation of Enalyzer SaaS solutions for data collection and reporting.

Chapter 3:
Independent auditor's assurance report on the description of controls, their design and operating effectiveness.

Chapter 4:
Auditor's description of control objectives, security measures, tests and findings.

Letter of Representation

Enalyzer A/S processes personal data on behalf of Data Controllers according to Data Processor Agreements regarding operation of Enalyzer SaaS Solutions.

The accompanying description has been prepared for the use of customers and their auditors, who have used Enalyzer A/S' SaaS solutions, 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.

Enalyzer A/S hereby confirms that

(A) The accompanying description, Chapter 2 (incl. Appendix 1) gives a true and fair description of Enalyzer A/S' control environment in relation to operations of Enalyzer SaaS solutions throughout the period 1 October 2021 - 30 November 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 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 is 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 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 Enalyzer SaaS 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 Enalyzer SaaS solutions performed throughout the period 1 October 2021 - 30 November 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 and operated effectively throughout the period 1 October 2021 - 30 November 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, and

(iii) The controls were applied consistently as designed, including that manual controls were performed by persons with adequate competences and authority throughout the period 1 October 2021 - 30 November 2022.

(C) Appropriate technical and organizational measures are established in order to honour the agreements with the Data Controllers, generally accepted data processing standards and relevant demands to Data Processors according to the General Data Processing Regulation.

(D) The accompanying description and the related criteria for fulfilling the control objectives and controls, Chapter 2 (incl. Appendix 1) have been prepared based on compliance with Enalyzer A/S' standard agreement as well as related Data Processing Agreement. The criteria for this basis are:

(i) Enalyzer – Data Processing Agreement
(ii) ISMS handbook
(iii) Employee Handbook

Copenhagen, 12 December 2022

Jakob Roed, Founder & Co-CEO   **Steen Ødegaard, Founder & CTO**
Enalyzer A/S, Refshalevej 147, DK-1432 Copenhagen K, CVR 24761618

Description of the control environment for the operation of Enalyzer SaaS solutions for data collection and reporting

Introduction

The purpose of this description is to provide information to Enalyzer A/S' customers and their auditors regarding the requirements of ISAE 3402, which is the international auditing standard for declaration tasks regarding controls at service providers.

The scope of this description is exposure of the technical and organizational security measures implemented in connection with the operation of the Enalyzer SaaS solutions for data collection and reporting, delivered as self-administered web applications or as an outsourced consulting project.

As a supplement to the description below, an independent paragraph (Compliance with the role as data processor) is added, including a description of essential requirements in connection with the role as data processor combined with general requirements from data processor agreements.

Description of Enalyzer A/S

Enalyzer A/S was established in 2000. Enalyzer's core business is to develop and operate its Enalyzer Software as a Service solutions, for the customers to run their survey activities efficiently. The solution is supplied as a service hosted in data centers operated by Enalyzer's hosting providers.

Besides that, Enalyzer provides consulting survey services, where projects are outsourced to Enalyzer, in full or in part.

Self-administered surveys on Enalyzer's survey platforms as well as projects outsourced to Enalyzer (mainly fully executed on Enalyzer's own platforms) normally address surveys within human resources, sales, marketing and education.

Scope of this description

As a SaaS supplier, Enalyzer is responsible for establishing and maintaining relevant procedures and controls, ensuring that any security issue is identified and managed according to the requirements laid down in the agreements with the customers.

This description is based on Enalyzer's security policies governing the everyday operations of Enalyzer SaaS solutions, and the relevant parts of Enalyzer's Data Processor Agreement with the customers.

Business strategy / IT security strategy

Enalyzer software is designed to secure that neither the customers nor the company are subjected to any unacceptable security risks.

The purpose of Enalyzer's IT security strategy is to ensure:

- The existence of relevant prerequisites for secure operations of Enalyzer SaaS solutions
- Enalyzer software and customer data are sufficiently protected against incidents
- Systems and data can be reestablished with predictability and according to familiar working methods
- Customer data is accessed by relevant Enalyzer personnel, when carrying out necessary tasks

- That exclusively authorized persons have access to the operating environment, systems and data

Enalyzer works with IT security at a business-strategic level to ensure a high degree of service and quality. The IT security policy emphasizes the importance of IT security in the company. In relation to its IT security strategy, Enalyzer has chosen to take ISO 27001 + 2 as its starting point, and has used the ISO method to implement the relevant security measures within the following areas:

• Information security policies	• Communications security
• Organisation of information security	• Supplier relationships
• Human resources security	• Information security incident management
• Asset management	• Information security aspects of business continuity management
• Access control	• Compliance with legal and contractual requirements
• Physical and environmental security	
• Operations security	

In addition, Enalyzer's Data Processing Agreement (DPA) binds the company to implement relevant security measures regarding:

- Data processing activities conducted on behalf of the customers (items 3 and 5 in the DPA)
- Data breach monitoring and reporting (item 7 in the DPA)

The implemented security measures at Enalyzer are described in appendix 2.

Enalyzer A/S' organization and organization of IT security

Enalyzer employs approximately 40 employees and has a flat organizational structure. The Co-CEO's manages the company together with the senior management group.

In order to ensure the correct level of focus on information security, Enalyzer has appointed a specific Information Security Board acting on behalf of the management and taking the responsibility of security issues. The security board consisted of:

Jakob Roed, Founder & Co-CEO
Steen Ødegaard, Founder & CTO
Wiktor Jespersen, System Administrator

The Information Security Board is chaired by Chief Security Officer Steen Ødegaard

Johan Leonhard, Nyborg & Rørdam, is Data Protection Officer (DPO).

Risk management at Enalyzer A/S

The purpose of the information security policy is to define a framework for the protection of valuable information and, in particular, to ensure that critical and sensitive information and information systems maintain their confidentiality, integrity and accessibility.

On this background, Enalyzer's management has chosen a risk-based information security management system, ensuring that all notable threats are mitigated in an appropriate manner. This way, predictable security problems can be prevented, and potential damages limited, ensuring effective restoration of information in case of an incident.

The risk management policy is established to cover or limit the risks created by everyday activities to a level enabling the company to maintain normal operations. Enalyzer carries out risk management and

internal checks in relevant areas and on relevant levels: the risk and impact assessment process is executed annually, in order to keep the management aware of the risk profile of Enalyzer. Risk assessments are also conducted, if significant changes take place in the company.

Enalyzer has carried out a risk analysis regarding the relevant operations and drawn up the Enalyzer Information Security Management System based on the results of the risk assessment. Furthermore, an incident response policy with a corresponding disaster recovery plan has been created utilizing the outcome of the risk management process.

As agreed, while creating the IT security strategy, Enalyzer works using known international standards for IT security. The ISO 27001 + 2 is the primary reference framework for IT security used at Enalyzer. The work process regarding IT security is a continual and dynamic process, ensuring that Enalyzer at all times complies with its customers' needs, and with legal and contractual requirements.

IT security execution

The management of Enalyzer has the day-to-day responsibility for IT security, ensuring that the overall requirements and framework for IT security are maintained. To ensure that information security is appropriately addressed in Enalyzer, the management has appointed an Information Security Board to handle security related work in Enalyzer. At all times, the Information Security Board consists of the Information Security Officer and members of the senior management group.

The structure of the Enalyzer ISMS is described in the central IT security policy created by the management. The aim of the Enalyzer ISMS is for the company to have a shared set of rules and guidelines regarding information security, ensuring a stable and secure operating environment. On a regular basis, Enalyzer makes improvements to policies, procedures and operations in order to ensure that we comply with our customers' requirements as well as with relevant legislation.

Enalyzer's IT security focus is on everyday operations, and on the ability to ensure that a well-functioning Enalyzer offers services to the customers on an acceptable level. The ISMS applies to all employees without exception, both permanent and temporary staff, and, where relevant, to outsourced workforce working for Enalyzer.

When outsourcing parts of Enalyzer's operations, the service provider must cooperate with Enalyzer to ensure the appropriate security level as well as ensuring operations being executed in accordance with the Enalyzer ISMS. Compliance related hereto is essentially documented by external independent IT audit reports. Enalyzer protects its information and solely allows use of and access to information in accordance with the company's guidelines and the current legislation.

HR, employees and training

All employees have the responsibility to help protect Enalyzer's information against unauthorized access, change and destruction as well as theft. Accordingly, Enalyzer has created an information security awareness program, ensuring continuous education in information security. The ongoing training concentrates on the key items of GDPR, and the implementation of the revised information security policies.

As users of Enalyzer's information, all employees must adhere to the information security policy and the guidelines deriving from it. Employees are only allowed to use Enalyzer's information in keeping with the work they perform in the company and are obliged to protect the information in a manner relevant to the sensitivity of the information.

The Information Security Board has devised guidelines for the recruitment, retention and resignation of staff, among other things to ensure that relevant skills are maintained and that Enalyzer's security policies are complied with.

Verification of the background of all job candidates must be carried out in accordance with relevant laws, regulations and ethical rules. This applies both to Enalyzer's employees and to the employees of the company's partners. The Information Security Board requires all employees and contractors to comply with information security in accordance with Enalyzer's policies and procedures.

The company's employees and relevant collaborative partners are regularly informed and made aware of Enalyzer's information security by means of training and updates. Information security responsibilities and obligations that apply after the end or change of employment are defined and communicated to the employee/supplier and enforced by the company.

Compliance related hereto is essentially documented by external independent IT audit reports.

The Information Security Board is responsible for security updates on a regular basis for the whole company, for arranging the appropriate security training in Enalyzer, and for ensuring that security matters are addressed on an acceptable level in the company.

Asset management

The following part of the chapter presents the more technical aspects of the Enalyzer software and the everyday operations of it. First, the management of key information assets is discussed, following by a walk-through of the access control highlights, physical and environmental security controls, and operations and communications security.

The Information Security Board has carried out an inventory of the assets according to the priorities and risks identified during the risk assessment process. All relevant assets are assigned an owner responsible for ensuring the appropriate level of security and for acceptable rules for the use of the assets.

The Information Security Board acknowledges that staff is often the biggest threat to an organization's security and has taken steps in order to lower that risk by drawing up clear internal guidelines about acceptable use of both internal and external key assets.

The Information Security Board has also devised guidelines about information assets: just like any tangible assets, important information assets are to be handled appropriately by first classifying and labeling them. Information assets are handled according to Enalyzer's acceptable use policies in order to ensure an appropriate level of security in handling information assets.

Like all Enalyzer's security policies, the rules regarding asset management are applied to all Enalyzer employees, and to partners, suppliers and outsourced staff when relevant. The asset management guidelines are revised regularly, as a minimum annually, and more often when relevant.

Access control

The logical and physical access control is an important part of Enalyzer's information security management system. The access control policies apply to all Enalyzer employees and to freelance workforce/external suppliers working for Enalyzer, if they are involved in work that grants access to any of the systems containing confidential information.

The Information Security Board has drafted a number of policies governing the access to systems containing confidential information. In general, access rights are granted on a need-to-have basis: if the person in question needs access to certain information, logical or physical location, he/she must address the matter with a person, who can grant that access, if this is deemed relevant.

Granting access rights to all relevant locations is a part of the onboarding process of a new employee. Revoking or granting access rights can also become relevant, when the roles and rights of an employee are reviewed. Access to all Enalyzer's systems and services are revoked, when an employee's contract with Enalyzer is terminated. All Enalyzer's employees are given access to certain systems during onboarding (email client, internal chat software, ticket handling system, internal documentation system etc.), but access to other systems is only granted, if the employee will be working in a role requiring certain access clearance.

Access to an Enalyzer customer instance is given on a need-to-have-basis: only relevant employees working for Customer Engagement or Research & Development can access customer instances, and only when it is needed for a legitimate cause. Access to a customer instance is revoked immediately after the task has been performed, and Enalyzer will always ask for a permission from the customer, if Enalyzer is going to perform significant changes to a customer instance outside the regular upgrade schedule.

Similarly, access to any recipient data is granted only if needed, and only to relevant people working for Customer Engagement or Research & Development. Access to recipient data must be cancelled immediately, when access is no longer needed to perform the task in question.

Enalyzer logs the user access to different instances and takes any breaches of access control rules very seriously; accessing customer instances for no legitimate reason can cause employment relationship to be terminated.

Access to Enalyzer's operational systems is regulated with personal LDAP logins, which all staff is obliged to use. Only specific employees are granted access to IT-systems that are critical for the operations and deployment of Enalyzer software. All deployments to Enalyzer source code are managed via controlled script in a secure environment, and only certain members of the R&D team have access in different areas within the deployment system. All operations conducted in the deployment system are logged, and access to the deployment environment is revoked, when it is no longer needed by the employee.

Physical and environmental security

Outsourcing the hosting services to Microsoft Azure helps Enalyzer to concentrate on the everyday operations of the SaaS solutions for data collection and reporting. The solutions are delivered as self-administered web applications or as an outsourced consulting project. Services by Microsoft Azure include server virtualisation, network, power and rack space for the physical servers.

Microsoft Azure are compliant with ISO 27001 security framework and are being audited regularly. Audit reports are reviewed annually by Enalyzer.

According to the latest audit reports of Microsoft Azure physical and environmental security, the mentioned suppliers applied the following ISO 27002 controls:

- A.11.1.1 Physical security perimeter
- A.11.1.2 Physical entry controls
- A.11.1.3 Securing offices, rooms and facilities
- A.11.1.4 Protecting against external and environmental threats
- A.11.1.5 Working in secure areas
- A.11.1.6 Delivery and loading areas

Enalyzer has reviewed the latest Microsoft Azure audit reports and found the results acceptable.

Enalyzer's office does not host any business-critical information related to the operation and development of the Enalyzer SaaS solutions. Enalyzer ensures the physical security of the office by having relevant physical access controls, video surveillance and fire protection in place.

Operations security

In order to ensure an appropriate level of operations security, Enalyzer has applied a variety of controls addressing security issues, covering:

- Operating procedures documentation
- Change management
- Capacity management
- Separation of development, testing, and operation environments
- Protection from malware
- Backup and recovery
- Logging and monitoring
- Installation of software on operation systems, and
- Management of technical vulnerabilities

The overview below will cover the parts of the policies considered relevant for external stakeholders.

Operating procedures documentation
Operating procedures documentation can cover, for example: processing and handling of information (information classification, confidentiality requirements), backup and restore procedures, work scheduling requirements, error handling, guidelines in case of a system failure etc.

Clear documentation guidelines ensure that all Enalyzer's operating procedures and system processes, as outlined in the IT Security Policy, are documented at an appropriate level.

Change management
Changes to the ICT infrastructure are undertaken by authorised staff working in an IT function authorised by Enalyzer A/S. The changes are subject to auditable change management procedures.

Changes to Enalyzer's ICT infrastructure and operation systems are controlled by a formal change control procedure. The change control procedure covers the reason for the change, relevant test documentation, impact assessments conducted, formal approval process, change communication, procedures for roll-back in case of unexpected issues, process for planning and testing of changes, including fall-back (abort/recovery) measures, documenting the changes made and identification of significant changes and relevant risk assessments.

All changes to the ICT infrastructure are assessed for impact on the security of information as a part of standard risk assessments.

Capacity Management
Operations Department monitors the capacity demands of Enalyzer's systems and makes projections of future capacity requirements to fulfil adequate power and data storage requirements.

Utilization of key system resources are monitored allowing additional capacity to be added online, when required.

Separation of development, testing, and operation environments
Development, testing, and operation environments are separated to reduce the risks of unauthorized access or changes to the operation environment. The operation environment runs separately and with

limited access. All development takes place locally on workstations, and required testing environments are provided, when needed.

Production environments are protected from malware via secure IT-architecture. Enalyzer has a number of logical environments, with each environment representing differing trust levels and each protected by a logical security perimeter. This perimeter is created by setting firewalls between the logical environment and interconnecting them in such a way that they control access and information flow between them.

Backup and recovery
The backup policy ensures appropriate protection against loss of data and ensures the ability to restore data that has been lost or corrupted in the client's system.

Backup copies of information, software and system images are taken and tested regularly in accordance with Enalyzer's backup setup rules. Restoring data is done in accordance with the recovery policies. IT backup and recovery procedures are documented, regularly reviewed and made available to the staff responsible for performing data and IT system backup and recovery – only the operations team is allowed to access the backups.

Enalyzer's backup and deletion setup adheres to the guidelines drafted in the standard SLA; full daily backup is kept and retained for a maximum period of 30 days. Backup data is stored in a remote location, and on redundant storage. Backups are performed daily, and the routine backup operations require no manual intervention, and cause no extra downtime to the customer instances. Customer data are encrypted, while being transferred, and all customer sensitive data is stored in an encrypted format while being located on Enalyzer's SaaS solutions.

Logging and monitoring
Enalyzer A/S logs system events and selected applications locally using a central logging solution. The logging facilities and log information are protected against tampering and unauthorized access.

The clocks of all relevant information processing systems, within the organization or security domain, are synchronized to time sources.

Control of operating software
Enalyzer has a procedure in place to control the installation of software on operating systems. The updating of the operating software, applications, and program libraries is performed only by trained administrators after being granted appropriate management authorization. Applications and operating system software are implemented only after extensive testing. An audit log is maintained of all updates to operating program libraries, and previous versions of the software are retained as contingency measures.

Third party software used in operating systems are maintained at a level supported by the supplier. Relevant software patches are applied to help remove or reduce security weaknesses. Where Enalyzer relies on externally supplied software and modules, relevant monitoring and controlling systems are in place to avoid unauthorized changes, which could introduce security weaknesses.

Management of technical vulnerabilities
Enalyzer Operations conduct reviews about technical vulnerabilities of information systems being used in Enalyzer. In case severe vulnerabilities are found, the exposure to such vulnerabilities is evaluated and appropriate measures are taken to reduce the risks to everyday operations.

Segregation of customer data

Enalyzer's SaaS solutions is a true multi-tenant solution. Each tenant's data is isolated and remains invisible to other tenants. To ensure this, the SaaS solutions check authorization on all requests for data. The authorization mechanism is a main part of the security architecture.

This affords us the ability to better adapt the solution to the customers' needs, and it improves the system security.

Communications security

Enalyzer ensures the protection of information in networks and its supporting information processing facilities, by having implemented relevant network controls. Networks are adequately managed and controlled to protect information in systems, applications, and data. The security of information in networks, and the protection of connected services are appropriately secured against unauthorized access.

Enalyzer has established controls to safeguard the confidentiality and integrity of data transferred via public networks or via wireless networks, to protect the connected systems & applications, and to maintain the availability of the network services and computers connected.

The architecture of Enalyzer's network is designed to reflect Enalyzer's needs and resources. The Network Managers implement a range of controls to achieve and maintain the security of information in Enalyzer's networks, particularly in those spanning across organizational boundaries. The controls are also implemented to protect the supporting infrastructure and to protect connected services from unauthorized access.

As mentioned earlier, the Enalyzer network setup is divided into a number of logical network environments, with each environment representing differing trust levels, each protected by a defence.

Formal transfer policies, procedures and controls are in place to protect the transfer of information internally.

Supplier relationships

Enalyzer works with suppliers in operating and developing the Enalyzer SaaS solutions. For key suppliers, who have access to customer instances, it is mandatory to have GDPR-compliant Subprocessor Agreements in place with Enalyzer, compelling the suppliers to follow the same regulations as Enalyzer. Relevant suppliers must also be compliant with Enalyzer's information security policies.

Furthermore, Enalyzer suppliers are expected to demonstrate an acceptable level of security by having relevant security documentation in place and by having their security setup audited regularly.

Breaches of these requirements may result in the supplier relationship being terminated.

Enalyzer's Information Security Board participates in the evaluation and approval of software development partners and software vendors. Furthermore, Enalyzer's customers are notified, if Enalyzer is changing software development partners, and the customers have the right to oppose such changes.

In case a supplier needs access to sensitive data, the supplier must document a satisfactory level of security, and document the actual level of security i.e. in the form of an audit report. The supplier must also have appropriate formal procedures in place for change management and patch management in accordance with best practice.

If the supplier has access to sensitive data or IT infrastructure, the supplier must guarantee appropriate network, firewall and encryption levels. The network architecture must demonstrate an appropriate security level. All this must be appropriately documented, and the documentation must be available to Enalyzer.

Managing IT security incidents

Enalyzer incident management policies are devised to ensure quick detection, reaction and response to security incidents, and to outline the processes following a security incident. All employees at Enalyzer are familiar with the procedures for reporting different types of incidents and weaknesses, which might influence operations security. Security incidents and weaknesses must be reported as quickly as possible to the management group.

The management group is responsible for defining and coordinating a structured management process that ensures an appropriate reaction to security incidents. All Enalyzer's employees, partners, contractors and suppliers have a responsibility to report security incidents and data breaches as quickly as possible to Enalyzer Support Team. This obligation also extends to any external organisation contracted to support or access the Enalyzer Information Systems.

Enalyzer is responsible for the security and integrity of all the data, it stores. Enalyzer protects data using all means necessary: incidents affecting data security are prevented and/or minimized in the best way possible. In case of an identified data breach, Enalyzer follows a specific data breach handling process. Enalyzer Support Team records all potential incidents and informs the CTO and Information Security Officer whenever relevant.

It is possible to report incidents to Enalyzer Support 24/7. Incident response will be initiated within business hours. Enalyzer monitors the software 24/7. If the software instance shuts down or does not respond, Enalyzer initiates corrective actions to ensure that the software returns to normal operation as soon as possible.

All incidents must be reported via a defined chain of command within Enalyzer. When an incident is reported, Enalyzer responds by default based on the priority set by the client. Critical incidents contain all of the following elements:

- Vital business operations are stopped due to system behaviour.
- System behaviour has severe business impact on vital operations and/or communications.
- System behaviour results in a severe breach of security and/or privacy.
- The client is unable to take effective mitigating actions to resolve the issue and thus needs Enalyzer Support Services.

All critical incidents are handled according to Enalyzer's incident handling process, and an incident report is produced and shared with the customer affected by the incident. Reporting critical incidents causes relevant Enalyzer employees and manager to be alerted in order to ensure efficient incident handling.

After a critical incident has been taken care of, a report will be submitted describing the incident, the findings of the investigations, and the responses undertaken. Any potential evidence for a crime investigation must be collected and saved during the incident handling and closure process.

Review of the event will be undertaken by the Information Security Officer together with relevant employees and managers to establish the cause of the incident, the efficiency of the response and to identify areas that require improvements. Lastly, recommended changes to systems, policies and procedures are documented and implemented as soon as possible.

Compliance with the role as Data Processor

It is the responsibility of Enalyzer A/S' management to ensure that all relevant legal and contractual requirements are identified and complied with correctly. Relevant requirements might be, e.g:

- The EU General Data Protection Regulation
- The Danish Data Protection Act
- Data Processor Agreements
- Enalyzer A/S' standard contract or other relevant sources

The existence of all necessary agreements, a comprehensive ISMS as well as other relevant documents, ensure compliance with all relevant legal and contractual requirements.

Enalyzer A/S is obliged to involve legal experts as needed in order to ensure compliance with law and regulations.

Furthermore, Enalyzer A/S' senior management reviews all Enalyzer A/S' security policies on a regular basis, including involving any relevant stakeholders. Enalyzer A/S' ISMS is regularly audited by an independent, external party, and on request the audit report is shared with all Enalyzer A/S' customers.

The EU General Data Protection Regulations (GDPR)
Enalyzer SaaS Solutions enable our customers to collect, process and report on data they collect from respondents or other data inputs. Enalyzer does not own the data our customers collect but develops and operates the software for our customers to utilise.

According to the EU General Data Protection Regulations and Danish additional regulation (The Danish Data Protection Act), Enalyzer A/S is the Data Processor, and the customer is the Data Controller.

Enalyzer A/S cooperates with legal experts in order to ensure that all legal requirements are identified and accommodated. Enalyzer A/S has also ensured relevant contracts with all key stakeholders (including customers, business partners, key suppliers etc.) in order to ensure compliance with law and regulations. In addition, Enalyzer A/S works together with the customers in order to ensure that the customers are aware of and comply with the relevant GDPR rules.

According to GDPR, compliance with the ISO 27001+2 standard ensures an appropriate security level. Besides compliance with the relevant ISO requirements, Enalyzer A/S ensures data privacy and data security on a contractual level.

Privacy and protection of personal data
As mentioned above, Enalyzer A/S is the customers' Data Processor, given that the customers are offered an IT service to which they can transfer and process data, and utilize it for further processing within their respective administrative assignments. Enalyzer A/S is not responsible for any data uploaded by the customers to their Enalyzer SaaS solutions. Based on the categories and confidentiality of the data entrusted to Enalyzer A/S by the customers, Enalyzer A/S must put into practice all necessary security measures required to ensure an appropriate level of security.

Below is described Enalyzer A/S' procedures of how Enalyzer A/S operates as Data Processor according to directions from the Data Controllers.

Data Protection Officer (DPO)
Enalyzer is affiliated with Johan Leonhard, Nyborg & Rørdam, to be DPO.

Data Protection Agreements

Enalyzer has Data Processor Agreements (DPA) in place with all our customers. These contracts outline Enalyzer's role and responsibilities as Data Processor, and the customers role and responsibilities as Data Controllers.

According to our standard DPA, Enalyzer keeps records of processing activities carried out on behalf of our customers. The records include:

- The name and contact information of the supplier, the subprocessors, and the customer.
- The categories of processing carried out by the supplier or any subprocessors on behalf of the customer.
- Transfer of personal data, if any, outside of EEA, including the name, if any, of the subprocessor and the concerned country or countries outside of EEA.
- Where possible, a general description of the technical and organisational security measures undertaken by the supplier to safeguard the personal data.

Access to the data in customer instances

In general, Enalyzer A/S does not access any customer instances unless specifically appointed by the customer. Enalyzer A/S does not collect data about the customer's customers (recipients), but can review the data, if our customers ask us to do it.

By request from our customer, Enalyzer can use recipients' personal data to:

- help and train the customer with their survey creation and reporting (customer support)
- investigate issues related to the customer's recipients (e.g. in case of reported errors)
- create survey projects for the customer, according to their instructions
- other relevant actions, on request from the customer

In short, Enalyzer A/S does not access data collected by its customers, unless specifically asked by the customer. Only specific employees at Enalyzer A/S are allowed to access customers' data upon request, and such employees are required to revoke the access immediately, when it is not required anymore. Enalyzer A/S logs and monitors the access to the customer instances to ensure no unauthorized persons are able to access any instance.

Important changes in relation to IT security

During the period covered by the report, there have been no significant changes in relation to IT security.

Customers' responsibilities (complementary controls at the customer)

The above description is based on the Enalyzer ISMS and other standard contractual clauses in place. This means that no account has been made for the agreements of individual customers.

Enalyzer expects the customer to handle the access control to the customer's own instance. Enalyzer grants the access to an appointed person working for the customer during onboarding, and afterwards it is the customer's responsibility to ensure that the access rights to their instance are appropriately controlled. The customer must have relevant access control restrictions in place in order to ensure the security of their Enalyzer instance.

The responsibility for the daily use of Enalyzer's platforms and customizations herein lies with the customer. Enalyzer A/S is not responsible for the customer's use of the software; it is the customer's own responsibility to ensure that the necessary internal security controls are in place, when using Enalyzer SaaS solutions for data collection and reporting. In general, Enalyzer recommends risk-based evaluations to take place when planning any changes to an Enalyzer instance: as the customer has the option

to modify their instance, the potential risks created by the modifications should always be assessed and limited.

Furthermore, Enalyzer does not take the responsibility regarding the data a customer collects and processes using their Enalyzer instance. As described above, Enalyzer does not access any customer instances, unless specifically asked by the customer, thus Enalyzer does not know, what kind of data the customer is collecting.

Enalyzer A/S applies the following control objectives and security measures from ISO27001 and 2

0. Risk Assessment and management
- 0.1. Assessment of security risks
- 0.2. Risk management

---

5. Information security policies
- 5.1. Management directions for information security

---

6. Organisering of information security
- 6.1. Internal organisation
- 6.2. Mobile devises and teleworking

---

7. Human resource security
- 7.1. Prior to employment
- 7.2. During employment
- 7.3. Termination or change of employment

---

8. Asset management
- 8.1. Responsibility for assets
- 8.3. Handling of media

---

9. Access control
- 9.1. Business requirements of access control
- 9.2. User access management
- 9.3. Users' responsibility

---

11. Physical and environmental security
** Limited responsibility**
- 11.1. Secure areas
- 11.2. Equipment

---

12. Operations security
** Limited responsibility**
- 12.1. Operational procedures and responsibilities
- 12.2. Protection from malware
- 12.3. Backup
- 12.4. Logging and monitoring
- 12.5. Operational software management

13. Communications security
** Limited responsibility**
- 13.1 Network security management

---

14. (Acquisition), development and maintenance of systems
- 14.1. Security requirements to the IT system
- 14.2. Security in development and auxiliary processes

---

15. Supplier relationships
- 15.1. Information security in supplier relationships
- 15.2. Supplier service delivery management

---

16. Information security incident management
- 16.1. Management of information security incidents and improvements

---

17. Information security aspects of business continuity management
- 17.1. Information security continuity
- 17.2. Redundancies

---

18. Compliance
- 18.1. Compliance with legal and contractual requirements

> ** Limited responsibility **
> Responsibility for compliance with the control objective is divided between Enalyzer A/S and the subcontractors Microsoft Azure.
>
> See description of controls in relation to covering the control risk, including how Enalyzer A/S continually supervises operations security and data security at Microsoft Azure.

Independent auditor's assurance report on the description of controls, their design and operating effectiveness

For the customers / users of Enalyzer SaaS solutions for data collection and reporting, and their auditors

Scope

We have been engaged to report on Enalyzer A/S' description in Chapter 2 (incl. Appendix 1), which is a description of the control environment in connection with the operations of Enalyzer SaaS solutions, see Data Processor Agreements with customers, throughout the period 1 October 2021 - 30 November 2022, as well as on the design and function of controls regarding the control objectives stated in the description.

We express our opinion with reasonable assurance.

The report is based on a partial approach, which means that the present report does not include the IT security controls and control activities related to the use of external business partners. The report does not include control or supervision of subcontractors in relation to operation activities. Enalyzer A/S' subcontractors are listed in the Data Processing Agreements with the customers

The scope of our report does not cover customer-specific conditions, and the report does not include the complementary controls and control activities conducted by the user company; see the description of the company in Chapter 2 under the section: Customers' responsibilities.

Enalyzer A/S' responsibility

Enalyzer A/S is responsible for the preparation of the description and accompanying assertion in Chapter 2 (including Appendix 1), 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, implementing and effectively operating 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 Enalyzer A/S' description and on the design and operation of controls related to the control objectives stated in the said description. We have conducted our engagement in accordance with ISAE 3402, Assurance Reports on Controls at a Service Organisation, issued by the IAASB. 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 and operate effectively.

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

Our procedures included testing the operating effectiveness of such controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description have been achieved. 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 Enalyzer A/S in Chapter 2 (including Appendix 1).

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

Limitations of controls at Enalyzer A/S

Enalyzer A/S' description is prepared to meet the common needs of a broad range of customers and their auditors 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 Enalyzer A/S may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at the service organisation may become inadequate or fail.

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 the control environment of Enalyzer A/S in relation to Enalyzer SaaS solutions, such as it was designed and implemented throughout the period 1 October 2021 - 30 November 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 throughout the period 1 October 2021 - 30 November 2022; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved in all material respects, had operated effectively throughout the period 1 October 2021 - 30 November 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 Enalyzer A/S' 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 customers i.e. the Data Controllers themselves have performed, when assessing compliance with the demands to the control environment as well as with the requirements of the General Data Protection Regulations.

Copenhagen, 13 December 2022

Beierholm
State-Authorized Public Accountants
CVR-number 32 89 54 68

Kim Larsen
State-authorized Public Accountant

Jesper Aaskov Pedersen
IT-auditor, Manager

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

We have structured our engagement in accordance with ISAE 3402 – Assurance Reports on Controls at a Service Organisation. For each control objective, we start with a brief summary of the control objective as described in the frame of reference ISO27001 and 2.

With respect to the period, we have tested whether Enalyzer A/S has complied with the control objectives throughout the period 1 October 2021 - 30 November 2022.

Below the grey field are three columns:

- The first column tells the activities Enalyzer A/S, according to their documentation, has put into practice in order to comply with the requirements.
- The second column tells how we have decided to test, whether facts tally with descriptions.
- The third column tells the findings of our test.

The Tests Performed

The tests performed in connection with establishing the control measures' design, implementation and operational efficiency are conducted using the methods described below:

Inspection	Reading of documents and reports containing information about execution of the control. This includes, inter alia, reading and deciding about reports and other documentation in order to asses, whether it can be expected that the design of specific control measures will be efficient, if implemented. Furthermore, it is assessed, whether control measures are monitored and controlled sufficiently and with appropriate intervals.
Enquiries	Enquiries to/interview with relevant staff at Enalyzer A/S. Enquiries have included how control measures are performed.
Observation	We have observed the performance of the control.
Repeating the control	Repeated the relevant control measure. We have repeated the performance of the control in order to verify that the control measure works as assumed.

Risk Assessment and Management

The risk assessment must identify and prioritise the risks based on the operation of SaaS Solutions. The findings are to contribute to the identification and prioritisation of management interventions and precautionary measures necessary to address relevant risks.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
Through a risk assessment, risks have been identified and prioritised. The SaaS Solutions defined in the description are used as basis for the assessment. The findings contribute to the identification and prioritisation of management interventions and precautionary measures necessary to address relevant risks.	We have requested and obtained the relevant material in connection with the audit of risk management. We have checked that regular risk assessments are carried out for operating activities in relation to business conditions and their development. We have checked that the risk assessment is deployed down through the company's organisation. We have checked that the company's exposure is managed on a current basis and that relevant adaptations of consequences and probabilities are made regularly.	No comments.

Information Security Policies

Management must prepare an information security policy that covers, among other things, management's security objectives, policies and overall action plan. The information security policy will be maintained, taking the current risk assessment into consideration.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
There is a written strategy covering, among other things, Management's security objectives, policies and overall action plan. The IT security policy and accompanying supporting policies are approved by the company's Management, and then deployed down through the company's organisation. The policy is available for all relevant employees. The policy is re-evaluated according to planned intervals.	We have obtained and audited Enalyzer A/S' latest IT security policy. During our audit, we checked that maintenance of the IT security policy is conducted on a regular basis. At the same time, we checked during our audit that the underlying supporting policies have been implemented. We have checked that the policy is approved and signed by the company's Supervisory and Executive Boards and made available for the employees on Enalyzer A/S' intranet.	No comments.

Organisation of Information Security

Management of the IT security must be established in the company. Organisational responsibility for the IT security must be placed with appropriate business procedures and instructions. The person responsible for IT security must, among other things, ensure compliance with security measures, including continuous updating of the overall risk assessment.

In relation to the use of mobile devices and/or teleworking, Management must decide and implement appropriate policies and security measures.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
Organisational responsibility for IT security has been placed, documented and implemented. The IT security has been coordinated across the company's organisation.	Through inspection and tests, we have ensured that the organisational responsibility for IT security is documented and implemented. We have checked that the IT security is deployed across the organisation in relation to SaaS solutions. By making interviews, we have checked that the person responsible for IT security knows his/her role and responsibilities.	No comments.
Risks in relation to use of mobile devices and teleworking have been identified.	We checked that formal policies exist in connection with the use of mobile devices and teleworking. On a test basis, we have inspected that the policy is implemented regarding employees using mobile devices. Regarding the use of teleworking at Enalyzer A/S, we have checked whether appropriate security measures have been implemented thus this area is covered in relation to the risk assessment of the area.	No comments.

Human Resource Security

It must be ensured that all new employees are aware of their specific responsibilities and roles in connection with the company's information security in order to minimise the risk of human errors, theft, fraud and abuse of the company's information assets.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
Based on the specified work processes and procedures, it is ensured that all new employees are informed of their specific responsibilities and roles in connection with their employment at Enalyzer A/S. This includes the framework laid down for the work and the IT security involved. Security responsibilities, if any, are determined and described in job descriptions and in the form of employment contract terms. The employees are familiar with their professional secrecy based on a signed employment contract and through Enalyzer A/S' HR policy.	We have verified that routines and procedures developed by Management in connection with start of employment and termination of employment have been adhered to. Based on random samples, we have tested whether the above routines and procedures have been complied with in connection with start of employment and termination of employment. Through interviews, we have checked that employees of significance to SaaS Solutions are familiar with their professional secrecy. We have examined the job descriptions and employment contracts of key employees and subsequently tested the awareness of the individual employee of their roles and related security responsibility. We have ensured that Enalyzer A/S' HR policy is easily accessible and has a section on terms for professional secrecy with respect to information obtained in connection with work conducted at Enalyzer A/S.	No comments.

Asset Management

Necessary protection of the company's information assets must be ensured and maintained, all the company's physical and functional assets related to information must be indentified, and a responsible owner appointed. The company must ensure that information assets related to SaaS Solutions have an appropriate level of protection.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
All information assets have been identified and an updated list of all significant assets has been established. An "owner" of all significant assets is appointed in connection with the operation of SaaS Solutions.	We have examined and checked the company's central IT register for significant IT entities in connection with the operation of SaaS Solutions. Through observations and control, we checked relations to central knowhow systems for the operation of SaaS Solutions. By observations and enquiries, we have checked that Enalyzer A/S complies with all material security measures for the area in accordance with the security standard.	No comments.
Procedures for dealing with destruction of data media are established.	We have: • Asked Management which procedures/ control activities are performed regarding data media. • On a sample basis gone through the procedures for destruction of data media.	No comments.

Access Control

Access to the company's systems, information and network must be controlled based on business and statutory requirements. Authorised users' access must be ensured and unauthorised access must be prevented.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
Documentation and updated directions exist for Enalyzer A/S' access control.	We have: • verified on a test basis that access control procedures exist and have been implemented; see Enalyzer A/S' directions. • by interviewing key staff and by inspection on a test basis, we have verified that access control for the operations environment comply with Enalyzer A/S' directions, and authorisations are granted according to agreement.	No comments.
A formal business procedure exists for granting and discontinuing user access. Granting and application of extended access rights are limited and monitored.	We have asked Management, whether access control procedures have been established at Enalyzer A/S. We have by inspection on a test basis verified: • that adequate authorisation systems are used in relation to access control at Enalyzer A/S. • that the formalised business procedures for granting and discontinuing user access have been implemented in Enalyzer A/S' systems, and registered users are subject to regular follow-up.	No comments.
Internal users' access rights are reviewed regularly according to a formalised business procedure.	By inspection on test basis, we have verified that a formalised business procedure exists for follow-up on authorisation control according to the directions, including: • that formal management follow-up is performed on registered users with ordinary rights every 6 months.	No comments.

The granting of access codes is controlled through a formalised and controlled process, which ensures, among other things, that standard passwords are changed.	We have asked Management whether procedures granting access code have been established at Enalyzer A/S. By inspection on a test basis, we have verified • that an automatic systems control takes place, when access codes are granted to check that passwords are changed after first login. • that standard passwords are changed in connection with imple-mentation of systems software, etc. • if this is not possible, that proce-dures ensure that standard pass-words are changed manually.	No comments.
Access to operating systems and networks are protected by passwords. Quality requirements have been specified for passwords, which must have a minimum length (8 characters) and re-quirements as to complexity, maximum duration.	We have asked Management whether procedures ensuring quality passwords in Enalyzer A/S are established. By inspection on a test basis, we have verified that appropriately programmed controls have been established to ensure quality passwords complying with the policies for: • minimum length of password • complexity of password	No comments.

Operations Security

Control objective: Operations procedures and areas of responsibility.

A correct and adequate running of the company's operating systems must be ensured. The risk of technology related crashes must be minimised. A certain degree of long-term planning is imperative in order to ensure sufficient capacity. A continuous capacity projection must be performed based on business expectations for growth and new activities and the capacity demands derived hereof.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
The operations procedures for business-critical systems are documented, and they are available to staff with work-related needs. Management has implemented policies and procedures to ensure satisfactory segregation of duties.	We have: • Asked Management whether all relevant operation procedures are documented. • In connection with our audit of the individual areas of operation verified on a test basis that documented procedures exist and that there is concordance between the documentation and the procedures actually performed. • Inspected users with administrative rights in order to verify that access is justified by work-related needs and does not compromise the segregation of duties.	No comments.
Management of operation environment is established in order to minimise the risk of technology related crashes. Continuous capacity projection is performed based on business expectations for growth and new activities and the capacity demands derived hereof.	We have: Asked Management about the procedures and control activities performed. On a test basis examined that the operation environment's consumption of resources is monitored and adapted to the expected and necessary capacity requirements.	No comments.

Control objective: Backup

To ensure the required accessibility to the company's information assets. Set procedures must be established for backup and for regular testing of the applicability of the copies.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
Backup is made of all the company's significant information assets, including, e.g. parameter setup and other operations-critical documentation, according to the specified directions.	We have: • asked Management about the procedures/ control activities performed. • examined backup procedures on a test basis to confirm that these are formally documented. • examined backup log on a test basis to confirm that backup has been completed successfully and that failed backup attempts are handled on a timely basis. • examined physical security (e.g. access limitations) for internal storage locations to confirm that backup is safely stored.	No comments.

Control objective: Logging and monitoring

To reveal unauthorised actions. Business-critical IT systems must be monitored, and security events must be registered. Logging must ensure that unwanted incidences are detected.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
Operating systems and network transactions or activities involving special risks are monitored. Abnormal conditions are examined and resolved on a timely basis. Enalyzer A/S logs, when internal users log off and on the systems. Only in the event of suspected or identified abuse of the systems, users are actively monitored.	We have: • asked Management about the procedures/ control activities performed, and have examined the system setup on servers and important network units as well as verified that parameters for logging have been set up, thus transactions made by users with extended rights are being logged. • checked on a test basis that logs from critical systems are subject to sufficient follow-up.	No comments.
A central monitoring tool is used which sends alerts, if known errors occur. If possible, it is monitored whether an error is about to occur in order to react proactively. Alerts are shown on the monitoring screen mounted in the project and operations department. Critical alerts are also sent by email and SMS. Status reports are sent by email from different systems. Some daily – others when incidents occur in the system. The operation function is responsible for checking these emails daily.	We have: • asked Management about the procedures/ control activities performed. • ensured that a monitoring tool is used and that this is available to all employees. • ensured that alerts are sent by email and SMS, if errors occur. • examined status reports. • ensured that an operations function is established and that this function checks reports on a daily basis.	No comments.

	Control objective: Managing operations software and managing vulnerability Ensuring establishment of appropriate procedures and controls for implementation and maintenance of operating systems.	
Enalyzer A/S' control procedures	**Auditor's test of controls**	**Test findings**
Changes in the operation environment comply with established procedures.	We have asked Management, whether procedures for patch management are established in Enalyzer A/S. By inspection on test basis, we have verified that • adequate procedures are applied, when controlled implementation of changes to the production environment of Enalyzer A/S is performed. • changes to Enalyzer A/S' operation environment comply with directions in force, including correct registration and documentation of applications about changes. On a test basis, we have inspected that the operating systems are updated in compliance with procedures in force and that current status is registered.	No comments.
Changes in existing user systems and operation environments comply with formalised procedures and processes.	We have asked Management, whether procedures for patch management are established in Enalyzer A/S. By inspection on test basis, we have verified that adequate procedures are applied for controlled implementation of changes in the production environments, including that demands to the patch management controls ensure that • applications for change are registered and described. • all changes are subject to formal approval before implementation • changes are subject to formal impact assessments. • fall-back plans are described. • systems affected by changes are identified. • documented test of changes is performed before implementation • documentation is updated reflecting the implemented changes in all material respects.	No comments.

(System acquisition), development and maintenance

Ensure that SaaS Solutions are managed using suitable IT security measures, including appropriate segregation of production and development environment.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
Enalyzer A/S has planned system development and maintenance activities based on the proprietary model for project management. The structure of the development organisation includes a central steering committee responsible for providing suitable work routines and accompanying control measures for the management. All changes meant to be put into operation in the production environment, must be approved by the development group for each of the SaaS Solutions. Software development must be placed in independent test environments.	We have: • asked Management, whether a general quality management model for managing software development is devised or does exist. • in connection with the audit checked the existence of procedures and routines for rolling out software changes. In connection with our audit, we have checked that internal education is conducted for staff working with development of SaaS Solutions and the accompanying development environment. During the process we tested, whether staff was trained in using quality model for development The control environment for the development platform is based on the same IT security structure as stated for the production environment. User management ensures suitable control measures in connection with managing the logical access control. We have checked that the different user groups are controlled at set intervals. The structure of the development organisation includes a central steering committee responsible for providing suitable work routines and accompanying control measures for the management. We have on a sample basis checked that all user activities are recorded and logged in the central database. The person responsible for IT security reviews the log database on a regular basis. We have checked the existence of procedures for segregation of the production environment and the environment for development and maintenance. We have on a sample basis tested that the production environment for development of SaaS Solutions is conducted from an independent IP segment.	No comments.

Supplier Relationships

External business partners are obliged to comply with the company's established framework for IT security level.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
Risks related to external business partners are identified, and security in third-party agreements is managed.	We have verified that in connection with the use of external business partners there are formal cooperation agreements. On a test basis, we have inspected that the cooperation agreements with external suppliers comply with the requirements about covering relevant security conditions in relation to the individual agreement.	No comments.
In case of changes with impact on the production environment, and where services from external suppliers are used, suppliers are selected by the IT Security Manager. Solely recognised suppliers are used.	We have asked Management about relevant procedures applied in connection with choosing external partners. We have ensured that appropriate procedures for managing cooperation with external partners are established. We have tested that key suppliers have updated and approved contracts.	No comments.
Monitoring must be conducted on a regular basis, including supervision of external business partners.	We have ensured that there are appropriate processes and procedures for ongoing monitoring of external suppliers. We have checked that ongoing supervision is conducted by means of independent auditor's reports.	No comments.

Information Security Incident Management

To achieve reporting of security incidents and weaknesses in the company's information processing systems in a way that allows for timely corrections.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
Security incidents are reported to Management as soon as possible, and the handling is performed in a consistent and efficient way.	We have asked Management whether procedures are established for reporting security incidents. We have verified that procedures and routines are developed for reporting and handling of security incidents, and that the reporting is submitted to the right places in the organisation; see the directions. We have verified that the responsibility for the handling of critical incidents is clearly delegated, and that the related routines ensure that security breaches are handled expediently, efficiently and methodically.	No comments.

Information Security Aspects of Business Continuity Management

Business continuity management is counteracting interruption in the company's business activities, protect critical information assets against the impact of a major crash or disaster, as well as ensure fast recovery.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
A consistent framework has been established for the company's contingency plans to ensure that all the plans are coherent and meet all security requirements and to determine the prioritisation of tests and maintenance.	We have asked Management whether business continuity management has been developed for SaaS Solutions at Enalyzer A/S. By inspection on a test basis, we have verified • that appropriate framework for preparation of business continuity management has been established • that contingency plans are prepared and implemented • that the plans include business continuity management across the organisation • that the plans include appropriate strategy and procedures for communication with the stakeholders of Enalyzer A/S. • that contingency plans are tested on a regular basis • that maintenance and reassessment of the total basis for business continuity management is undertaken on a regular basis.	No comments.

Compliance with the Role as Data Processor

Principles for processing personal data:

There is compliance with procedures and controls ensuring that collecting, processing and storing of personal data are performed in accordance with the agreement about processing personal data.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
A uniform framework is established in the form of standard contracts, Service Level Agreements, as well as Data Processor Agreements or the like, containing an outline of the basis for processing personal data.	We have controlled the existence of updated procedures in writing for processing personal data, and that the procedures include requirements to legal processing of personal data.	No comments.
Only the kind of processing of personal data included in directions from Data Controller is performed.	We have controlled that Management ensures that processing of personal data is solely performed in accordance with Directions. We have checked, using a sample consisting of a suitable number of processings that processing is performed according to directions.	No comments.
Management immediately informs the Data Controller, if Directions in the Data Processor's view is contrary to the General Data Protection Regulation or data protection provisions according to other EU legislation or the national legislation of the member states.	We have controlled that Management ensures that processing is reviewed and the existence of formalised procedures securing that processing of personal data is not performed against the EU General Data Protection Regulation or other legislation. We have controlled the existence of procedures for informing the Data Controller in cases, when processing of personal data is deemed to be against legislation. We have controlled that the Data Controller was informed in cases, when processing of personal data were deemed to be against legislation.	No comments.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
There are procedures in writing with requirements about storing and erasing of personal data in accordance with the agreement with the Data Controller. On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.	We have controlled that there are formalised procedures for storing and erasing of personal data in accordance with the agreement with the Data Controller. We have checked that the procedures are updated.	No comments.
According to the agreement with the Data Controller, when processing of personal data is finished, data is • Returned to the Data Controller, and/or • Erased, when erasing is not against other legislation.	We have controlled that there are formalised procedures for handling the Data Controllers' data, when processing of personal data is finished. We have controlled by random check using a suitable population of finished data processing cases that conducting the agreed erasing or returning of data is documented.	No comments.
There are procedures in writing including demands that personal data is only stored in accordance with the agreement with the Data Controller. On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.	We have controlled that there are formalised procedures ensuring that storing and processing of personal data are solely undertaken according to the Data Processor Agreements. We have checked that the procedures are updated. We have controlled on a sample basis, whether documentation exists that data processing is conducted in accordance with the Data Processor Agreement.	No comments.

The Data Processor's responsibility:

There is compliance with procedures and controls ensuring that solely approved sub-processors are used, and that the data processor ensures an adequate processing by follow-up on the sub-processors' technical and organisational security measures for protection of the Data Subjects' rights as well as follow-up on the processing of personal data.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
There are procedures in writing including demands to the Data Processor in relation to use of sub-processors, including demands about Sub-processor Agreements and Directions. On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.	We have controlled that there are formalised procedures regarding the use of sub-processors, including demands about Sub-processors Agreements and Directions. Inspected that procedures are updated.	No comments.
The Data Processor has a list of approved Sub-processors including the following information: • Name • CVR.no. • Address • Outline of the processing For processing personal data, the Data Processor solely uses Sub-processors, who are specifically or generally approved by the Data Controller.	We have controlled that the Data Processor has a total and updated list of approved sub-processors used. Inspected that the list as a minimum includes the required information about each sub-processor. Inspected using a sample of 3 Sub-processors from the Data Processor's list that it is documented that the Sub-processor's data processing is included in the Data Processor Agreements – or in other ways approved by the Data Controller.	No comments.
The Data Processor has placed the same data protection obligations on the Sub-processors as the obligations included in the Data Processor Agreement or similar document with the Data Controller.	We have controlled the existence of signed Sub-processor Agreements with all sub-processors used and included in the Data Processor's list. Inspected using a sample of 3 Sub-processor Agreements that the agreements include the same demands and obligations as stated in the Data Processor Agreements between the Data Controllers and the Data Processor.	No comments.

Assisting the Data Controller:

Procedures and controls are complied with to ensure that the Data Processor can assist the Data Controller in handing out, correcting, deleting or restricting processing of personal data as well as providing information about the processing of personal data to the Data Subjects.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
Written procedures exist which include a requirement that the Data Processor must assist the Data Controller in relation to the rights of Data Subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have controlled that formalised procedures are in place for the Data Processor's assistance to the Data Controller in relation to the rights of Data Subjects. Inspected that procedures are up to date.	No comments.
The Data Processor has established procedures in so far as this was agreed that enable timely assistance to the Data Controller in handing out, correcting, deleting or restricting processing as well as providing information about the processing of personal data to Data Subjects.	We have controlled that the procedures in place for assisting the Data Controller include detailed procedures for: • Handing out data; • Correcting data; • Deleting data; • Restricting the processing of personal data; • Providing information about the processing of personal data to Data Subjects. Inspected documentation that the systems and databases used support the performance of the said relevant detailed procedures.	No comments.

Records of processing activities:

There is compliance with procedures and controls ensuring that the Data Processor keeps records of processing personal data for which the Data Processor is responsible.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
There are records of the processing activities for each online service activity in combination with the relevant Data Controller.	We have controlled documentation displaying the existence of processing activities records for each online service activity combined with the relevant Data Controller.	No comments.
Assessment is made on an on-going basis – and at least once a year – that the records are updated and correct.	We have controlled the documentation disclosing that the records of the processing activities for each Data Controller are updated and correct.	No comments.

Reporting breaches of personal data security to the Supervisory Authority (the Danish Data Protection Agency):

There is compliance with procedures and controls ensuring that any security breaches are managed in accordance with the entered Data Processor Agreement.

Enalyzer A/S' control procedures	Auditor's test of controls	Test findings
There are procedures in writing - updated at least once a year – describing how to manage personal data security breaches, including timely communication to the Data Controller.	We have controlled the existence of updated procedures in writing regarding managing personal data security breaches, including description of timely communication to the Data Controller.	No comments.
Data Processor ensures recording of all personal data security breaches.	We have controlled documentation disclosing that all personal data security breaches are recorded at the Data Processor.	No comments.
Management has ensured that all personal data security breaches are timely and sufficiently communicated to the Data Controller, including personal data security breaches occurred at Data Processors used as subcontractors.	We have controlled documentation displaying that Management has ensured that all personal data security breaches are timely and sufficiently communicated to the Data Controller, including personal data security breaches occurred at Data Processors used as subcontractors.	No comments.