*OCTOBER 2018*

# FRONTSAFE A/S

CVR-number 29631123

## ISAE 3402 TYPE 2 ASSURANCE REPORT

Independent Auditor's Report on coverage of the technical and organizational security measures in relation to operation of Cloud Backup.

In addition, a control description has been provided in relation to the General Data Protection Regulation and Frontsafe A/S' role as a data processor.

**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 technical and organizational security measures for the operation of Cloud Backup.

## Chapter 3:

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

## Chapter 4:

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

CHAPTER 1:

# Letter of Representation

This description in Chapter 2 of Frontsafe A/S' technical and organizational security measures as well as the role as data processor has been prepared for customers, who have used or plan to use Frontsafe A/S' Cloud Backup, 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. Frontsafe A/S hereby confirms that

(A) The description in Chapter 2 gives a true and fair description of the technical and organizational security measures of Frontsafe A/S' Cloud Backup throughout the period 1 October 2017 - 30 September 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 security 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 entities 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 security measures

(ii) includes relevant information about changes in Frontsafe A/S' technical and organizational security measures made during the period 1 October 2017 - 30 September 2018

(iii) 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 his 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 2017 - 30 September 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, 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 2017 - 30 September 2018.

(C) The accompanying description and the related criteria for fulfilling the control objectives and controls, Chapter 2, have been prepared based on compliance with Frontsafe A/S' standard agreement, the basis for Cloud Backup and services regarding the technical and organizational security measures. The criteria for this basis are:

(i) Service Level Agreement for Cloud Backup Version 7 – 2016

(ii) General conditions for Cloud Backup Version 7 - 2016

Høje Taastrup, 26 October 2018

Einar Boije, General Manager

Reda Al Karabalaie, Technical Partner Manager

CHAPTER 2:

# Frontsafe A/S' description of technical and organizational security measures for the operation of Cloud Backup

## Introduction

The purpose of this description is to provide Frontsafe A/S' customers and their auditors with information regarding the requirements of ISAE 3402, which is the international auditing standard for assurance reports on controls at service organisations.

In addition, this description is coverage of the technical and organizational security measures implemented in connection with the operation of Cloud Backup.

As a supplement to the description below 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.

Furthermore, the description also provides information on the controls used for the operation of Frontsafe A/S' Cloud Backup during the period 1 May 2017 – 30 September 2018.

## Description of Frontsafe A/S and scope of services

Frontsafe A/S is part of j2 Global, which is one of the world's biggest service supplier within Cloud backup. There is still Danish support, operations and sales focusing on building a well-functioning partner strategy.

Frontsafe A/S has it domicile in Taastrup and data centres situated in Viby J.

Frontsafe A/S is a specialised and focused supplier of Cloud backup for businesses on the Danish market. Frontsafe A/S provides its Cloud Backup solutions to thousands of customers, whose more than 13.000 servers are secured on a daily basis through reliable service and support with more than 10 years' experience of operating Storage and Backup.

In recent years, Frontsafe A/S has developed knowhow and competences, and today offers the market backup-related services, including VEEAM Cloud Repository, which together with IBM Spectrum Protect is leading on the world market for Backup, both as a service and On-Premise solutions.

## Business strategy/IT security strategy

At Frontsafe A/S, our goal is continuously reducing the impact that the operation of our services has on the environment. We have set a specific goal, which is to reduce the energy consumption per stored GB by at least 5 per cent each year. Accordingly, Frontsafe Purchasing Department is required to ensure that the acquisitions of hardware and software for the operations have a positive impact on the fulfilment of our goal. The following figures show the savings in percentages from year to year in KW power consumption per stored GB in the Frontsafe production over the last seven years of operation:

KW/GB savings in percent in relation to the previous year

2011: 34.66%
2012: 24.63%
2013: 5.79%
2014: 22,86%

2015: 30,57%
2016: 10,08%
2017: 16,80%

As shown above, Frontsafe A/S has lived up to the goal of an annual reduction in the power consumption per stored GB of at least 5 per cent.

It is an important element in Frontsafe A/S' strategy that sufficient security is incorporated in the business so that the company is not exposed to unacceptable risks.

Frontsafe A/S has three overall strategic benchmarks:

- Frontsafe A/S helps companies make optimum use of modern information technology
- Frontsafe A/S is operating primarily with administrative systems to secure data
- Frontsafe A/S is a good place to work for a stable and well-trained team of employees

Frontsafe A/S is working with IT security at a business-strategic level and is therefore making a continuous effort to secure high service and quality levels. In the company's security policy, Management emphasises that IT security is and must be an important part of the company's business culture. Frontsafe A/S has chosen to base its IT security strategy on ISO27002:2013, and has in this way used the ISO methodology for implementation of relevant security measures within the following areas:

- Information security policies
- Organisation of information security
- Human resource security
- Asset management
- Access control
- Physical and environmental security
- Operations security
- Communication security
- Supplier relationships
- Information security management
- Information security aspects of business continuity management

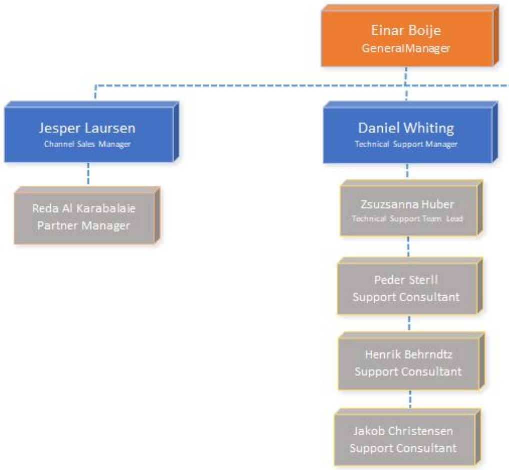
The precautionary measures implemented at Frontsafe A/S appear from appendix 1 of this description.

## Frontsafe A/S' organisation and organisation of IT security

J2 Global is a listed company on the US stock exchange NASDAQ. It was founded in 1995 with focus on business critical technology and employs a staff of more than 2.000.
J2 Global services more than 11 million satisfied customers on 6 continents.

Frontsafe A/S employs a staff of 9 and has a flat organisational structure. In charge of IT security: Network & Operations Director

For the purpose of external cooperation partners, a cooperation agreement is prepared before any work is initiated.



## Risk management at Frontsafe A/S

It is Frontsafe policy that the risks related to the company's activities must be covered or limited to such an extent that the company will be able to continue normal operations. Frontsafe A/S performs risk management and internal controls within several areas and at different levels. An annual risk and threat assessment is made. The approach is very informal. The informal risk assessment is conducted at intervals, and when we make changes to existing systems or implement new systems, which we consider relevant in connection with re-assessing our general risk assessment. The responsibility for handling this is placed at the General Manager, and must subsequently be deployed and approved by the Management of the company.

As part of the above-mentioned IT security strategy, Frontsafe A/S is working with the international standards for IT security – ISO27002:2013 – constituting the primary framework for the IT security. The work process regarding IT security is a continuous and dynamic process ensuring that Frontsafe A/S lives up to its customers' requirements and needs at all times.

## IT security management

The Network & Operations Director holds the day-to-day responsibility for IT security supported by the Management, which ensures compliance with all overall requirements and frameworks for IT security. In the central IT security policy, management has described Frontsafe A/S’ IT security structure. The IT security policy has to be revised at least once a year.

Frontsafe A/S’ quality assurance system has been defined based on the overall objective about delivering stable and secure IT operations to the customers. In order to be able to do so, it is necessary that we have introduced policies and procedures ensuring that our deliveries are consistent and transparent.

The Frontsafe A/S’ IT security policy has been prepared with reference to the above, and the policy applies to all employees and all deliveries. In the event of errors and security flaws in our operating environment, the error/security flaw will be remedied immediately.

All servers and network devices are documented in the Frontsafe documentation system. Here, all changes are logged by our system. Configuration files for network devices (firewall, routers, switches, etc.) are stored in our documentation system.

The security policy lays down the general policies for the infrastructure of Frontsafe A/S and does not deal with issues regarding specific products, services or users.

The security policy has been prepared to provide Frontsafe A/S with one common set of rules. In this way, we achieve a stable operating environment and a high security level. We are making regular improvements to policies, procedures and operations.

Frontsafe A/S' current technical setup is described in Service Level Agreement version 7.

## HR, employees and training

At the start of their employment, all employees must get security clearance and a background check is made incl. that they have no criminal record. They must sign j2 Global's security policies and a "Business code of ethics". Furthermore, we go over Frontsafe A/S' local information security together with the employee, including confidentiality in relation to customers and partners.

All employees must know their responsibility and role in connection with IT security in order to minimise the risk of human error such as theft, fraud and misuse of information assets.

Frontsafe A/S is a certified IBM Partner with capabilities on IBM Spectrum Protect, and is furthermore a certified Veeam Partner.

All performing consultants possess qualifications within their respective fields of work. Documentation for these exists in the form of relevant certifications.

Frontsafe A/S has to comply with various requirements from IBM and Veeam, including specific requirements that a specific number of consultants have passed specific product certifications, which must be renewed regularly. Through regular product training and course participation, Frontsafe A/S ensures that this high certification status is maintained.

## Physical security

Frontsafe A/S' backup facilities are placed in a safe data centre for which assurance reports have been issued according to ISAE 3402 and with the following security measures based on the ISO 27002 standard:

- The emergency power system will start automatically in case of failure or errors in the primary power supply. Furthermore, all equipment is equipped with UPS to ensure that normal operations can continue without interruptions.
- Cooling ensures an ideal temperature in the operations environment.
- To avoid disasters in the event of smoke development and fire, a highly sensitive fire-alarm system has been installed. This system has a smoke sniffer system and ion alarms that take in and analyse the air in the server room and trigger fire-fighting measures in the event of the slightest smoke development.
- Inergen systems have been installed for fire fighting purposes making use of gases that remove oxygen from the air and extinguishes the fire immediately. The server room is designed as a separate fire cell. The fire-fighting system has direct alarm transfer to the fire brigade.
- Distributor boxes and network equipment are placed in a locked server room.
- Personal access cards with codes are used.
- Alarm system is used for all alarm monitoring. Alarm logs are kept. All alarms are transferred to a call centre and/or operations monitoring service team, who initiates and decides on the required actions.
- Primary data lines are established as redundant lines. These lines are forwarded as independent fibres to two different TDC centrals.

## Monitoring

Frontsafe A/S has established automatic monitoring of servers, storage systems, networks, etc. and has trained staff on call in a rotation system, which ensures that the required qualifications are available 24/7/365.

If an error is identified, an alarm is sent both visually on the monitoring screen and by SMS/e-mail. In the event that errors are identified in a component that is not subject to the automatic monitoring, actions will be taken for future registration hereof in the system. The data centre is monitored with respect to power failure, temperature, fire, water, air humidity. Moreover, the entire data centre is under camera surveillance.

If incidents occur that might affect operations, the monitoring systems will automatically alert the contingency team and well-established escalation procedures exist with ultimate involvement of the General Manager.

The list of persons with access to the data centre is reviewed regularly in accordance with the procedure above.

## Backup

At present Frontsafe A/S offers 3 backup services:

1. Cloud backup

   Data are sent directly to Fronsafe A/S' IBM Sprectum Project backup servers and storage. Then the customer's data is copied to Frontsafe's secondary data store on a different physical location.
   With Cloud Backup solution the customer has 2 offsite copies of the data.

2. Hybrid backup

   By choosing this solution, the customer has a local copy and an offsite copy of the backup data.
   a. The customer has a local IMB Spectrum Protect server, which is a Front Server. This Front Server synchronises its backup storage with data stored on Frontsafe's backup servers.
   b. The customer has a local Veeam backup solution sending an offsite copy of its backup storage to Frontsafe's storage.

3. Veeam Cloud Connect (Repository backup)
   The service includes the possibility of saving extra copies of the Veeam backup at Frontsafe's data centre, where it is possible to recreate data at any time.

Backup at Frontsafe A/S is stored at Danish data centres secured physically and electronically (described under Control Objectives 9-13).

The purpose of backup is securing that the customer's data at Frontsafe'A/S's data centre can be restored, accurately and quickly.

All data is secured on a daily basis in another server room at a different geographical location.

## Patch management / change management

The purpose of patch management is to ensure that all relevant updates, such as patches, fixes and service packs from suppliers, are implemented to protect the systems against downtime and unauthorised access and that the implementation is carried out in a well-managed fashion.

All production servers are updated by critical and important updates in the monthly service window. This ensures that production servers do NOT have critical or important updates older than 30 days.

Frontsafe A/S has prepared a fall-back plan in relation to patch management. The purpose of the fall-back plan is to ensure that the systems can return to normal operations, if the updates do not perform as intended.

## Managing IT security incidents

Security incidents and weaknesses in the Frontsafe A/S' systems must be reported in a way that allows for timely adjustments.

All Frontsafe A/S' employees are familiar with the procedure for reporting different types of incidents and weaknesses that may impact the security of Frontsafe operations. Security incidents and weaknesses must be reported to Management as quickly as possible.

It is Management's responsibility to define and coordinate a structured management process ensuring an appropriate reaction to security incidents.

## User management / access security

The logical security includes logical protection of electronic systems and information regarding the service. For example, it specifies that only authorised persons have electronic access.

- Password requirements – all users with access to Frontsafe A/S' systems use passwords containing at least 7 characters including both digits and letters.
- Screen savers are required – screen savers are activated for all our users to protect them against unauthorised access.

## Business Continuity Management

In the event of serious errors, an e-mail is sent to the e-mail group "Frontsafe Outage". The e-mail includes a brief error description and a time horizon for the downtime. At the end of the error correction procedure, a new e-mail is sent to the e-mail group with a message that the error has been solved and a thorough error description.

If one of the server rooms is completely damaged, an action plan is prepared about what is going to happen, including re-establishment of hardware. The systems will then be restored from the backup server.

Every six months, a simulation testing the Frontsafe disaster recovery plan will be performed.

## Compliance with the role as Data Processor

It is the responsibility of Frontsafe 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
- Frontsafe A/S' Service Level Agreement
- Frontsafe A/S standard contract or other  relevant sources

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

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

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

### The EU General Data Protection Regulation (GDPR)

Frontsafe A/S' backup-services support the customers' work processes. Frontsafe A/S does not own the data our customers collect, but develops and operates the IT services our customers use for performing the necessary personal data processing. According to the EU General Data Protection Regulations and Danish additional regulation (The Danish Data Protection Act), Frontsafe A/S is the Data Processor, and the customer is the Data Controller.

Frontsafe A/S cooperates with legal experts to ensure that all legal requirements are identified and accommodated. Frontsafe A/S has also ensured relevant contracts with all key stakeholders (including customers, business partners, key suppliers etc.) to ensure compliance with law and regulations. In addition, Frontsafe A/S works together with the customers 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, Frontsafe A/S ensures data privacy and data security on a contractual level.

### Privacy and protection of personal data

As mentioned above, Frontsafe A/S is the customers' Data Processor, given that the customers are offered a backup service to which they can to transfer data. Frontsafe A/S is not responsible for any data uploaded by the customers to their backup service. Based on the categories of confidentiality of the data entrusted by the customers to the data processing, Frontsafe A/S must put all necessary security measures required into practice to ensure an appropriate level of security.

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

### Data Processor Agreements

Frontsafe A/S has Data Processor Agreements (DPA) in place with all of our customers. The Data Processor Agreement is an established procedure when entering a contract, and either Frontsafe A/S's own model contract is used or the customer's model. These contracts outline Frontsafe A/S' role and responsibilities as Data Processor.

As data processor, Frontsafe A/S is subject to a particular responsibility defined in the General Data Protection Regulation, implemented as requirements in a Data Processor Agreement. Frontsafe A/S must, inter alia:

- Record the categories of personal data processed in the various IT services
- Describe the technical and organizational security measures undertaken in order to safeguard the personal data.
- Contribute to the fulfilment of the customer's obligation in relation to the the data subject's rights (see Section 3 in the EU General Data Protection Regulations).
- Put expertise at our customers' disposal in order to ensure compliance with Articles 32 – 34.
  - Article 32 – processing security
  - Article 33 – reporting breaches regarding personal data security

  - Article 34 – informing the data subjects about breaches regarding personal data security
- Adhere to the customer’s requirements in relation to transfer of personal data outside of the EEA.
- Name and contact information of suppliers who are sub-processors.
- Ensure that the customer’s requirements regarding processing of personal data in line with the demands to the sub-processor.

At the request of the customer, Frontsafe A/S must make this list available to the customer or to the Danish Data Protection Agency at any time.

### Decision of purpose as well as legal basis

As data processor, Frontsafe A/S works with personal data based on the customers’ directions describing the restrictions regarding the purpose for the use of data. In this way, it is the responsibility of Frontsafe A/S that data collected for a particular purpose is not processed contrary to the said purpose.

The legal basis for processing personal data in relation to Cloud Backup provided by Frontsafe A/S is found in the data controller’s compliance with legal obligations or in performance of obligations under a contract (see GDPR Art. 6 L b & c).

### Access to the data in customer instances

Frontsafe A/S offers solutions like Cloud Backup operated by Frontsafe A/S’ Operations Department. In this way, Frontsafe A/S assumes the full responsibility for processing the customers’ data. In general, Frontsafe A/S’ employees have no access to customer data, unless such access is called for in relation to particular tasks.

Frontsafe A/S has laid down principles for employees’ access to and processing customers’ data.

- Only trusted employees have access to customer data and only, when there is a work-related need.
- Comprehensive introduction courses focusing on rules regarding processing customer data, as well as follow-up in the form of awareness campaigns.
- Procedure for granting, review and control of access to customer data.
- Rules for processing customer data in Frontsafe A/S’ ISMS.

Frontsafe A/S logs and monitors accesses to the customers’ data in order to secure that no unauthorized persons get access, and that granted accesses are not violated.

## Significant changes in relation to IT security

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

## The customers' responsibility (complementary customer controls)

This chapter describes the general framework for Frontsafe A/S’ Cloud Backup, which means that agreements with individual customers have not been taken into consideration.

Frontsafe A/S is not responsible for access rights, including granting, changes and removal, in relation to the individual customer's users and their access to Frontsafe A/S’ Cloud Backup. The customer is responsible for ensuring the controls necessary in connection with this control objective. In connection with handling of password security, the audit is performed based on a general perspective.

For some user companies the security in relation to creation of passwords might be below the frame, if the customer’s Management wanted it. The responsibility for reconciliation of the control environment for password security stays with each user company, and with those using this report.

The customers are responsible for data transmission to Frontsafe A/S' Cloud Backup, and it is the responsibility of the customers to create the required data transmission to the Frontsafe data centre. The customer must ensure the controls necessary in connection with this control objective.

Frontsafe A/S' continuity management is constructed based on an overall contingency plan that describes the approach and procedures to be applied, if recovery of Frontsafe A/S' Cloud Backup is needed. Specific contingency plans can be prepared for the individual customer according to need in proportion to the risk of interrupting business processes.

APPENDIX 1:

# Frontsafe 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 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

(not covered by the Auditor's Report)
11.1 Secure areas
11.2 Equipment

### 12. Operations security

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. Communication security

13.1. Network security management

### 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

CHAPTER 3:

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

For the customers of Frontsafe A/S' Cloud Backup and their auditors

## Scope

We have been engaged to report on Frontsafe A/S's description in Chapter 2 (including appendix 1), which is a description of technical and organizational security measures conducted in connection with the operation of Frontsafe A/S' Cloud Backup for processing customers' transactions during the period 1 October 2017 - 30 September 2018, and on the design and operating effectiveness of controls related to the control objectives mentioned 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 controls and control activities related to the use of external business partners. Frontsafe A/s uses external partners in connection with operations of their Cloud Backup in the following areas:

- Co-location / data centre – the physical security in relation to Frontsafe production equipment.

The report does not cover customer-specific conditions. Furthermore, the report does not cover the complementary controls and control activities conducted by the user company; see the description of the company in Chapter 2 under the section about complementary controls.

## Frontsafe A/S' responsibility

Frontsafe 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 on Frontsafe A/S'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 and operate effectively in all material respects. 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 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 those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were 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 in Chapter 2 (including appendix 1) by Frontsafe A/S.

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

## Limitations of controls at Frontsafe A/S

Frontsafe A/S'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 its own particular environment. In addition, because of their nature, controls at Frontsafe A/S may not prevent or detect all errors or omissions in processing or reporting transactions. The projection of any evaluation of effectiveness to future periods is subject to the risk that controls at the service organisations 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 technical and organizational security measures of Frontsafe A/S for Cloud Backup, such as they were designed and implemented throughout the period 1 May 2017 – 30 September 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 the period 1 October 2017 - 30 September 2018; 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, operated effectively throughout the period 1 October 2017 - 30 September 2018.

Please, note that there may be specific circumstances in relation to the individual customers, which means that the general conclusion is not fully adequate. If it has been agreed between the customer and Frontsafe A/S that a specific statement should be prepared regarding the customer's contract, the conditions will appear from hereof.

## 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 intended only for Frontsafe 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.

Søborg, 26 October 2018

**Beierholm**
State-Authorized Public Accountant Partner Company

Kim Larsen
State Authorised Public Accountant

Jesper Aaskov Pedersen
IT Auditor, Manager

CHAPTER 4:

# 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 ISO27002:2013.

With respect to the period, we have tested whether Frontsafe A/S has complied with the control objectives throughout the period 1 October 2017 - 30 September 2018.

Below the gray field are three columns:

- The first column tells the activities Frontsafe A/S, according to its 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 Frontsafe 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. |

CONTROL OBJECTIVE 5:

# 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.

| Frontsafe 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.<br>The IT security policy and accompanying supporting policies are approved by the company's Management and then deployed down through the company's organisation.<br>The policy is available for all relevant employees.<br>The policy is re-evaluated according to planned intervals. | We have obtained and audited Frontsafe A/S' latest IT security policy.<br>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.<br>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 Frontsafe A/S' intranet. | During our test, we did not identify any material deviations. |

CONTROL OBJECTIVE 6:

# 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 ensure, among other things, compliance with security measures, including continuous updating of the overall risk assessment.

| Frontsafe A/S' control procedures | Auditor's test of control procedures | Test findings |
|---|---|---|
| Organisational responsibility for IT security has been placed, documented and implemented.<br>The IT security has been coordinated across the company's organisation.<br>Appropriate business procedures exist for employees regarding professional secrecy statements. | Through inspection and tests, we have ensured that the organisational responsibility for IT security is documented and implemented.<br>We have checked that the IT security is deployed across the organisation in relation to Cloud Backup.<br>By making interviews, we have checked that the person responsible for IT security knows his/her role and responsibilities.<br>Through enquiries and samples from employment contracts, we checked that Frontsafe A/S' employees are familiar with their professional secrecy. | During our test, we did not identify any material deviations. |
| Risks in relation to use of mobile devices and teleworking are identified, and managing security conditions is appropriate. | We checked that formal cooperation agreements exist in connection with the use of mobile devices and teleworking.<br>On a test basis, we have inspected that the policy is implemented regarding employees using mobile devices.<br>Regarding the use of teleworking at Frontsafe A/S, we have checked, whether appropriate security measures have been implemented ensuring that this area is covered in relation to the risk assessment of the area. | During our test, we did not identify any material deviations. |

CONTROL OBJECTIVE 7:

# 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.

| Frontsafe A/S' control procedures | Auditor's test of control procedures | 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 Frontsafe A/S. This includes the framework laid down for the work and the IT security involved.<br>Security responsibilities, if any, are determined and described in job descriptions and in the terms of the employment contract.<br>The employees are familiar with their professional secrecy based on a signed employment contract and through Frontsafe 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.<br>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.<br>Through interviews, we have checked that employees of significance to Cloud Backup are familiar with their professional secrecy.<br>We have examined the job descriptions of key employees and subsequently tested the awareness of the individual employee of their roles and related security responsibility.<br>We have ensured that Frontsafe 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 Frontsafe A/S. | During our test, we did not identify any material deviations. |

CONTROL OBJECTIVE 8:

# Asset Management

The required protection of the company's information assets must be ensured and maintained, and all of the company's physical and functional information-related assets must be identified, and a responsible "owner" must be appointed. The company must ensure that the information assets in relation to Cloud Backup are suitably protected.

| Frontsafe A/S' control procedures | Auditor's test of control procedures | Test findings |
|---|---|---|
| All information assets have been identified and an updated list of all significant assets has been established.<br>An "owner" of all significant assets is appointed in connection with the operation of Cloud Backup. | We have examined and checked the company's central IT register for significant IT entities in connection with the operation of Frontsafe A/S' Cloud Backup.<br>Through observation and control, we have checked relations to central knowhow systems for the operation of Cloud Backup.<br>By observations and enquiries, we have checked that Frontsafe A/S complies with all material security measures for the area in accordance with the security standard. | During our test, we did not identify any material deviations. |
| Information and data in relation to Cloud Backup and the subsequent hosting centre operation are classified based on business value, sensitivity and need for confidentiality. | We have checked that there is appropriate division and related procedures/business procedures in connection with protection of ownership between applications and data as well as other entities in relation to Frontsafe A/S' operation of Cloud Backup.<br>We have checked that contracts and SLA are used as central tools to ensure the definition, segregation and delimitation of Frontsafe A/S' responsibilities and the customer's responsibilities with respect to access to information and data.<br>Accordingly, the customer is typically responsible for ensuring that a suitable protection level exists for own information and data. | During our test, we did not identify any material deviations. |
| Procedures of dealing with destruction of data media are established. | We have:<br>• Asked Management which procedures/control activities are performed.<br>• On a sample basis gone through the procedures for destruction of data media as confirmation that these are formally documented. | During our test, we did not identify any material deviations. |

CONTROL OBJECTIVE 9:

# 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.

| Frontsafe A/S' control procedures | Auditor's test of control procedures | Test findings |
|---|---|---|
| Documentation and updated direction exist for Frontsafe A/S' access control. | We have:<br>• asked Management whether access control procedures have been established at Frontsafe A/S.<br>• verified on a test basis that access control procedures exist and have been implemented; see Frontsafe A/S' directions.<br>• by interviewing key personnel and by inspection on a test basis, we have verified that access control for the operations environment comply with Frontsafe A/S' directions, and authorisations are granted according to agreement. | During our test, we did not identify any material deviations. |
| A formal business procedure exists for granting and discontinuing user access.<br>Granting and application of extended access rights are limited and monitored. | We have asked Management whether access control procedures have been established at Frontsafe A/S.<br>By inspection on a test basis, we have verified<br>• that adequate authorisation systems are used in relation to access control at Frontsafe A/S.<br>• that the formalised business procedures for granting and discontinuing user access have been implemented in Frontsafe A/S' systems and registered users are subject to regular follow-up. | During our test, we did not identify any material deviations. |
| 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:<br>• that formal management follow-up is performed on registered users with extended rights every three months.<br>• that formal management follow-up is performed on registered users with ordinary rights every six months. | During our test, we did not identify any material deviations. |

| | | |
|---|---|---|
| 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 access code granting procedures have been established at Frontsafe A/S.<br>By inspection on a test basis, we have verified<br>• that an automatic systems control takes place, when access codes are granted to check that passwords are changed after first login.<br>• that standard passwords are changed in connection with implementation of systems software etc.<br>• if this is not possible, that procedures ensure that standard passwords are changed manually. | During our test, we did not identify any material deviations. |
| Access to operating systems and networks are protected by passwords.<br>Quality requirements have been specified for passwords, which must have a minimum length (7 characters) including requirements as to complexity. However, no maximum duration is required, and likewise password setup means that passwords might be reused.<br>Furthermore, the user will be barred in the event of repeated unsuccessful attempts to login. | We have asked Management whether procedures ensuring quality passwords in Frontsafe A/S are established.<br>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:<br>• minimum length of password<br>• complexity<br>• lockout after unsuccessful login attempts | During our test, we did not identify any material deviations. |

CONTROL OBJECTIVE 12:

# 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.

| Frontsafe A/S' control procedures | Auditor's test of control procedures | Test findings |
|---|---|---|
| The operations procedures for business critical systems have been documented, and they are available to staff with work-related needs.<br>Management has implemented policies and procedures to ensure satisfactory segregation of duties. | We have:<br>• asked Management whether all relevant operations procedures have been documented.<br>• 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 actions actually performed.<br>• 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. | During our test, we did not identify any material deviations. |
| Management of operational environment is established in order to minimise the risk of technology related crashes.<br>Continuous capacity projection is performed based on business expectations for growth and new activities and the capacity demands derived hereof. | We have:<br>• asked Management about the procedures and control activities performed.<br>• on a test basis examined that the operation environment's consumption of resources is monitored and adapted to the expected and necessary capacity requirements. | During our test, we did not identify any material deviations. |

Control objective: Protection from malware

To protect from malicious software, such as virus, worms, Trojan horses and logic bombs. Precautions must be taken to prevent and detect attacks from malicious software.

| Frontsafe A/S' control procedures | Auditor's test of control procedures | Test findings |
|---|---|---|
| Preventive, detecting and remedial security and control procedures have been established, including the required training and provision of information for the company's users of information systems against malicious software. | We have:<br>• enquired about and inspected the procedures/ control activities performed in the event of virus attacks or outbreaks.<br>• enquired about and inspected the activities meant to increase the employees' awareness of precautions against virus attacks or outbreaks.<br>• verified that anti-virus software has been installed on servers and inspected signature files documenting that they have been updated. | During our test, we did not identify any material deviations. |

Control objective: Backup

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

| Frontsafe A/S' control procedures | Auditor's test of control procedures | Test findings |
|---|---|---|
| Backup is made of all of the company's significant information assets, including, e.g. parameter setup and other operations-critical documentation, according to the specified directions. | We have:<br>• asked Management about the procedures/ control activities performed.<br>• examined backup procedures on a test basis to confirm that these are formally documented.<br>• 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.<br>• examined physical security (e.g. access limitations) for internal storage locations to confirm that backup is safely stored. | During our test, we did not identify any material deviations. |

| Control objective: Logging and monitoring<br>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. | | |
|---|---|---|
| Frontsafe A/S' control procedures | Auditor's test of control procedures | Test findings |
| Operating systems and network transactions or activities involving special risks are monitored. Abnormal conditions are examined and resolved on a timely basis.<br>Frontsafe A/S logs, when internal users log off and on the systems.<br>Only in the event of suspected or identified abuse of the systems, the users are actively monitored. | We have:<br>• 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.<br>• checked on a test basis that logs from critical systems are subject to sufficient follow-up. | During our test, we did not identify any material deviations. |
| 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.<br>Alerts are shown on the monitoring screen mounted in the project and operations department. Critical alerts are also sent by email and SMS.<br>Status reports are sent by email from different systems. Some every day – others when incidents occur in the system. The operations monitoring function is responsible for checking these emails on a daily basis. | We have:<br>• asked Management about the procedures/ control activities performed.<br>• ensured that a monitoring tool is used and that this is available to all employees.<br>• ensured that alerts are sent by email and SMS, if errors occur.<br>• examined status reports.<br>• ensured that an operations monitoring service is established and that this function checks reports on a daily basis. | During our test, we did not identify any material deviations. |

Control objective: Managing operations software and managing vulnerability

Ensuring establishment of appropriate procedures and controls for implementation and maintenance of operating systems.

| Frontsafe A/S' control procedures | Auditor's test of control procedures | Test findings |
|---|---|---|
| Changes in the operation environment comply with established procedures. | We have asked Management, whether procedures for patch management are established at Frontsafe A/S.<br>By inspection on test basis, we have verified that<br>• adequate procedures are applied, when controlled implementation of changes to the production environments of Frontsafe A/S are performed.<br>• changes to Frontsafe A/S' operation environments comply with directions in force, including correct registration and documentation of change requests.<br>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. | During our test, we did not identify any material deviations. |
| Changes in user systems and operation environments comply with formalised procedures and processes. | We have asked Management, whether procedures for patch management are established in Frontsafe A/S.<br>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 change management controls ensure that<br>• change requests are registered and described<br>• all changes are subject to formal approval before implementation<br>• changes are subject to formal impact assessments<br>• fall-back plans are described<br>• systems affected by changes are identified<br>• documented test of changes is performed before implementation<br>• documentation is updated reflecting the implemented changes in all material respects<br>• procedures are subject to managing and coordination in a "change board". | During our test, we did not identify any material deviations. |

CONTROL OBJECTIVE 13:

# Communication Security

To ensure protection of information in networks and support of information processing facilities.

| Frontsafe A/S' control procedures | The auditor's test of controls | Test findings |
|---|---|---|
| Networks must be protected against threats in order to secure network based systems and the transmitted data.<br>Production environment must be secured against failing supply in relation to redundancy to network connection to the internet.<br>Network traffic/access from production environment to the outside world is available by means of multiple supply entries or access from more than one supplier. | It has been checked that necessary protection against unauthorised access is implemented, including:<br>• Appropriate procedures for managing network equipment are established.<br>• Segregation of user functions is established.<br>• Appropriate logging and monitoring procedures are established.<br>• Managing the company's network is coordinated in order to ensure optimal utilisation and a coherent security level.<br>• Ensured that connections for data communication with the internet are established via more than one ISP supplier.<br>• On a sample basis gone through documentation from the supplier about written basis for contract, as well as regular settlement of accounts for services rendered by the ISP supplier. | During our test, we did not identify any material deviations. |
| Adequate procedures for managing threats in the form of attacks from the internet (cyber-attacks) must be implemented.<br>In this connection, tools for managing the contingency approach in the event of a cyber-attack must be devised. | • We have controlled that an adequate number of procedures with accompanying contingency plans regarding managing threats in relation to cyber-attacks are implemented.<br>We have by inspection on a test basis ensured<br>• that appropriate framework for managing cyber-attacks are devised.<br>• that plans for managing the threat are devised and implemented.<br>• that the plans include cross-organisational collaboration between internal groups. | During our test, we did not identify any material deviations. |

CONTROL OBJECTIVE 15:

# Supplier Relationships

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

| Frontsafe A/S' control procedures | Auditor's test of control procedures | Test findings |
|---|---|---|
| Risks related to external business partners are identified, and security in third-party agreements and security in relation to customers are managed. | We have verified that in connection with the use of external business partners there are formal cooperation agreements.<br>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. | During our test, we did not identify any material deviations. |
| 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.<br>We have ensured that appropriate procedures for managing cooperation with external partners are established.<br>We have tested that key suppliers have updated and approved contracts. | During our test, we did not identify any material deviations. |
| Monitoring must be conducted regularly, including supervision of external business partners. | We have ensured that there are appropriate processes and procedures for ongoing monitoring of external suppliers.<br>We have checked that ongoing supervision is conducted by means of independent auditor's reports. | During our test, we did not identify any material deviations. |

CONTROL OBJECTIVE 16:

# 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.

| Frontsafe A/S' control procedures | Auditor's test of control procedures | Test findings |
|---|---|---|
| Security incidents are reported to Management as soon as possible, and the managing is performed in a consistent and efficient way. | We have asked Management whether procedures have been established for reporting of security incidents.<br>We have verified that procedures and business procedures have been developed for reporting and managing security incidents, and that the reporting is submitted to the right places in the organisation; see the directions.<br>We have verified that the responsibility for managing critical incidents is clearly delegated and that the related business procedures ensure that security breaches are managed expediently, efficiently and methodically. | During our test, we did not identify any material deviations. |

CONTROL OBJECTIVE 17:

# Information Security Aspects of Business Continuity Management

Business continuity management must counteract 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.

| Frontsafe A/S' control procedures | Auditor's test of control procedures | 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 Frontsafe A/S' Cloud Backup.<br>By inspection on a test basis, we have verified<br>• that appropriate framework for preparation of business continuity management has been established<br>• that contingency plans are prepared and implemented<br>• that the plans include business continuity management across the organisation<br>• that the plans include appropriate strategy and procedures for communication with the interested parties of Frontsafe A/S.<br>• that contingency plans are tested on a regular basis<br>• that maintenance and reassessment of the total basis for business continuity management is undertaken on a regular basis. | During our test, we did not identify any material deviations. |

CONTROL OBJECTIVE 18:

# 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 principles for processing personal data.

| Frontsafe A/S' control procedures | Auditor's test of control procedures | 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. | During our test, we did not identify any material deviations. |

**Data Processor:**

There is compliance with procedures and controls ensuring that the Data Processor's technical and organizational measures for protection of the data subject's rights as well as the processing of personal data, are approved by the Data Controller.

| Frontsafe A/S' control procedures | Auditor's test of control procedures | Test findings |
|---|---|---|
| There are directions for processing and protection of personal data at the Data Processor, including directions for processing at other Data Processors. | We have controlled that there is documentation displaying that the Data Controller has provided the Data Processor with directions for processing and protecting personal data. | During our test, we did not identify any material deviations. |

**Records of processing activities:**

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

| Frontsafe A/S' control procedures | Auditor's test of control procedures | Test findings |
|---|---|---|
| There are records of the processing activities for each Cloud Backup solution in combination with the relevant Data Controller. | We have controlled documentation displaying the existence of processing activities records for each Cloud Backup solution combined with the relevant Data Controller. | During our test, we did not identify any material deviations. |

| | | |
|---|---|---|
| Assessment is made on an ongoing basis – and at least once a year – that the records are updated and correct. | We have controlled the documentation displaying that the records of the processing activities for each data controller are updated and correct. | During our test, we did not identify any material deviations. |

**The Data Controller's responsibility:**

There is compliance with procedures and controls ensuring that processing of personal data is only performing according to contract or other legally binding document (Data Processor Agreement), as well as ensuring that data processing is performed solely by a Data Processor approved by the Data Controller.

| Frontsafe A/S' control procedures | Auditor's test of control procedures | Test findings |
|---|---|---|
| The Data Controller has provided directions for processing and protection of personal data at the Data Processor, including processing at other Data Processors when used. | We have controlled documentation displaying that the Data Controller has provided the Data Processor with directions for processing and protection of personal data. | During our test, we did not identify any material deviations. |
| The Data Controller has approved the guarantees given by the Data Processor that procedures, technical measures and controls meet the requirements of the GDPR. | We have controlled the documentation displaying that the Data Controller has approved the guarantees given and approved by the Data Processor that procedures, technical measures and controls meet the requirements of the GDPR. | During our test, we did not identify any material deviations. |
| The Data Controller has approved the Data Processor's use of other Data Processors as subcontractors. Control of processing at Data Processors used as subcontractors is performed. | We have controlled the documentation displaying that the Data Controller has approved the use of other Data Processors. | During our test, we did not identify any material deviations. |

**Reporting breaches of personal data security to the supervisory authority (the Danish Data Protection Agency):**

There is compliance with procedures and controls ensuring that the Data Processor in the event of personal data security breaches is able to support the Data Controller's obligation to timely and sufficient reporting to the supervisory authority, as well as information to the data subjects, whose personal data is included in the breach.

| Frontsafe A/S' control procedures | Auditor's test of control procedures | 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. | During our test, we did not identify any material deviations. |

| | | |
|---|---|---|
| Data Processor ensures recording of all personal data security breaches. | We have controlled documentation displaying that all personal data security breaches are recorded at the Data Processor. | During our test, we did not identify any material deviations. |

| | | |
|---|---|---|
| Management has ensured that all personal data security breaches are timely and sufficiently communicated to the Data Controller, including personal data security breaches happened 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 happened at Data Processors used as subcontractors. | During our test, we did not identify any material deviations. |