BEIERHOLM
VI SKABER BALANCE

June 2023

Ajour System A/S

ISAE 3402 TYPE 2 REPORT

CVR number 84667811

Independent auditor's report on coverage of the control description regarding technical and organizational security measures for Ajour System A/S in relation to SaaS solutions.

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

Beierholm
Statsautoriseret Revisionspartnerselskab
Knud Højgaards Vej 9
2860 Søborg
CVR 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 technical and organizational security measures in relation to development and operations of Ajour System A/S’ SaaS solutions.

Chapter 3:

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

Chapter 4:

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

CHAPTER 1:

Letter of Representation

Ajour System A/S processes personal data on behalf of customers according to Data Processor Agreements regarding operation of Ajour System A/S' SaaS solutions

The accompanying description has been prepared for the use of customers and their auditors, who have used Ajour System A/S' SaaS solutions, and who have sufficient understanding to consider the description along with other information, including information about controls operated by the customers i.e. the Data Controllers themselves, when assessing, whether the demands to the control environment as well as requirements laid down in the General Data Protection Regulation are complied with.

Ajour System A/S hereby confirms that:

(A) The accompanying description, Chapter 2 (incl. Appendix 1) gives a true and fair description of Ajour System A/S' control environment in relation to operations of Ajour System A/S' SaaS solutions throughout the period April 1st 2022 to March 31st 2023. 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 Ajour System A/S' SaaS solutions – have been implemented by the Data Controllers and which, if necessary to fulfil the control objectives mentioned in the description, have been identified in the description
- Other aspects of our control environment, risk assessment process, information system (including the accompanying work routines) and communication, control activities and monitoring controls relevant for processing of personal data

(ii) Includes relevant information about changes in Ajour System A/S' SaaS solutions processing of personal data performed throughout the period April 1st 2022 to March 31st 2023

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

(B) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period April 1st 2022 to March 31st 2023. The criteria for this assertion are that:

(i) The risks threatening the fulfilment of the control objectives mentioned in the description were identified

(ii) The identified controls would, if used as described, provide reasonable assurance that the risks in question would not prevent the fulfilment of the said control objectives, and

(iii) The controls were applied consistently as designed, including that manual controls were performed by persons with adequate competences and authority throughout the period April 1st 2022 to March 31st 2023.

(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 (incl. Appendix 1) have been prepared based on compliance with Ajour System A/S' standard agreement as well as related Data Processing Agreement, the basis for Ajour System A/S SaaS solutions. The criteria for this basis are:

(i) Ajour System – Information security policy
(ii) Ajour System – Data Processor Agreement

Odense, June 29th 2023

ABjaaland

Senior Vice President , Aleksander Bjaaland
Ajour System A/S, Østerbro 5B st. th, DK-5000 Odense C, CVR-no.: 84667811

CHAPTER 2

Description of control environment in relation to development and operation of the *Ajour System*

Introduction

This description is prepared for customers, who have received professional services provided by Ajour System A/S.

The framework for the present description is to provide information about the Ajour System to customers and their auditors regarding the requirements of ISAE 3402, which is the international auditing standard for assurance engagements.

The present control description identifies the technical and organizational security measures implemented in connection with the operation of the Ajour System.

Description of Ajour System A/S

Ajour System A/S is one of the country's leading software providers for the construction and property industry, and we develop and sell user-friendly digital tools and BIM solutions developed in collaboration with some the industry's experts and based on the newest technology.

We unify the parties of the construction industry with the purpose of delivering quality products, sustainable with fewer resources, flexible processes, and our platform is used every day by more than 40.000 users in several countries.

Ajour System A/S develops the SaaS solutions AjourBuild and AjourCollab.

AjourBuild is software for use in connection with quality control at constructions, maintenance of buildings, calls for tender, and project web. The AjourBuild product also includes an app to use on iOS and Andriod units.

AjourCollab software is used to collect and edit data from BIM models. Apart from the SaaS solution, this product also includes plugin to Revit.

Ajour System A/S was until 1 April 2022 a Danish privately owned business. Ajour System A/S has been purchased by EG A/S and will from 1 April 2023 be completely integrated with EG A/S.

Business Strategy / IT Security Strategy

It is Ajour System A/S' strategy that the business must have a sufficient built-in level of security to avoid that the company incurs unacceptable risks. As a supplier to private and public enterprises, Ajour System A/S works with information security on a business-strategical level. The goal is to be a professional product provider with a sharp attitude towards taking care of the data our customers entrust to us.

It is Ajour System A/S' position always to ensure compliance with existing laws and to do what is technically and financially possible to secure a high level of confidentiality, integrity,and availability of the data processing.

Information security is a priority at all levels of the organisation. All employees must know the importance of this focus and must be instrumental themselves in the ongoing process of improving the work regarding security.

Ajour System A/S' objective in relation to information security is that Ajour system A/S carries out all necessary activities to ensure:

- **Availability** of the Ajour system: to achieve high availability with a high level of uptime and minimum risk of crash.
- **Integrity**: to achieve a reliable and correct operation of the Ajour system and a minimized risk of incorrect data used, due for instance to human or systemic errors or external incidents.
- **Confidentiality**: to ensure confidential processing, transmission, and storage of data only accessible by authorized users.

It is Ajour System A/S' goal to maintain an information security level which as a minimum:

- Complies with existing law
- Follows the generally accepted standards of the industry
- Lives up to the customer's wishes, requirements, and expectations.

The General Data Protection Regulation (GDPR) represents the regulatory framework for processing of personal data in the Ajour system, as included in the agreement between the customer (the Data Controller) and Ajour System A/S (the Data Processor). It is Ajour System A/S' responsibility to implement the technical and organizational security measures ensuring that personal data is processed in a safe and sound manner.

To ensure the delivery of a uniform service, which lives up to the best standards of the industry, Ajour System A/S has decided to subject the operation of the Ajour system to an audit process aimed at meeting the requirements of an ISAE 3402 Assurance Report. The audit process is repeated annually, and the result is an Auditor's Report.

The Report is a contribution to the customer's (the data owner's) control of, whether Ajour System A/S lives up to the directions in the agreed Data Processor Agreement.

Ajour System A/S has decided to base the IT security strategy on ISO27001 and ISO27002, and has thus used the ISO methodology to implement the relevant security measures in the following areas:

- Information security policies
- Organisation of information security
- Human resources security
- Asset management
- Access control
- Encryption
- Physical and environmental security
- Operations security

- Communication security
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance (law)

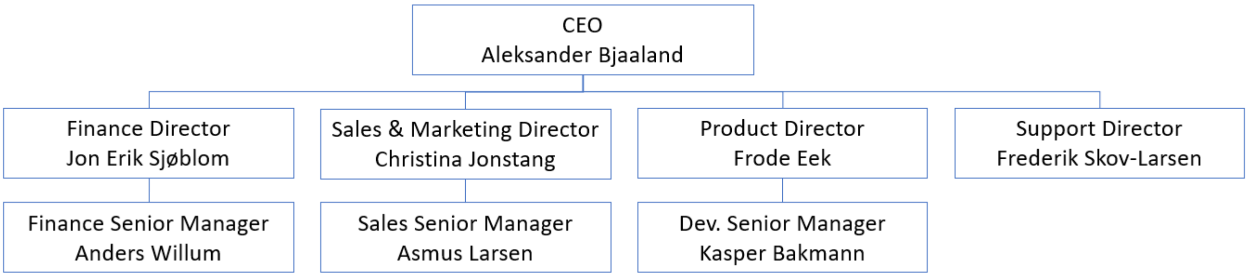
The framework for which control objectives and underlying controls (elements of security) Ajour System A/S' management has defined as relevant for our work for an appropriate security environment is described in more detail in Appendix 1.

Scope of this description

The following part of this chapter is a description of Ajour System A/S' services which are subject to the general IT control measures included in this report. The scope of the report is general processes and system setup etc. at Ajour System A/S.

Control measures in relation to the application systems are not included in this report.

Ajour System A/S' organization and structure of IT-security



CEO
Aleksander Bjaaland

Finance Director
Jon Erik Sjøblom

Finance Senior Manager
Anders Willum

Sales & Marketing Director
Christina Jonstang

Sales Senior Manager
Asmus Larsen

Product Director
Frode Eek

Dev. Senior Manager
Kasper Bakmann

Support Director
Frederik Skov-Larsen

Risk Management in Ajour System A/S

To focus Ajour System A/S' IT security efforts, the work is conducted according to a structured approach for risk control. The result of the risk control including assessment of risks is made by Ajour System A/S' Management.

Management is immediately informed about material deviations in the current threat assessment, and the adaptations this assessment gives rise to regarding the focus areas and control measures. Minor deviations are collected and reported at intervals to Ajour System A/S' CEO, and are included in the annual reporting, too.

Managing IT Security

To ensure segregation of duties and embedding the responsibility of IT security at Ajour, the primary roles and responsibilities in relation to information security are stated below:

The responsibility of the CEO

The CEO has the general responsibility for IT security at Ajour. This implies the responsibility to:

- Provide the necessary framework and resources to achieve the desired IT security level
- Ensure that a relevant IT security policy is implemented
- Take the necessary measures in the event of a major breakdown

The responsibility of the Day-to-Day Management

The Day-to-Day Management ensures compliance with the IT security policy. Including, to:

- Ensure that the IT security policy is complied with and is sufficiently implemented via work routines, procedures, and directions
- Create a joint organisational understanding of IT security as a common responsibility, and that each and everybody - both internal and external parties - is subject to the directions, work routines etc.
- Ensure that roles and responsibilities are described and appointed within Ajour as well as in relation to collaborators and suppliers
- Put IT security initiatives into practice
- Prepare deviation reports for CEO

Data Protection Officer (DPO)

No DPO (Data Protection Officer) is appointed for Ajour System A/S, as Ajour System A/S does not process personal data as a core activity, and furthermore does not process personal data to a great extent. This decision was made based on Datatilsynets "Vejledning om databeskyttelsesrådgiver" (the Danish Data Supervision Authority's "Directions regarding Data Protection Officer"), Section 3.1, dated December 2017.

Chief Information Security Officer (CISO)

The Development Senior Manager is responsible for IT security and is thus the Chief Information Security Officer, as well as having the day-to-day and operational responsibility for IT security, including:

- The ongoing work and further development of the IT security level at Ajour, ensuring it is in accordance with the requirements of the IT security policy. This includes all accompanying procedures and directions as well as compliance with existing legislation
- Ensuring that suppliers comply with the requirements stated in outsourcing contracts, including that the basis for contract with suppliers is in accordance with the IT security policy in relation to control, follow-up, and reporting
- Monitoring and reporting any IT security incidents in accordance with the fixed set of rules in the IT security policy in question
- Initiating own investigations or tests to the extent considered necessary
- Taking on the role of general IT security coordinator
- Work as contact person for the external audit in connection with IT audit
- Work as contact point for data subjects, collaborators, and the supervisory authority, including reporting personal data security breaches to the supervisory authority
- Ensuring that Ajour System A/S complies with the terms and conditions of the General Data Protection Regulation, including keeping tabs on the organization's compliance with the data protection rules and relevant documentation supporting the compliance
- Attend, and prepare material for, training and awareness activities for the organization
- Be the organization's internal point of contact in relation to instruction and advice

Asset Management

Ajour System A/S manages assets using a procedure for handing out and returning equipment to and from employees. Furthermore, Ajour System A/S provides clear instructions about the proper use of USB sticks and how to dispose of IT equipment no longer in use.

The intangible assets are managed using a list of assets. The list documents the following features:

- Ajour categorisation
- Archive of information
- Description
- Legal basis
- Type of information
- Data classification
- Comments
- Owner
- Responsible person at Ajour
- Supplier agreement

The list is maintained by Chief Information Security Officer and Management at Ajour System A/S.

Human Resources and Education

The employees are Ajour System A/S' most important operations and development resource. They are, however, at the same time a risk in relation to information security. Focus on compliance with the IT security policy and providing relevant directions for the employees within each area of the work are thus paramount for the security level at Ajour System A/S.

All employees ought to consider themselves ambassadors of IT security. The employees have a co-responsibility for IT security and are obliged to comply with the rules laid down in the IT security policy including accompanying work routines, directions, procedures etc.

Based on the specific assessment of each case, violation of the rules might be considered a breach of employment contract.

The employees' domain knowledge and competences are important requisites for Ajour System A/S' business. Ajour System A/S works with ongoing training and exchange of experience based on the individual employee's needs to support the professional development of the employees.

New employees are given a thorough introduction course to the business. The course contains information about information security, including IT security rules, introduction to the information security organisation, appropriate IT behaviour, classification of data, and special focus on Ajour System A/S' role as data processor.

To a limited extent, it is possible for Ajour System A/S' employees to work from other facilities than the offices in Odense, Copenhagen, Reykjavik, Malmo, and Wroclaw. The company has devised a procedure describing rules and good advice for teleworking. Ajour System A/S has established technical measures ensuring an encrypted connection to office facilities. Access to back-end systems and operation environments is technically limited.

All employees have a confidentiality clause in their employment contracts. As part of our termination procedure, an exit talk with the nearest superior is included, and here we remind the employee that the confidentiality clause is still in force after the end of the employment.

To ensure a continuous approach to the information security culture, Ajour System A/S holds an annual meeting about IT security information. The information is re-assessed annually by the information security organisation.

User Management / Access Security

Logical access control ensures that only authorized users have access to the systems.

Granting access to operation environment must be in accordance with business related purposes and the classification of information. Both physical and logical access is based on the principles "need-to-know" and "least-privilege", and according to these principles access is granted to information the individuals will need to carry out their assignment/job or role.

Request for access to internal IT systems and production environments follows an established procedure that ensures segregation between request, approval, verification, and implementation.

Physical Security

Ajour System A/S utilizes two external suppliers as hosting suppliers: EnergiFyn and Microsoft Azure for internal servers and the Ajour system. It means that Ajour System A/S has entrusted the basic data centre tasks to the supplier, who is experienced in the building and operation of data centres.

EnergiFyn is responsible for physical security, fire and water detection and fighting, power and cooling.

The hosting suppliers’ data centre provides several layers of security and comply with approved international standards of information security regarding management systems and business continuity management.

As of 3 December 2022, all hosting was moved to Team Blue now taking care of all infrastructure operations. EG CloudOps takes care of the operations of software services.
The hosting suppliers’ data centre provides several layers of security and comply with approved international standards of information security regarding management systems and business continuity management.

Operation of the Ajour System

Fixed operational tasks are carried out at fixed intervals. These tasks are managed at Ajour System A/S by the DevOps team and in collaboration with EG CloudOps.

Malware Protection

To secure that the Ajour System is not attacked by malware, the following steps are initiated:
The employees have been trained in detecting and handling suspicious approaches. These might be phone calls as well as e-mails.

On all office laptops antivirus software is installed, which updates and retrieves new definitions automatically.

Backup

The purpose of backup is to ensure that the customer’s data in the Ajour system can be re-created accurately and quickly, to avoid unnecessary waiting time for the customers. Backup of Ajour’s systems is forwarded to an external partner. The external partner is responsible to the running of the backup service. Ajour System A/S monitors the process to check, whether the backup was run correctly.

Backup policy
Ajour System A/S secures data based on an agreed security policy.
The policies mentioned below are in force as the standard. The standard can be changed by Ajour System A/S, or by the customer if the customer has administrative rights to the server in question. The policy currently in force is displayed in the server’s configuration file.

Backup is taken on all data essential for the continuation of the Ajour system. This includes files, SQL databases, EventStore nodes. Furthermore, backup is taken of internal servers.

Encrypting of data
By encrypting data, the data becomes impossible to read by everybody apart from those with the encryption key.
Ajour System A/s also encrypts data stored at Ajour System A/S’ data backup.

Logging and Monitoring

Ajour System A/S has established automatic monitoring of servers, storage systems, networks etc.

If an error occurs, an alert is sent both visually on a monitoring screen and on SMS. If a situation occurs of an error discovered on a component not part of the automatic monitoring, steps will be taken to register this in the system in the future. The hosting centre is monitored for power outages, temperature, fire, water, and in addition the entire hosting centre is covered by CCTV.

If incidents affecting operations occur, the monitoring system will automatically notify the response team on duty, and there is an established procedure for escalation ending with the involvement of the CEO.

The list of persons with access to the Ajour system is reviewed on a regular basis, see the relevant procedure.

Communication Security

In the event of any unusual activity, the DevOps team in cooperation with the EG CloudOps team will analyze internet traffic and FW traffic and will assess, in consultation with the Chief Information Security Officer, whether it is necessary to interfere with the network.

Access to wireless network for guests

Guests, whose identity is known, can get a password to Ajour System A/S' guest WiFi, and access it using their own equipment.

Connecting equipment to network

Employees are allowed connecting equipment to the network, if approved by the Chief Information Security Officer. The equipment is not allowed to disrupt the network, and the Chief Information Security Officer has the power to demand the disconnection of the equipment.

Segregation of networks

Ajour System A/S has divided the physical network into 2 sub-nets. One sub-net for the production environment (Production), meaning the net for operation of Ajour System A/S' proprietary software. In addition, a sub-net for the office environment (Office), meaning a net for Ajour System A/S' employees to access the shared drives and internet. Furthermore, there is a sub-net for administration (Administration) and VPN access (VPN).

Development Environment

Ajour System A/S uses a development environment segregated from the production environment.

To avoid the occurrence of any backdoors to the Ajour system – backdoors that might be exploited for illicit purposes – the development process is supported by training the developers in secure development.

The development process is compared to the ten biggest challenges defined by OWASP (https://owasp.org/www-project-top-ten/). This entails that every time there is a new development or change in the software, an assessment is made of the changes in relation to the principles of OWASP. Employees engaged in software development at Ajour System A/S are trained in secure development every 6 months.

Managing Supplier Relationships

As provider to critical parts of the operation environment, Ajour System A/S monitors on an annual basis, whether the hosting suppliers live up to requirements and SLA for their services. Ajour System A/S evaluates the supplier's certifications and compare them with our own observations. Subsequently, Ajour System A/S will assess, whether the supplier lives up to the agreed services, and whether there is reason to bring up any aspects with them.

All suppliers to Ajour System A/S should always pursue the following policies:

1) Comply with GDPR and other legal requirements
2) Have implemented ISAE 3402 or similar standard for IT security

IT Security Incident Management

Security incidents and weaknesses in Ajour System A/S' systems must be reported in a way that makes it possible to make timely corrections.

All employees at Ajour System A/S are aware of the procedure reporting of different types of incidents and weaknesses that might make an impact on the security of Ajour System A/S' operations. Any security incidents and weaknesses must be reported to the management as soon as possible.

It is the management's responsibility to define and coordinate a structured process ensuring an adequate response to security incidents.

Business Continuity Management

Ajour System A/S' management has the general responsibility for handling security breaches. The Chief Information Security Officer is responsible for establishing procedures ensuring fast, efficient, and methodical management of security breaches.

All employees at Ajour System A/S are responsible for reporting information security breaches. Employees must be instructed that everybody is responsible for reacting on incidents exhibiting signs that might threaten security or result in losses.

Compliance with the Role as Data Processor

Ajour System A/S' management team is responsible for ensuring that all relevant legal and contractual requirements are identified and properly complied with. Relevant requirements include, inter alias:

- General Data Protection Regulation (GDPR)
- The Danish Data Protection Act
- Data Processor Agreements

In addition, the management team reviews all Ajour System A/S' security policies on a regular basis.

EU General Data Protection Regulation (GDPR)
Ajour System A/S' IT services support the customers' work processes. Ajour System 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 Regulation and Danish additional regulation (The Danish Data Protection Act), Ajour System A/S is the Data Processor, and the customer is the Data Controller.

Ajour System A/S has ensured relevant contracts with all key stakeholders (including customers, business partners, key suppliers etc.) to ensure compliance with law and regulations. In addition, Ajour System A/S works together with the customers to ensure that the customers are aware of and comply with the relevant GDPR requirements.

Privacy and protection of personal data
As mentioned above, Ajour System A/S is the customers' Data Processor, given that the customers are offered an IT service to which they can transfer and process data that might contain personal data. Ajous System A/S is not responsible for any data the customers produce using Ajour System A/S software. Based on the categories and confidentiality of the types of data entrusted by the customers to processing, Ajour System A/S must put all necessary security measures required into practice to ensure an appropriate level of security.

Below is a description of Ajour System A/S' procedures of how to operate as Data Processor according to directions from the Data Controllers.

Data Processor Agreements
Ajour System A/S enters Data Processor Agreements (DPA) with all our customers. The Data Processor Agreement is an established procedure when entering a contract, and Ajour System A/S' own model contract is used. These contracts outline role and responsibilities in relation to the roles as Data Processor and Data Controller.

As data processor, Ajour System A/S is subject to a special responsibility defined in the General Data Protection Regulation. This includes, inter alia, the demand to:

- Record the categories of personal data processed in the various IT services
- Describe the technical and organizational security measures undertaken to safeguard the personal data.
- Contribute to the fulfilment of the customer's obligation in relation to the Data Subject's rights (see Section 3 in the EU General Data Protection Regulation).
- Put expertise at the customer's disposal to ensure compliance with Articles 32 – 34 of the GDPR
  - 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.
- Register name and contact information of suppliers who are sub-processors.
- Ensure that the customer's requirements regarding processing of personal data are in line with the demands to the sub-processor.

Decision of purpose and legal basis
As data processor, Ajour System A/S works with personal data based on the customers' directions describing the restrictions regarding the limitations of the purpose for the use of data.

The data controller is responsible for ensuring the legal basis for processing the personal data in question.

Access to the data in customer instances
Ajour System A/S offers solutions as Software as a Solution operated by Ajour System A/S' DevOps team. Development, tests, and release are handled by Ajour System A/S' own Development Department or by suitable subcontractors. In this way, the DevOps Department takes on the full responsibility for processing the customers' data. In general, employees have only access to customer data, if their specific work tasks call for such access.

Ajour System A/S has laid down principles for employees' access to and work with customers' data:

- There is only access to customer data when the employee has 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.

Significant Changes in Relation to IT Security

Ajour System A/S keeps an incident log documenting changes in hardware, software, and other incidents in the production environment. Likewise, if an anomaly occurs in the operation, it is documented in the incident log.

The Customers' Responsibility (Complementary Customer Controls)

This chapter describes the general framework for Ajour System A/S' services, which means that agreements with individual customers have not been taken into consideration.

The customers themselves are responsible for the business systems and user systems operated via Ajour System A/S' solution. The customers are responsible for securing the necessary controls in connection with system development, acquisition and change management.

The customers are responsible for data transmission to Ajour System A/S. The customer must ensure the controls necessary in connection with this control objective.

Ajour System A/S' continuity management is constructed based on an overall contingency plan that describes the approach and procedures to be applied if recovery of Ajour System A/S' solutions is needed.

Significant Changes during the Control Period

Ajour System A/S was acquired by EG A/S as of 1 April 2022. Ajour System A/S continues as a separate legal entity with own CVR no.

Ajour System A/S moved office address from Sanderumvej 16B, 5250 Odense SV to Østerbro 5B, 5000 Odense C as of 13 June 2022. Notice of termination regarding the lease of the office premises on Sanderumvej was given as of the same date.

Ajour System A/S has after this date a lease of server room and office.

The server room at Sanderumvej 16B was transferred to hosting environment at EG A/S (Team Blue) on 3 December 2022. The equipment at Sanderumvej was disposed of on 15 December 2022 and notice of termination regarding lease of server room and office was given on 19 December 2022.

APPENDIX 1:

Ajour System A/S has worked with the following control objectives and security measures from ISO27002:2017

5. Information Security Policies

5.1. Directions for managing information security

6. Organization of Information Security

6.1. Internal organization

6.2. Mobile devices and teleworking

7. Human Resources Security

7.1. Prior to employment

7.2. During employment

7.3. Termination and change of employment

8. Asset Management

8.1. Responsibility for assets

8.2. Information classification

8.3. Media handling

9. Access Control

9.1. Business requirements of access control

9.2. User access management

9.3. User responsibilities

9.4. System and application access control

11. Physical and Environmental Security

Limited responsibility

11.1. Secure Areas

11.2. Equipment

12. Operations Security

Limited responsibility

12.1. Operational procedures and responsibilities

12.2. Protection from malware

12.3. Backup

12.4. Logging and monitoring

12.5. Operational software management

12.6. Vulnerability management

12.7. Considerations regarding audit of Information systems

13. Communications Security

Limited responsibility

13.1. Network security management

13.2. Information transfer

14. System acquisition, Development, and Maintenance

14.1. Security requirements of information systems

14.2. Security in development and support processes

14.3. Test data

15. Supplier Relationships

15.1. Information security in supplier relationships

15.2. Supplier service delivery management

16. Information Security Incident Management

16.1. Management of information security incidents and improvements

17. Information Security Aspects of Business Continuity Management

17.1. Information security continuity

17.2. Redundancies

18. Compliance

18.1. Compliance with legal and contractual requirements

Limited responsibility

Responsibility for compliance with the control objective is divided between Ajour System A/S and the subcontractors.

See description of controls in relation to covering the control risk, including how Ajour System A/S continually supervises operations security at subcontractors.

CHAPTER 3:

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

For the customers / users of Ajour System A/S services and their auditors

Scope

We have been engaged to report on Ajour System A/S’ description in Chapter 2 (incl. Appendix 1), which is a description of the control environment in connection with the operations of Ajour System A/S SaaS solutions, see Data Processor Agreements with customers, throughout the period April 1st 2022 to March 31st 2023, as well as on the design and function of controls regarding the control objectives stated in the description.

We express our opinion with reasonable assurance.

The report is based on a partial approach, which means this report does not include the IT security controls and control objectives related to use of external business partners. The report does not include control or supervision of subcontractors in relation to Ajour System A/S’ SaaS solutions. These subcontractors are listed in detail in Data Processing Agreements with the customers.

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

Ajour System A/S’ responsibility

Ajour System 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 ISQM 1 and thus sustain a comprehensive system of quality management, including documented policies and procedures for compliance with ethical rules, professional standards as well as requirements in force under existing laws and additional regulation.

Auditor’s responsibility

Our responsibility is to express an opinion, based on our procedures, on Ajour System A/S' description and on the design and operation of controls related to the control objectives stated in the said description. We have conducted our engagement in accordance with ISAE 3402, Assurance Reports on Controls at a Service Organisation, issued by the IAASB. The standard requires that we comply with ethical requirements and that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and whether the controls in all material aspects are appropriately designed and operate effectively.

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

Our procedures included testing the operating effectiveness of such controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description have been achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified and described by Ajour System A/S in Chapter 2 (including Appendix 1).

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

Limitations of controls at Ajour System A/S

Ajour System A/S' description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment. Moreover, because of their nature, controls at Ajour System A/S may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at the service organisation may become inadequate or fail.

Opinion

Our opinion is based on the matters outlined in this report. The criteria on which our opinion is based are those described in Chapter 1 under Letter of Representation. In our opinion,

a) The description fairly presents the control environment for the operation of Ajour System A/S' SaaS solutions, such as it was designed and implemented throughout the period April 1st 2022 to March 31st 2023 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 April 1st 2022 to March 31st 2023; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved in all material respects, had operated effectively throughout the period April 1st 2022 to March 31st 2023.

Description of tests of controls

The specific controls tested and the nature, timing and findings of those tests are listed in Chapter 4.

Intended users and purpose

This report and the description of the test of controls in Chapter 4 are solely intended for Ajour System A/S' customers and their auditors, who have sufficient understanding to consider them along with other information, including information about the customers' own control measures, which the customers 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.

Søborg, July 13th 2023

Beierholm
Limited Partnership Company
CVR-nr. 32 89 54 68

Kim Larsen	Allan Nielsen
State-authorized Public Accountant	Senior Consultant, IT Audit

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 ISO27001 and 27002:2017.

With respect to the period, we have tested whether Ajour System A/S has complied with the control objectives throughout the period April 1st 2022 to March 31st 2023.

Below the grey field are three columns:

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

The Tests Performed

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

Inspection	Reading of documents and reports containing information about execution of the control. This includes, inter alia, reading and deciding about reports and other documentation in order to assess, 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 Ajour System 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 - INTRODUCTION:

Risk Assessment and Management

The risk assessment must identify and prioritise the risks based on the operation of Ajour System A/S' SaaS solutions. The findings are to contribute to the identification and prioritisation of management interventions and security measures necessary to address relevant risks.

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Through a risk assessment, risks have been identified and prioritised. The Ajour System A/S' SaaS solutions defined in the description are used as basis for the assessment. The findings contribute to the identification and prioritisation of management interventions and security measures necessary to address relevant risks.	We have requested and obtained the relevant material in connection with the audit of risk management. We have checked that regular risk assessments are carried out for Ajour System A/S' SaaS solutions in relation to business conditions and their development. We have checked that the risk assessment is deployed down through the company's organisation. We have checked that the company's exposure is managed on a current basis and that relevant adaptations of consequences and probabilities are made regularly.	During our test, we did not identify any material deviations.

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 is maintained, taking the current risk assessment into consideration.

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
There is a written strategy covering, among other things, Management's security objectives, policies and overall action plan. The IT security policy and accompanying supporting policies are approved by the company's Management, and then deployed down through the company's organisation. The policy is available for all relevant employees. The policy is re-evaluated according to planned intervals.	We have obtained and audited Ajour System A/S' latest IT security policy. During our audit, we checked that maintenance of the IT security policy is conducted on a regular basis. At the same time, we checked during our audit that the underlying supporting policies have been implemented. We have checked that the policy is approved and signed by the company's management and made available for the employees.	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, among other things, ensure compliance with security measures, including continuous updating of the overall risk assessment.

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Organisational responsibility for IT security has been placed, documented and implemented. The IT security has been coordinated across the company's organisation.	Through inspection and tests, we have ensured that the organisational responsibility for IT security is documented and implemented. We have checked that the IT security is deployed across the organisation in relation to Ajour System A/S SaaS solutions. By making interviews, we have checked that the person responsible for IT security knows his/her role and responsibilities.	During our test, we did not identify any material deviations.
Risks in relation to use of mobile devices and teleworking have been identified.	We checked that formal policies and security measures exist in connection with the use of mobile devices and teleworking. On a test basis, we have inspected that the policy and security measures are implemented regarding employees using mobile devices. Regarding the use of teleworking at Ajour System A/S, we have checked whether appropriate security measures have been implemented thus this area is covered in relation to the risk assessment of the area.	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.

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Based on the specified work processes and procedures, it is ensured that all new employees are informed of their specific responsibilities and roles in connection with their employment at Ajour System A/S. This includes the framework laid down for the work and the IT security involved. Security responsibilities, if any, are determined and described in job descriptions and in the form of terms and conditions in the employment contract terms. The employees are familiar with their professional secrecy based on a signed employment contract.	We have verified that routines and procedures developed by Management in connection with start of employment and termination of employment have been adhered to. Based on random samples, we have tested whether the above routines and procedures have been complied with in connection with start of employment and termination of employment. By making interview, we have checked that employees of significance to Ajour System A/S' services are familiar with their professional secrecy. Through enquiries and samples from employment contracts, we have checked that Ajour System A/S employees are familiar with their professional secrecy. We have ensured that Ajour System 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 Ajour System A/S.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 8:

Asset Management

Necessary protection of the company’s information assets must be ensured and maintained, all the company’s physical and functional assets related to information must be indentified, and a responsible owner appointed. The company must ensure that information assets related to Ajour System A/S’ SaaS solutions have an appropriate level of protection.

There must be reassuring controls to ensure that data media are properly disposed of when no longer needed, in accordance with formal procedures.

Ajour System A/S’ control procedures	Auditor’s test of controls	Test findings
All information assets have been identified and an updated list of all significant assets has been established. An “owner” of all significant assets is appointed in connection with the operation of Ajour System A/S services.	We have examined and checked the company's central IT register for significant IT entities in connection with the operation of Ajour System A/S’ SaaS solutions. We have controlled that risk assessments have been conducted for new assets. By enquiries, we have checked that Ajour System 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 are classified based on business value, sensitivity and need for confidentiality.	We have controlled that there is an appropriate division of assets for Ajour System A/S’ SaaS solutions. In this connection, we have controlled, whether internal procedures/routines regarding ownership to applications and data are complied with.	During our test, we did not identify any material deviations.
Procedures for dealing with destruction of data media are established.	We have: • Asked Management which procedures/ control activities are performed regarding data media. • On a sample basis gone through the procedures for destruction of data media.	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.

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Documentation and updated directions exist for Ajour System A/S access control.	We have: • asked Management, whether access control procedures have been established at Ajour System A/S. • verified on a test basis that access control procedures exist and have been implemented; see Ajour System A/S' directions. • by interviewing key staff and by inspection on a test basis, we have verified that access control for the operations environment comply with Ajour System 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. Granting and application of extended access rights are limited and monitored.	We have by inspection on a test basis verified: • that adequate authorisation systems are used in relation to access control at Ajour System A/S. • that the formalised business procedures for granting and discontinuing user access have been implemented in Ajour System 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: • that formal management follow-up is performed on registered users with extended rights. • that formal management follow-up is performed on registered users with ordinary rights.	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.

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
The granting of access codes is controlled through a formalised and controlled process, which ensures, among other things, that standard passwords are changed.	We have asked Management whether procedures granting access code have been established at Ajour System A/S. By inspection on a test basis, we have verified: • that an automatic systems control takes place, when access codes are granted to check that passwords are changed after first login. • that standard passwords are changed in connection with implementation of systems software, etc. • 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. Quality requirements have been specified for passwords, which must have a minimum length (8 characters), requirements as to complexity and maximum duration (max 180 days.	We have asked Management whether procedures ensuring quality passwords in Ajour System A/S are established. By inspection on a test basis, we have verified that appropriately programmed controls have been established to ensure quality passwords complying with the policies for: • minimum length of password • complexity of password • maximum life of password	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 11:

Physical Security

Access to the company's information processing facilities must be protected to prevent unauthorized physical access, damage and interference to the organisation's information, equipment and information processing facilities. Measures must be established to prevent loss, damage, theft or compromise of assets and interruption to Ajour System A/S' assets. These measures should also encounter supporting utilities and destruction of old or damaged equipment.

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Secure physical perimeters of buildings and offices has been established and protected against unauthorised access.	We have asked Management whether all relevant operation procedures are implemented. In connection with our audit of the individual areas of operation, verified by observation that perimeters of buildings and offices are protected against unauthorised access.	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.

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
The operations procedures for business-critical systems are documented, and they are available to staff with work-related needs. Management has implemented policies and procedures to ensure satisfactory segregation of duties.	We have: • Asked Management whether all relevant operation procedures are documented. • In connection with our audit of the individual areas of operation, verified on a test basis that documented procedures exist and that there is concordance between the documentation and the procedures actually performed.	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. Continuous capacity projection is performed based on business expectations for growth and new activities and the capacity demands derived hereof.	We have: • Asked Management about the procedures and control activities performed. • Verified 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 12:

Operations Security

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.

Ajour System A/S' control procedures	Auditor's test of control procedures	Test findings
Preventive, detecting and remedial security and control measures have been established, including the required training and provision of information for the company's users of information systems against malicious software.	We have: • enquired about and inspected the procedures/ control activities performed in the event of virus attacks or outbreaks. • enquired about and inspected the activities meant to increase the employees' awareness of precautions against virus attacks or outbreaks. • Verified that anti-virus software has been installed on servers and security scans are performed on a regular basis.	During our test, we did not identify any material deviations.

Control objective: Backup

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

Ajour System A/S' control procedures	Auditor's test of controls	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: • asked Management about the procedures/ control activities performed. • examined backup procedures on a test basis to confirm that these are formally documented. • examined backup control reports to confirm that backup has been completed successfully and that failed backup attempts are handled on a timely basis.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 12:

Operations Security

Control objective: Logging and monitoring

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

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Operating systems and network transactions or activities involving special risks are monitored. Abnormal conditions are examined and resolved on a timely basis. Audit logs are activated on all systems. Only in the event of suspected or identified abuse of the systems, users are actively monitored.	We have: • asked Management about the procedures/ control activities performed and ensured that logging parameters are set up so that actions performed by users with elevated privileges are logged. • controlled that abnormal conditions are examined and resolved. • verified that audit logs are activated and are subject to sufficient follow-up.	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.

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Changes in the operation environment comply with established procedures.	We have asked Management, whether procedures for patch management are established. By inspection on test basis, we have verified that • adequate procedures are applied, when controlled implementation of changes to the production environment is performed. • changes to operation environment comply with directions in force, including correct registration and documentation of applications about changes.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 12:

Operations Security

Control objective: Managing operations software and managing vulnerability

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

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Changes in existing user systems and operation environments comply with formalised procedures and processes.	By inspection on test basis, we have verified that adequate procedures are applied for controlled implementation of changes in the production environments, including that demands to the patch management controls ensure that: • applications for change are registered and described. • all changes are subject to formal impact assessments before implementation. • systems affected by changes are identified. • Documented test of changes is performed before put into operation • documentation is updated reflecting the implemented changes in all material respects.	During our test, we did not identify any material deviations.
The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	We have asked Management, whether procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests. By inspection on test basis, we have verified that • documentation exists regarding regular testing of the technical measures established. • any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner and communicated to the data controllers as appropriate.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 13:

Communications Security

To ensure protection of information in networks and support of information processing facilities.		
Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Networks must be protected against threats in order to secure network based systems and the transmitted data. Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	It has been checked that necessary protection against unauthorised access is implemented, including: • Appropriate procedures for managing network equipment are established. • Managing the company's network is coordinated in order to ensure optimal utilisation and a coherent security level. • Ensured that connections for data communication with the internet are established via more than one ISP supplier. • That encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	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. 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. By inspection on a test basis, we have ensured: • that appropriate framework for managing cyber-attacks is devised. • that plans for managing the threat are devised and implemented. • that the plans include cross-organisational collaboration between internal groups.	During our test, we did not identify any material deviations.

KONTROLMÅL 14:

(System acquisition), Development and Maintenance

Ensure that Ajour System A/S' SaaS solutions are managed using suitable IT security measures, including appropriate segregation of production and development environment.		
Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Ajour System A/S has defined formal control procedures for system acquisition and development process for system development and maintenance. All changes, meant to be put into operation in the production environment, must be approved before released to production environment. Software development must be placed in independent test environments.	We have: • asked Management, whether a general quality management model for managing software development is devised or does exist. • in connection with the audit checked the existence of procedures and routines for rolling out software changes. The control environment for the development platform is based on the same IT security structure as stated for the production environment. User management ensures suitable control measures in connection with managing the logical access control. We have checked that the different user groups are controlled at set intervals. We have checked the existence of procedures for segregation of the production environment and the environment for development and maintenance.	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.

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Risks related to external business partners are identified, and security in third-party agreements are managed.	We have verified that in connection with the use of external business partners there are formal cooperation agreements. On a test basis, we have inspected that the cooperation agreements with external suppliers comply with the requirements about covering relevant security conditions in relation to the individual agreement.	During our test, we did not identify any material deviations.
Monitoring must be conducted on a regular basis, including supervision of external business partners.	We have ensured that there are appropriate processes and procedures for ongoing monitoring of external suppliers. We have checked that ongoing supervision is conducted by means of independent auditor's reports.	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.

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Security incidents are reported to Management as soon as possible, and the handling is performed in a consistent and efficient way.	We have asked Management whether procedures are established for reporting security incidents. We have verified that procedures and routines are devised for reporting and handling of security incidents, and that the reporting is submitted to the right places in the organisation. We have verified that the responsibility for the handling of critical incidents is clearly delegated, and that the related routines ensure that security breaches are handled expediently, efficiently and methodically.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 17:

Information Security Aspects of Business Continuity Management

Business continuity management is to 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.

Ajour System A/S’ control procedures	Auditor’s test of controls	Test findings
A consistent framework has been established for the company's contingency plans to ensure that all the plans are coherent and meet all security requirements and to determine the prioritisation of tests and maintenance.	We have asked Management whether business continuity management has been devised for Ajour System A/S SaaS solutions. By inspection on a test basis, we have verified: • that appropriate framework for preparation of business continuity management has been established • that contingency plans are prepared and implemented • that the plans include business continuity management across the organisation • that the plans include appropriate strategy and procedures for communication with the stakeholders of services Ajour System A/S. • that contingency plans are tested on a regular basis • that maintenance and reassessment of the total basis for business continuity management is undertaken on a regular basis.	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 the agreements for processing personal data.

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
A uniform framework is established in the form of standard contracts, Service Level Agreements, as well as Data Processor Agreements or the like, containing an outline of the basis for processing personal data.	We have controlled the existence of updated procedures in writing for processing personal data, and that the procedures include requirements to legal processing of personal data.	During our test, we did not identify any material deviations.
The data processor only processes personal data stated in the instructions from the data controller.	We have controlled that Management ensures that processing of personal data is solely performed in accordance with Directions. We have checked, using a sample of personal data processing operations that these are conducted consistently with instructions.	During our test, we did not identify any material deviations.
Management immediately informs the Data Controller, if Directions in the Data Processor's view is contrary to the General Data Protection Regulation or data protection provisions according to other EU legislation or the national legislation of the member states.	We have controlled that Management ensures that processing is reviewed and the existence of formalised procedures securing that processing of personal data is not performed against the EU General Data Protection Regulation or other legislation. We have controlled the existence of procedures for informing the Data Controller in cases, when processing of personal data is deemed to be against legislation. We have controlled that the Data Controller was informed in cases in cases where the processing of personal data was evaluated to be against legislation.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 18:

Compliance with the Role as Data Processor

Data Processing:

Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
There are procedures in writing with requirements about storing and erasing of personal data in accordance with the agreement with the Data Controller. On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.	We have controlled that there are formalised procedures for storing and erasing of personal data in accordance with the agreement with the Data Controller. We have checked that the procedures are updated.	During our test, we did not identify any material deviations.
According to the agreement with the Data Controller, when processing of personal data is finished, data are • Returned to the Data Controller, and/or • Erased, when erasing is not against other legislation	We have controlled that there are formalised procedures for handling the Data Controllers' data, when processing of personal data is finished.	During our test, we did not identify any material deviations.
There are procedures in writing including demands that personal data is only stored in accordance with the agreement with the Data Controller. On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.	We have controlled that there are formalised procedures ensuring that storing and processing of personal data are solely undertaken according to the Data Processing Agreements. We have checked that the procedures are updated. We have controlled on sample basis, whether documentation exists that data processing is conducted in accordance with the Data Processing Agreement.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 18:

Compliance with the Role as Data Processor

The Data Processor's responsibility:

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

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
There are procedures in writing including demands to the Data Processor in relation to use of sub-processors, including demands about Sub-processor Agreements and Directions. On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.	We have controlled that there are formalised procedures regarding the use of sub-processors, including demands about Sub-processors Agreements and Directions. Inspected that procedures are updated.	During our test, we did not identify any material deviations.
The Data Processor has a list of approved Sub-processors including the following information: • Name • CVR.no. • Address • Outline of the processing For processing personal data, the Data Processor solely uses Sub-processors, who are specifically or generally approved by the Data Controller.	We have controlled that the Data Processor has a total and updated list of approved Sub-processors used. Inspected that the list as a minimum includes the required information about each Sub-processor. We have controlled on sample basis from the Data Processor's list of Sub-processors that it is documented that the Sub-processor's data processing is included in the Data Processing Agreements – or in other ways approved by the Data Controllers.	During our test, we did not identify any material deviations.
The Data Processor has placed the same data protection obligations on the Sub-processors as the obligations included in the Data Processor Agreement or similar document with the Data Controller.	We have controlled the existence of signed Sub-processor Agreements with all Sub-processors used and included in the Data Processor's list. We have controlled on sample basis that the Sub-processor Agreements include the same demands and obligations as stated in the Data Processing Agreements between the Data Controllers and the Data Processor.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 18:

Compliance with the Role as Data Processor

Assisting the Data Controller:

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

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Written procedures exist which include a requirement that the Data Processor must assist the Data Controller in relation to the rights of Data Subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have controlled that formalised procedures are in place for the Data Processor's assistance to the Data Controller in relation to the rights of Data Subjects. Inspected that procedures are up to date.	During our test, we did not identify any material deviations.
The Data Processor has established procedures in so far as this was agreed that enable timely assistance to the Data Controller in handing out, correcting, deleting or restricting processing as well as providing information about the processing of personal data to Data Subjects.	We have controlled that the procedures in place for assisting the Data Controller include detailed procedures for: • Handing out data; • Correcting data; • Deleting data; • Restricting the processing of personal data; • Providing information about the processing of personal data to Data Subjects. Inspected documentation that the systems and databases used support the performance of the said relevant detailed procedures.	During our test, we did not identify any material deviations.

Records of processing activities:

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

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
Records exist of processing activities for Ajour System A/S' SaaS solutions.	We have controlled documentation displaying the existence of records for processing activities.	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 disclosing that the records of the processing activities are updated and correct.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 18:

Compliance with the Role as Data Processor

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

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

Ajour System A/S' control procedures	Auditor's test of controls	Test findings
There are procedures in writing - updated at least once a year – describing how to manage personal data security breaches, including timely communication to the Data Controller.	We have controlled the existence of updated procedures in writing regarding managing personal data security breaches, including description of timely communication to the Data Controller.	During our test, we did not identify any material deviations.
Data Processor ensures recording of all personal data security breaches.	We have controlled documentation disclosing that all personal data security breaches are recorded at the Data Processor.	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.