BEIERHOLM
VI SKABER BALANCE

OCTOBER 2020

CYBERPILOT APS

ISAE 3402 TYPE 1 ASSURANCE REPORT

CVR 37435392

Independent auditor's report on the control environment related to the operation of "Software as a Service" (SaaS) solutions.

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

Beierholm
State Authorized Public Accountants
Copenhagen
Knud Højgaards Vej 9
DK-2860 Søborg
Denmark
CVR no. DK 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

Structure of the Assurance Report

Chapter 1:

Letter of Representation.

Chapter 2:

Description of the control environment related to the operation of SaaS solutions.

Chapter 3:

Independent Auditor's Assurance Report on the description of the controls and their design.

CHAPTER 1:

Letter of Representation

CyberPilot ApS processes personal data on behalf of Data Controllers according to Data Processor Agreements regarding operation of CyberPilot ApS' SaaS solutions.

The accompanying description has been prepared for the use of customers and their auditors, who have used CyberPilot ApS' 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. CyberPilot ApS hereby confirms that

(A) The accompanying description, Chapter 2 gives a true and fair description of CyberPilot ApS' control environment in relation to operations of SaaS solutions as of 29 October 2020. The criteria for this assertion are that the following description:

(i) Gives an account of how the controls were designed and implemented, including:

- **The types of services delivered, including the type of personal data processed**
- **The processes in both IT and manual systems that are used to initiate, record, process and, if necessary, correct, erase and limit the processing of personal data**
- **The processes utilized to secure that the performed data processing was conducted according to contract, directions or agreements with the customer i.e. the Data Controller**
- **The processes securing that the persons authorized to process personal data have pledged themselves to secrecy or are subject to relevant statutory confidentiality**
- **The processes securing that - at the Data Controller's discretion - all personal data are erased or returned to the Data Controller, when the data processing is finished, unless personal data must be stored according to law or regulation**
- **The processes supporting the Data Controller's ability to report to the Supervisory Authority as well as inform the Data Subjects in the event of personal security breaches**
- **The processes ensuring appropriate technical and organizational security measures for processing personal data taking into consideration the risks connected to processing, in particular accidental or illegal actions causing destruction, loss, change, unauthorized forwarding of or access to personal data that is transmitted, stored or in other ways processed**
- **Control procedures, which we assume – with reference to the limitations of the 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 regarding CyberPilot ApS' SaaS solutions in the processing of personal data in connection with performance of the audit assignment.

(iii) Does not omit or misrepresent information relevant for the scope of the controls described, taking into consideration that the description has been prepared to meet the common needs of a broad range of customers and their auditors, and may not, therefore, include every aspect of the control system that each individual customer may consider important in their own particular environment.

(B) **The controls related to the control objectives stated in the accompanying description were suitably designed as of 29 October 2020. 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**

c) **Appropriate technical and organizational security measures are established in order to honour the agreements with the Data Controllers, generally accepted data processor 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 have been prepared based on compliance with CyberPilot ApS' standard agreement. The criteria for this basis are:**

(i) **CyberPilot Information Security Statement V.1**

(ii) **CyberPilot Information Security Manual V.1**

(iii) **Data Processor Agreement (appendix to terms and conditions of the agreement)**

Aarhus, 30 October 2020

Rasmus Hangaard Vinge, CEO
CyberPilot ApS, Fredens Torv 8 B, 1. sal, DK-8000 Aarhus C, CVR 37425392

Chapter 2:

Description of the control environment in connection with operation of SaaS solutions

Scope of this description

The purpose of the present description is to inform customers and their auditors of the requirements of ISAE 3402, which is the international standard for Assurance Reports on Controls at a Service Organisation.

The scope of this description includes the technical and organizational security measures implemented in connection with the operation of the following security services managed by CyberPilot ApS:

- **Awareness training**
- **Phishing training**
- **Vulnerability scanning**
- **Log management**

The services are supplied as "Software as a Service" (SaaS) solutions.

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

Description of CyberPilot ApS

CyberPilot is an information security company that offers, develops, operates and markets managed cyber security and compliance services to companies and organizations. The services are offered as Software-as-a-Service solutions to our clients. We both develop our own applications and leverage third party applications to deliver high quality and value-creating services to our customers.
The services include:

- **Awareness training – e-learning courses on information security and GDPR-compliance delivered through the CyberPilot e-learning platform**
- **Phishing training – phishing-simulations including access to web-plugin with all relevant data about the phishing-campaigns**
- **Vulnerability scanning – scanning and reporting of vulnerabilities performed by CyberPilot and delivered through web-plugin.**
- **Log management - collection and analysis of log files from customers' IT assets and alerts and reports delivered through web plugin.**

The core activity in CyberPilot is the development and operation of these CyberPilot services.

CyberPilot operates 24/7/365 in hosted IT environments provided by suppliers.

CyberPilot Information security

CyberPilot follows the principles of ISO27001+2. Processes and working methods based on ISO27001+2 are in place to ensure high standards regarding confidentially, integrity and availability of the product and services provided to customers and partners.

IT security statement and strategy

CyberPilot's overall framework and strategic objectives related to information security is defined in CyberPilot's information security statement. This statement is drawn up by the board andis reviewed annually.

By following the information security statement put forward by the board, the management prioritizes information security as an important part of the company's business culture.

The overall objectives for CyberPilot's information security are:

- **CyberPilot works with information security to secure confidentiality, integrity and availability of CyberPilot's assets, systems and data.**
- **CYBERPILOT must comply with ISO 27001+2:2017. This will be documented through an ISAE 3402 report.**
- **A risk-based approach must be applied to identify and manage the relevant risks related to CyberPilot information security. CyberPilot must therefore implement a continuous process of risk assessment.**
- **An information security manual must be developed and continuously reviewed and updated. The information security manual should include descriptions of the measures implemented to manage the information security of CyberPilot and should include references to further relevant policies, working procedures and work instructions related to the information security of CyberPilot.**
- **The information security statement and the objectives will be reviewed on an annual basis.**

Organization of information security

The steering managing and prioritization of CyberPilot's activities related to information security iscarried out by the person responsible for information security – Rasmus Hangaard Vinge, CEO of CyberPilot.

The CEO of CyberPilot has the day-to-day responsibility for IT security, and it is thus ensured that the overall requirements and framework for IT security are maintained.

Other employees will be involved in the activities when considered necessary.

The rules for the employees regarding CyberPilot's usage of IT is defined in specific guidelines. All employees are subject to these rules, which cover:

- **Confidentiality**
- **Access codes**
- **Etc.**

Human Resource Security

CyberPilot acknowledges the fact that its employees play an important role in the information security of the company. CyberPilot has therefore implemented measures to ensure processes concerning information security prior to, during and after employment. The CEO and direct line managers have specified responsibilities to perform the relevant tasks set out in the specific guidelines.

All individuals employed by CyberPilot are subject to screening prior to employment.

Employees are furthermore contractually informed and obligated to follow the rules and guidelines set out by the management of CyberPilot regarding information security.

During the employment at CyberPilot, individual employees are obligated to participate in the information security awareness training program.

And in the case of termination of employment, CyberPilot has a defined procedure to ensure that the relevant IT equipment is returned, and user access rights are closed or in other ways handled.

Asset Management

CyberPilot has limited ownership of physical assets. Trusted suppliers primarily deliver operating servers and IT infrastructure. CyberPilot has an interest in ensuring that all assets are securely operated. CyberPilot has therefore assigned ownership of each of assets to specific employees within CyberPilot.

Ownership of an assets means that the specified employee has the responsibility of ensuring that the asset is implemented and operated with respect to the overall objectives for the information security of CyberPilot.

Ownership of asset can be delegated from the management to relevant employees.

Ownership of hardware and software assets is documented, reviewed and adjusted as part of the yearly risk assessment process.

Access Control

Physical and logical access control is of priority in CyberPilot. There is a clear motivation to control access to CyberPilot's assets and limit it to the people, who have a clear need-to-know and carry out tasks related to the access given.

CyberPilot's overall guidelines to controlling the access to assets are documented in the access control policy.

Access control is focused around 1) access to the CyberPilot IT infrastructure and 2) access within the CyberPilot services:

1) IT infrastructure: CyberPilot is dependent on suppliers for the IT infrastructure and sets demands for the suppliers and sets demands for the suppliers about access management and user rights.

2) Within CyberPilot services: For all services, a logical layered access control scheme is implemented, which ensures that the relevant user categories (both internal and external) have the appropriate access to the CyberPilot system and underlying data.

Physical and environmental security

CyberPilot's offices are located in Aarhus, Denmark.

The IT infrastructure (servers) from where the CyberPilot services is operated is physically located in data centers operated by selected suppliers. CyberPilot has entered into an agreement with these suppliers, who are responsible for the physical security of the servers.

Employees are instructed to follow guidelines related to the daily work routines.

Operation Security

CyberPilot has implemented security measures, which require operational attention. The daily task of operation is shared between tasks handled by CyberPilot and tasks handled by external suppliers.

See below for a description of the operational measures:

Firewall
All traffic to the CyberPilot servers is routed through firewalls.

Backup
To prevent data loss, CyberPilot has implemented backup procedures for the individual services.

The backup is also tested continuously to make sure that restore is possible if needed.

Patch management procedures
CyberPilot has defined clear processes for patch management to ensure that applications and systems are continuously kept up to date which significantly decreases the risk of vulnerabilities on the systems.

Monitoring
The CyberPilot servers are monitored to ensure continuous and stabile operation.

The monitoring combined with alerts ensures that any disruption of the operation of the servers can be quickly identified and handled.

Log management
Relevant security logs from the servers are collected and the logs are analyzed using rules and algorithms. Alerts are raised in case of suspicious activity.

The log management makes it possible to identify and mitigate security incidents.

Technical vulnerability management
To identify technical vulnerabilities in the CyberPilot IT infrastructure, continuous testing is performed. This ensures that any new vulnerabilities, misconfigurations etc. are identified and managed accordingly.

Description of development, test and production environment
CyberPilot has separate environments for the development, test and production. The purpose of the separating development, test and production environments is to ensure a continuous development of the applications while making sure that only changes which have been appropriately tested are launched into the production environment.

Network security management

CyberPilot uses primarily two networks, one for workstations and a separate network of Cloud IAAS.

CyberPilot's use of the CP network is limited to workstations and shared office resources. The employees' use of the network is regulated in the IT-usage guidelines.

The cloud IAAS-network is operated by AWS and is strictly used for operation of the CyberPilot servers. This means that there are several security measures implemented on the network.

Networks are therefore segregated by default. One network for employees and workstations and one network for the CP-services.

System acquisition, development and maintenance

There is a strong focus on securing that the development of the services meets the requirements of CyberPilot's customers and partners.

CyberPilot has established separate environments for the development, test and production of the services.

The overall goal is to ensure that updates and new developments meet high standards by following development, testing and approving processes before release and at the same time maintain a flexible approach, which enables CyberPilot to constantly develop the services.

Supplier relationships

CyberPilot is dependent on a few key suppliers in our daily operation and development of the CyberPilot services.

All supplier relationships are governed through formal agreements contracts.

Risks and relevant security controls related to specific assets/suppliers are (as a minimum) discussed as part of the yearly risk assessment.

To ensure that information security is evaluated and prioritized before entering into agreements with new suppliers, CyberPilot has defined specific policies for selection of suppliers.

Agreements with key suppliers are reviewed annually.

Information security incident management

At CyberPilot we have prepared ourselves for security incidents by delegating the responsibility of the management of security incidents to the various organisational levels.

Furthermore, all employees are instructed to report any security incidents to ensure that all incidents are handled quickly and effectively.

All security incidents are logged to ensure that incidents are categorized, handled appropriately and closed when dealt with. The purpose of this is also to ensure that new controls are implemented, and that the organisation can 'learn' from past incidents and avoid similar incidents in the future.

Information security aspects of business continuity management

CyberPilot has taken relevant measures to ensure business continuity. Plans define the actions needed to be taken in the case of security incidents that are affecting the CP-services. The main priority is to re-establish service of the production environments.

Measures have been implemented to ensure that the production environment is protected, that relevant redundancies are in place and that service can be restored in cases of hardware and/or software failures.

Compliance with the role as Data Processor

CyberPilot works with the legal advisors to ensure that the company is constantly aware of laws and regulations that can affect the operation of the company. The main areas for CyberPilot regarding compliance are:

- Contracts with partners and end-users
- Personal data protection law i.e. GDPR

The identification of compliance risk is included in the overall risk assessment process of CyberPilot.

CyberPilot ensures that all legal contracts with partners and customers are developed in close collaboration with our legal advisors.

CyberPilot also works to ensure that requirements in contracts i.e. obligations to perform independent reviews on CyberPilot's information security are met.

Furthermore, CyberPilot is continuously working to ensure that CyberPilot services follow the relevant regulations regarding accounting standards and personal data protection.

CHAPTER 2:

Independent Auditor's Assurance Report on the controls and their design

For the customers / users of CyberPilot ApS' SaaS solutions and their auditors

Scope

We have been engaged to report on CyberPilot ApS' description in Chapter 2 which is a description of the control environment related to the operation of SaaS solutions as of 29 Oktober 2020 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. The report does not include control or supervision of subcontractors in relation to operation activities. CyberPilot ApS' subcontractors are listed in the Data Processing Agreements with the customers.

CyberPilot ApS' responsibility

CyberPilot ApS is responsible for the preparation of the description and accompanying assertions in Chapter 2, including the completeness, accuracy and method of presentation of the description and assertion; for providing SaaS solutions 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 CyberPilot ApS' description and on the design 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 the SaaS solutions 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 by CyberPilot ApS. 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 CyberPilot ApS

CyberPilot ApS' 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 control environment of CyberPilot ApS' SaaS solutions, such as it was designed and implemented as of 29 October 2020 in all material respects; and

b) The controls related to the control objectives stated in the description were in all material respects suitably designed as of 29 October 2020.

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 CyberPilot ApS 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 CyberPilot ApS' customers and their auditors, who have sufficient understanding to consider them, along with other information, including information about the customers' own control measures, which the customers as Data Controllers have performed themselves, when assessing whether the control environment is appropriate, and there is compliance with the requirements of General Data Protection Regulation.

Copenhagen, 30 October 2020

Beierholm
State Authorized Public Accountants
CVR-no. 32 89 54 68

Kim Larsen
State-authorized Public Accountant

Jesper Aaskov Pedersen
IT-auditor, Manager