MAY 2018

ENALYZER A/S

ISAE 3402 TYPE 1 ASSURANCE REPORT

Independent auditor's report on coverage of the technical and organizational measures related to the operation of Enalyzers SaaS solution for datacollection and reporting. Delivered as self-administered web applications or as a outsourced consulting project.

Beierholm
Statsautoriseret Revisionspartnerselskab
Knud Højgaards Vej 9
2860 Søborg
CVR-nr. 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

BEIERHOLM
VI SKABER BALANCE

Structure of the Assurance Report

Chapter 1:

Letter of Representation.

Chapter 2:

Description of of the technical and organizational measures for the operation of SaaS solution.

Chapter 3:

Independent Auditor's Assurance Report on the description of the technical and organizational measures, their design and operating effectiveness.

CHAPTER 1:

Letter of Representation

This description in Chapter 2 incl. Appendix 1 of Enalyzer A/S' technical and organizational measures has been prepared for customers, who have used or plan to use Enalyzer SaaS solution, and their auditors, who have sufficient understanding to consider the description, along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatement in their financial statements. Enalyzer A/S hereby confirms that

(A) The description in Chapter 2 incl. Appendix 1 gives a true and fair description of Enalyzer A/S' technical and organizational measures in relation to Enalyzer SaaS solution as at 24 May 2018. The criteria for this assertion are that this description:

(i) gives an account of how the controls were designed and implemented, including:
- the types of services delivered, when relevant
- the processes in both IT and manual systems that are used to manage the technical and organizational measures
- relevant control objectives and control procedures designed to achieve these goals
- control procedures that we have assumed – with reference to the system's design – would be implemented by the user companies and which, if necessary to fulfil the control objectives mentioned in the description, have been identified in the description together with the specific control objectives that we cannot fulfil ourselves
- other aspects of our control environment, risk assessment process, information system and communication, control activities and monitoring controls that have been relevant for the technical and organizational measures

(ii) does not omit or misrepresent information that is 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 system that each individual customer may consider important in their own particular environment.

(B) The controls related to the control objectives stated in the accompanying description were suitably designed as at 24 May 2018. The criteria for this assertion are that:

(i) the risks that threatened 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 these control objectives.

(C) 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, the basis for hosting activities and services regarding the technical and organizational measures. The criteria for this basis are:

(i) Enalyzer – Data Processing Agreement on Microsoft Azure
(ii) Enalyzer – Data Processing Agreement on Itadel Hosting
(iii) ISMS handbook (IT security handbpook) as at 24.05.2018

Copenhagen, 28 May 2018

Jakob Roed, Founder & Co-CEO **Steen Ødegaard, Founder & CTO**

Enalyzer A/S, Refshalevej 147, DK-1432 Copenhagen K, CVR: 24761618

CHAPTER 2:

Description of the technical and organizational measures for the Operation of Enalyzer SaaS solution

Introduction

The purpose of the current description is to offer information to Enalyzer A/S' customers and their auditors concerning the relevant ISO 27001 requirements and controls implemented in Enalyzer A/S' security policy. ISO 27001 is an information security standard published by the International Organization for Standardization (ISO).

The purpose of this description is exposure of the technical and organizational measures implemented in connection with the operation of the SaaS solution for datacollection and reporting. Delivered as self-administered web applications or as a outsourced consulting project. As a supplement to the description, is added an independent paragraph (accordance with the role as data handler), including a description of essential requirements regarding the role as data handler.

Furthermore, the description provides information about the controls applied for the operation of Enalyzer A/S' SaaS solution as of 24 May 2018.

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 SaaS solution, for its 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.

Both self-administered surveys on Enalyzers survey platforms, and when projects are outsourced to Enalyzer (mainly fully executed on Enalyzers own platforms), normally addresses surveys within human resource, 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 solution, and the relevant parts of Enalyzer's Data Processing Agreement with its customers.

Business strategy / IT security strategy

Enalyzer software is designed to be secure, so that neither the customers nor the company is 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 solution
- 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 27001:2013 as its starting point, and has used the ISO method to implement the relevant security measures within the following areas:

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

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

- Data processing activities conducted on behalf of the customers (item 3 and 7 in the DPA)
- Data breach monitoring and reporting (item 6 in the DPA)

The implemented security measures at Enalyzer are described in appendix 1.

Enalyzer A/S' organization and organization of IT security

Enalyzer employs approximately 50 employees and has a flat organizational structure. The CEO 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 Committee acting on behalf of the management and taking the responsibility of security issues. In 2018, the board consisted of:

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

The Information Security Committee is chaired by Chief Security Officer Steen Ødegaard.
Karin Absalonsen, 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.

Therefore, Enalyzer 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 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 with known international standards for IT security. The ISO 27001:2013 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 named an Information Security Board to handle security related work in Enalyzer. The Information Security Board consists of the Information Security Officer and a minimum of two members of the senior management group at all times.

The structure of 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. Enalyzer makes regular improvements to policies, procedures and operations in order to ensure that both our customers' requirements and relevant legislation are complied with.

Enalyzer's IT security focus is on everyday operations, and 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 Enalyzer ISMS. Enalyzer protects its information and solely allows use and access for 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. In 2018, the training concentrated 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.

The Information Security Board is responsible for the regular security updates 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 the 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 information asset handling.

As 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 a relevant 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 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 performing 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 it 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 helps Enalyzer to concentrate on the everyday operations of the SaaS solution for datacollection and reporting. Delivered as self-administered web applications or as a outsourced consulting project. Services by Microsoft Azure and Itadel Hosting include server virtualisation, network, power and rack space for the physical servers.

Microsoft Azure and Itadel Hosting are compliant with ISO 27001 security framework and are being audited regularly. Audit reports are submitted to Enalyzer A/S for review annually.

According to the latest audit report of Microsoft Azure and Itadel Hosting's physical and environmental security, the mentioned suppliers applied the following ISO 27001 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 and Itadel Hosting 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 solution; the servers located at Enalyzer's office are used for testing purposes. 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 operational 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 data and 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 in order 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 production 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. The network is divided into a number of logical network sites, with each site representing differing trust levels, each protected by a defend logical security perimeter. This perimeter is created by setting firewalls between the logical sites and interconnecting them in such a way that they control access and information flow between the sites.

A graduated set of controls are applied in the different logical network sites to further segregate the network security environments, e.g. publicly accessible systems, internal networks, and critical assets. This gateway is configured to filter traffic between these domains and to block unauthorized access in accordance with the organization's access control policy.

Backup and recovery
The backup policy ensures appropriate protection against loss of data and ensures the ability to restore production 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 are 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 are stored in an encrypted format while being located on Enalyzer's SaaS solution.

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 conducts reviews about technical vulnerabilities of information systems being used in Enalyzer. In case of severe vulnerabilities being 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 solution is a true multi-tenant solution. Each tenant's data is isolated and remains invisible to other tenants. To ensure this, the solution checks authorization on all request for data. The authorization mechanism is a main part of the security architecture.

This affords us the ability to adapt the solution better 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 from unauthorized access.

Enalyzer has established controls to safeguard the confidentiality and integrity of data passing over public networks or over 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 in earlier, the Enalyzer network setup is divided into a number of logical network sites, with each site representing differing trust levels, each protected by a defence. A set of controls are applied in the different logical network sites to further segregate the network security environments, e.g. publicly accessible systems, internal networks, and critical assets.

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 solution. For key suppliers, who have access to customer instances, it is mandatory to have GDPR-compliant sub-data processing 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 defines the following four categories of supplier relationships:

1. Suppliers of non-data processing goods and services
2. Suppliers of software utilised to deliver services supporting Enalyzer's core operations
3. Software development partners (software development companies helping Enalyzer A/S by coding or maintaining Enalyzer SaaS solution or separate parts thereof)
4. Software vendors (suppliers of software components used when operating Enalyzer SaaS solution)

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 followed after a security incident.
All employees at Enalyzer are familiar with the procedures for reporting different types of incidents and weaknesses, which can influence operational 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 keeps. 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 (management system for managing information security) 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'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 software enables 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 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 to 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 IT service. Based on the categories and confidentiality of the data entrusted to Enalyzer A/S by the customers, Enalyzer A/S must put all necessary security measures required to ensure an appropriate level of security into practice.

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

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

- The name and contact information of the supplier, the sub-data processors, and the customer.
- The categories of processing carried out by the supplier or any sub-data processors on behalf of the customer.
- Transfer of personal data, if any, outside of EEA, including the name, if any, of the sub-data processor 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.

At the request of the customer, Enalyzer A/S must make the list available to the customer or to the Danish Data Protection Agency (Datatilsynet) at any time.

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 campaign creation and reporting (customer support)
- investigate issues related to the customer's recipients (e.g. in case of reported errors)
- create marketing communication campaigns to the customer, according to their instructions
- other relevant actions, on request from the customer

In short, Enalyzer A/S does not access the 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 ditch 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 is able to access any instance.

Important changes in relation to IT security

Enalyzer's IT-security strategy, the relevant framework and the ISMS have undergone a large-scale change during 2018 as a part of our security focus. The implementation of the latest version has caused the establishment of a wide variety of new security controls during the process. Enalyzer's aim has been that all the security controls presented above were implemented by the 24th of May 2018.

Enalyzer A/S will continue to work with information security in 2018 with focus on the relevant legislation, further improving the current controls and improving security controls around software development practices. We are committed to a new audit by an external auditor in a year, and will share the audit report, when it has been made available to us.

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 solution for datacollection 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 recommends only to collect and use data that are relevant for creation of automated marketing communication.

APPENDIX 1:

Enalyzer A/S applies the following control objectives and security measures from ISO27002:2013

5. Information Security Policies

5.1. Management directions for information security

6. Organisation of Information Security

6.1. Internal organisation
6.2. Mobile devices 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. Media handling

9. Access Control

9.1. Business requirements of access control
9.2. User access management:
9.3. Users' responsibility

12. Operations Security

12.1. Operational procedures and responsibilities
12.2. Protection from malware
12.3. Backup
12.4. Logging and monitoring
12.5. Control of operational software
12.6. Technical vulnerability management

13. Communications Security

13.1. Network security management
13.2. Information transfer

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

18. Compliance

18.1 Compliance with legal and contractual requirements

CHAPTER 2:

Independent Auditor's Assurance Report on the Description of the Technical and Organizational Measures and their Design

For the customers / users of Enalyzer SaaS solution 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 technical and organizational measures conducted in connection with Enalyzer SaaS solution as of 24 May 2018 and on the design of the controls mentioned in the description.

We have not conducted any procedures in relation to the operating functionality of the controls mentioned in the description, and thus express no opinion in this regard.

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. Enalyzer A/S uses external partners in the following areas:

- Hosting activities and operational tasks from Microsoft Azure and Itadel Hosting. The solutions cover the following categories: SaaS (Software as a Service), PaaS (Platform as Service) and IaaS (Infrastructure as a Service).

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: Complementary controls.

The current IT security strategy with accompanying framework and ISMS (IT security handbook) were devised and implemented during the period February - May 2018. The development of IT security has led to further control measures being devised and implemented during the implementation period.

It has been our underlying basis, that the complete IT security framework and accompanying IT security controls should be in effect from the middle of May 2018. All direct controls carried out once, twice or four times a year have, as far as it has been possible, been conducted within the said period and until 24nd of May 2018.

Enalyzer A/S' responsibility

Enalyzer A/S is responsible for the preparation of the description and accompanying assertions in Chapter 2 (incl. appendix 1), including the completeness, accuracy and method of presentation of the description and assertion; for providing Enalyzer SaaS solution as 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 on Enalyzer A/S' description and on the design and operation of controls related to the control objectives stated in that description based on our procedures. We 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 are appropriately designed in all material respects.

An assurance engagement to report on the description and design of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of the technical and organizational measures related to Enalyzer SaaS solution as well as for the design of the 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. 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 in Chapter 2 (including appendix 1) by Enalyzer A/S.

As stated above, we have not conducted procedures related to the operating functionality of the controls included in the description, and thus we express no opinion in this regard.

Beierholm believes 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 thus may not include every aspect of the system that each individual customer may consider important in their own particular environment. In addition, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions.

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 technical and organizational measures of Enalyzer A/S for Enalyzer SaaS solution, such as they were designed and implemented at 24 May 2018 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 at 24 May 2018.

Please, note that there may be specific circumstances in relation to the individual customers, which mean that the general conclusion is not fully adequate. If it has been agreed between the customer

and Enalyzer A/S that a specific statement should be prepared regarding the customer's contract, the conditions will appear from hereof.

Intended users and purpose

This report and the description are intended only for Enalyzer A/S' customers and their auditors, who have sufficient understanding to consider them, along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatement in their financial statements.

Copenhagen, 28 May 2018

Beierholm
Statsautoriseret Revisionspartnerselskab

Kim Larsen
State-authorized Public Accountant

Jesper Aaskov Pedersen
IT-auditor, Manager