Assurance report

Emply ApS

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to the data processing agreement with customers throughout the period from 1 April 2022 to 31 March 2023

July 2023

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Table of Contents

Section 1: Emply ApS' description of processing activity for the supply of Emply ApS' services 3

Section 2: Emply ApS' statement 10

Section 3: Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to Emply ApS' data processing agreement with customers 12

Section 4: Control objectives, controls, tests, and results hereof 14

Section 5: Supplementary information from Emply ApS 33

Section 1: Emply ApS' description of processing activity for the supply of Emply ApS' services

The purpose of this description is to provide information to Emply ApS' customers and their auditors regarding the requirements of ISAE 3000, the International Standard on Assurance Engagements (ISAE 3000).

The purpose of this description is to cover the technical and organizational measures involved in the operation of Emply ApS' Software-as-a-Service solutions (SaaS solution).

As a supplement to the above description, a separate section (Compliance with the role as a data processor) has been added with a description of key requirements in connection with the role as a data processor, combined with general requirements from data processing agreements.

In addition, the description provides information about the controls used for the operation of Emply ApS' SaaS solution and how they are implemented.

Description of Emply ApS

Emply was founded in Copenhagen in 2010. The SaaS solution was developed to serve the needs of HR employees for a modern solution. The platform can be adapted to any company regardless of industry, size, organizational structure or HR workflows, no matter where in the world companies are located. Today, Emply is available in more than 16 languages and is used in more than 50 countries.

Emply ApS provides proprietary Software-as-a-Service, which includes 100% operations, service and support, consulting services and training. Emply provides ongoing customization of functionality and integrations so that the systems meet customer requirements as well as current legislation and regulations.

Emply ApS' SaaS solution is currently delivered to private and public companies. The solution is operated in Denmark and run as a private cloud solution at GlobalConnect in Glostrup. Emply ApS operates the solution and GlobalConnect provides "only" housing, power and internet access as well as the backup solution. During the period, GlobalConnect has been replaced by Cibicom. During the period, NetNordic A/S has become the Backup center.

Business strategy / IT-security strategy

It is Emply ApS' strategy that the necessary security must be built into the business so that the company does not incur unacceptable risks.

The purpose of the security policy is also to indicate to everyone who has a relationship with Emply that the use of information and information systems is subject to standards and guidelines.

Maintaining and expanding a high level of security is an essential prerequisite for Emply to appear credible both nationally and internationally.

To maintain Emply ApS' credibility, it must be ensured that information is treated with the necessary confidentiality and that complete, accurate and timely processing of approved transactions takes place.

IT systems are considered Emply ApS' most critical resource, second only to its employees. Therefore, emphasis is placed on reliability, quality, compliance with legal requirements and user-friendliness.

Effective protection against IT security threats must be created to ensure the best possible protection of Emply ApS' image and the employees' safety and working conditions. The protection must be directed against natural, technical and man-made threats. All persons are considered as possible causes of security breaches; i.e. no employee should be above the security regulations.

The goals are therefore to:

- Achieve high reliability with high uptime percentages and minimized risk of major breakdowns and data loss - ACCESSIBILITY
- Achieve correct functioning of the systems with minimized risk of manipulation and errors in both data and systems – INTEGRITY
- Achieve confidential processing, transmission and storage of data – CONFIDENTIALITY
- Achieve mutual security of the parties involved – AUTHENTICITY

- Achieve a security of mutual and documentable contact – INDISTINCTNESS

Information security level that, as a minimum:

- Complies with applicable legislation
- Follows good business practices
- Meet customer needs, requirements and expectations of a professional supplier

The Danish Data Protection Act and the EU General Data Protection Regulation constitute the legislative framework for the processing of personal data in IT services. Data processing agreements are entered into between customers and Emply ApS.

Our responsibility is to take the necessary technical and organizational measures to ensure that personal data is processed in a secure and responsible manner.

To ensure a consistent delivery that meets the industry's best standards, we have chosen to support the operation of our SaaS solutions with an audit process to meet the requirements of an ISAE 3000 statement. Emply ApS' SaaS solutions are supported by a housing supplier (GlobalConnect) that provides an ISAE 3402 statement. During the period, GlobalConnect has been replaced by Cibicom, which has also delivered an ISAE 3402 declaration. During the period, NetNordic A/S has become a Backup center and has also delivered an ISAE 3402.

The audit process is repeated annually and the result in an audit statement is presented to existing and potential new customers. The statement can contribute to customers' (data controller) control of whether Emply complies with the instructions in the data processing agreement enteredinto.

Emply ApS has around the IT security strategy used methods to implement the relevant measures in the following areas:

- Informationsecurity policy
- Organization of IT security
- Employee security
- Access conditions
- Physical security and supplier relationships
- Operational security
- Network security
- Development environment
- Security incident management
- Emergency management
- Compliance with the role as a data processor (Compliance)

Risk management at Emply ApS

It is Emply ApS' policy that the risks arising from the company's activities must be hedged or limited to such a level that the company will be able to maintain normal operations.

Emply has incorporated procedures for risk assessment of the business. This ensures that the risks associated with the services we provide are minimized to an acceptable level.

Risk assessment is carried out periodically, as well as when changes are made to existing systems or new systems are implemented and assessed. The risk assessment is part of the IT Security Officer's responsibility.

Information security policy

Emply's management has the day-to-day responsibility for IT security, ensuring that the overall requirements and framework for IT security are met. The IT security policy must be revised at least once a year.

Emply ApS' IT security policy has been prepared with reference to the above and applies to all employees and all deliveries. In the event of an error or security breach in our operating environment, the error/security hole is rectified immediately. Specific procedures are followed to ensure transparency, preventive and corrective actions.

All servers, storage and network devices are documented in Emply ApS. All changes to our system are logged here. Configuration files for network devices (firewall, routers, switches and the like) are stored and accessible.

The security policy is designed so that all employees at Emply ApS have a common set of rules. This ensures a stable operating environment and a high level of security. We make continuous improvements to policies, procedures and operations.

Emply ApS' organization and organization of IT-security

Emply was acquired in January 2021 by Lessor Group, the market-leading provider of payroll, HR, time and attendance, and scheduling software for small and large businesses in Denmark and Germany. They have 180 employees and more than 65,000 companies today use one or more systems from Lessor Group.

Since 2018, Lessor Group has been owned by Paychex, Inc, the leading provider of integrated HCM solutions in the US market. Emply ApS is 100% owned by Lessor Group.

Emply ApS' organizational structure:

Management is responsible for the day-to-day running of both the organization and IT.

Sales & Marketing is the department that handles all communication to customers in connection with sales, software demonstrations, attending trade fairs, making offers and closing orders.

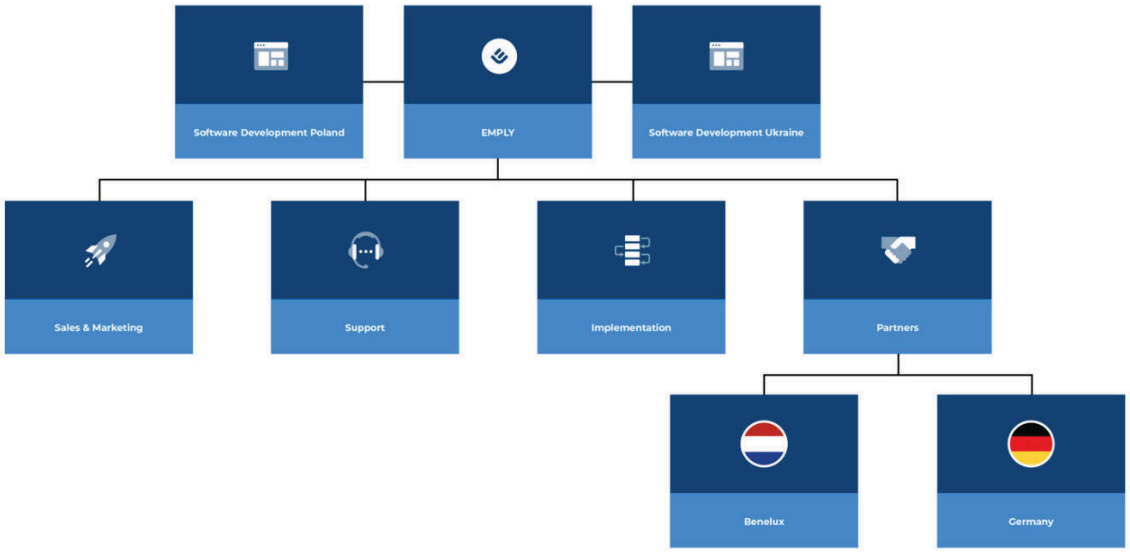
Support is the department that provides a high level of support to all our customers.

Implementation is the department that ensures that all new customers have a positive experience when starting at Emply.

Partners is the department that ensures that Emply can be sold and delivered outside Denmark.

Software Development Ukraine and Poland are the departments that develop Emply software. Ukraine deals exclusively with software development and testing. Data processing takes place in Denmark. For special tasks, such as re-creation of databases, etc. Emply can, with the customer's consent, give Polish developers access to solve customer-related tasks.

Responsibility for IT security in Emply ApS is placed in the Lessor Group's security organization. The organizational anchoring of IT security is a natural part of the management's area of responsibility.



Employee safety

Emply ApS' employees are an important prerequisite for Emply ApS' business. It is important to maintain and develop the skills we have at our disposal so that we can adapt to our customers' needs. We work with an annual KPI target, which enables us to work as a team.

Emply ApS uses its proprietary SaaS solution. New employees go through an introduction to all areas of Emply. Both existing and new employees go through Emply ApS' policies and procedures. This is done for all employees.

All Emply ApS employees have a confidentiality agreement that also covers how customer data is processed. Emply ApS employees have limited opportunities to work from other facilities.

Access conditions

Only authorized Emply users/employees have access to Emply systems. Access to the operating environment is granted according to purpose. Rights and access to information needed to perform their tasks/roles in the best possible way are granted.

Access management is done by Emply management.

Physical security and supplier relationships

GlobalConnect and NetNordic A/S annually deliver an ISAE 3402 on physical security and an ISAE 3000 on network and information security.

Emply is delivered as a private cloud service that runs on a virtual Microsoft web farm. The application is hosted on multiple virtual machines. Each virtual machine runs on a VMware cluster solution.

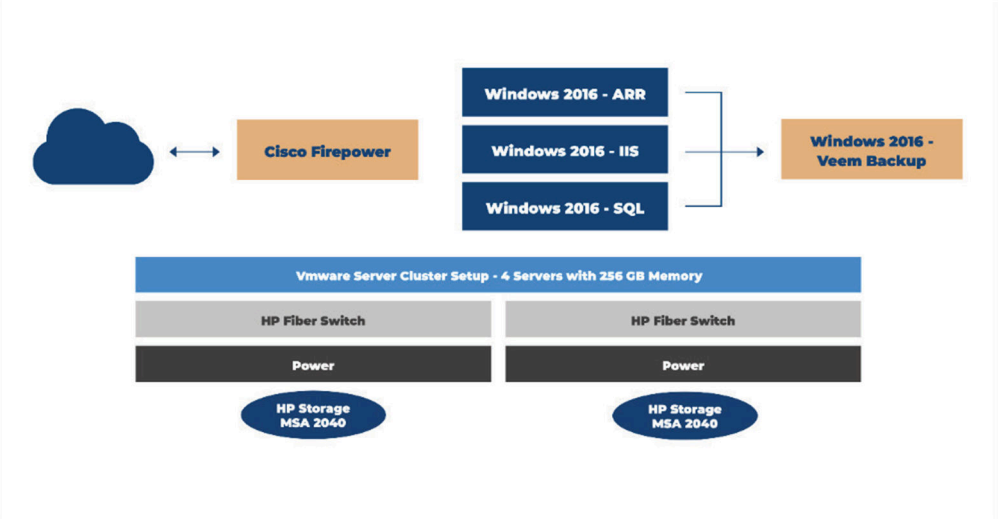
The VMware cluster solution runs on six physical servers and all data is stored in an SD storage system.

The Emply SaaS solution is built with Microsoft.Net. All customers use different SQL databases to ensure a stable and secure software solution. The Emply solution is additionally monitored by several software solutions to achieve a stable production environment.

The Emply solution has several integrations such as SSO (Single Sign-on), ADFS, two-factor authentication and several extended web service APIs in both SOAP and RES. All transactions in Emply ApS are saved and stored in multiple log files.

Operational reliability

Operational tasks are performed by Emply ApS at fixed intervals. Emply ApS also performs checks, maintenance, and operation of all servers.



Monitoring

The operating environment is monitored 24/7/365 via automated service. Server resources (CPU, RAM, disk, disk, network) and availability are monitored. Monitoring also includes relevant IT services such as backups, web and system availability for customers and internal use.

The primary monitoring takes place internally in the operating environment, but to also cover external availability, we have established remote monitoring.

Errors are reported directly to Emply ApS, after which the error is investigated. In the case of critical errors in servers or services, the on-duty operations employee is notified directly.

Customers experiencing operational problems must contact Emply ApS via the agreed support channels, either by phone or via support@emply.com.

We are open for customer inquiries during daytime hours Monday-Thursday from 8:30-16:30 and Friday from 8:30-15:30.

Loggin

Logging is a valuable tool for monitoring, error handling and investigation. As logs contain many different types of information, we can divide them into two levels:

- Systemlog: Emply ApS has developed its own system for monitoring errors.
- User log: All Emply customers have access to the Emply system to see what activities they have carried out as a customer. Here you can search for activities on the customer's own users, specific dates, projects, etc.

Backup

The purpose of backup is to ensure that customer data can be restored accurately and quickly, avoiding unnecessary waiting time. Backups are taken at different levels such as virtual servers, configurations and data. Every Emply customer has their own database, this is done to ensure quick and easy restoration via backup.

All customers' databases are stored as encrypted in the Veem Backup Solution. The backup service is provided by GlobalConnect at the beginning of the period and subsequently by NetNordic. Backups are established daily and stored via dedicated backup servers in the operating environment. Daily backups of customer databases are stored for 14 days. After that, the last backup of each month is stored. Back-ups older than 1 month are automatically deleted.

Patch management

The purpose of patch management is to ensure that all relevant updates such as patches, fixes and service packs from vendors are deployed to protect systems from downtime and unauthorized access, and that the deployment is done in a controlled manner.

Maintenance of Windows operating systems and associated backend systems from Microsoft is handled by Microsoft's built-in WSUS (Windows Server Update Service), where security and critical patches are automatically installed at fixed intervals.

Communication security

Data lines and network security

The connection to the operating environment consists of 2 independent fiber lines. If the primary line breaks down, traffic is automatically routed via the secondary. When the primary is re-established, traffic is routed through it again.

The firewall is rule-based and by default has a "deny all" traffic rule. On top of this, a set of rules has been created that allows specific protocols against a given server grouping. The firewall has a built-in "Load Balancer" that is used to ensure the distribution of the total traffic to multiple servers.

Finally, the firewall performs data packet inspection (IDS). Automated scanning and blocking of traffic based on the vulnerability situation is updated daily.

Development environment

When Emply ApS develops software, dedicated test environments are used from which the software can be run for development and testing. These environments are not the environments used by Emply ApS' customers.

Security incident management

Emply ApS has established procedures for incident management and deviation reporting, including security breaches.

The procedures ensure that work is done systematically, necessary data collection and documentation is carried out, so that there is a good basis for subsequent evaluation.

Management is responsible for defining and coordinating a structured process that ensures an appropriate response to security incidents.

Emergency management

Emply ApS' IT contingency plan must ensure that the IT-dependent business-critical work processes in Emply can be re-established and are functional after a critical incident has directly or indirectly prevented normal operations for a period of time. This is done to ensure stable operation of Emply.

The IT contingency plan must be activated when one or more incidents disrupt or interrupt critical parts of Emply for an extended period of time and the IT systems are not restored during normal operation and troubleshooting within the set timeframe, which is 2 hours within normal working hours and 4 hours outside.

The plan describes how to handle 4 scenarios:

- Physical incidents in the Emply Data Center (fire, water damage or other) that put Emply out of operation,
  fully or partially.
- IT incidents that affect operations at Emply
- IT incidents that affect Emply's IT infrastructure (virus outbreaks and hacker attacks)
- IT incidents involving compromise of Emply with risk of data leakage, where others unauthorized or unintentional access to Emply data or Emply customers' data

Compliance, with the role as a data processor

The management of Emply ApS is responsible for ensuring that all relevant legal and contractual requirements are identified and properly complied with. Relevant requirements can for example be:

- EU General Data Protection Regulation
- Danish Data Protection Act
- Data processing agreement
- Emply's standard client agreement
- Emply's standard client terms of use

The presence of the above agreements, as well as other relevant documents, ensures compliance with relevant legal and contractual requirements.

EU General Data Protection Regulation (GDPR)

Emply's SaaS solution supports customers' HR work processes. Emply ApS does not own the data that the customers collect and store in the SaaS solution, but solely develops and operates the SaaS solution, which the customers use to perform the necessary personal data processing. According to the General Data Protection Regulation and the Danish supplementary provisions (the Danish Data Protection Act), Emply ApS is the data processor and the customer is the data controller.

Data processing agreement

As a data processor, Emply ApS has a special responsibility under the General Data Protection Regulation, implemented as requirements in a data processing agreement. Emply ApS must, among other things:

- Keep records of the categories of personal data processed

- Describe the technical and organizational security measures implemented to protect personal data
- Contribute to fulfilling the Customer's obligations regarding the data subject's rights (cf. Chapter 3 of the EU General Data Protection Regulation)
- Provide expertise to the Customer to ensure compliance with Articles 32-34.
  - Article 32 - Security of processing
  - Article 33 - Notification of personal data breaches
  - Article 34 - Notification of personal data breaches to data subjects
- Inform the customer of the name and contact details of suppliers who are sub-processors.
- Ensure that any requirements from the customer are also reflected in the sub-processor.

As a data processor, Emply ApS works with personal data based on instructions from customers describing the purpose for which data may be used. It is Emply ApS' responsibility to ensure that the data collected is used exclusively for this purpose.

Access to customer data

The Emply solution is a SaaS solution operated by Emply ApS. Testing and releases are handled by Emply ApS itself. Therefore, Emply ApS has full responsibility for the processing of customer data. In general, Emply ApS employees do not have access to customer data unless specific work tasks require it. Only support and the management of Emply ApS have access to customer data.

All employees at Emply ApS have signed a confidentiality agreement with a focus on how we at Emply process customer data.

Changes in the audit period

During the period, GlobalConnect has been replaced by Cibicom and NetNordic A/S has become a Backup center.

Complementary controls at the data controllers

This chapter describes the general conditions of Emply ApS' SaaS solution, which means that the individual customer's agreement is not taken into account.

Emply ApS is not responsible for access rights, including assignment, modification and termination, in relation to the individual customer's users and their access to the SaaS solution. The customer is itself obliged to ensure the necessary controls in relation to this control objective.

The data controllers also have the following obligations:

- to ensure that the personal data is up to date,
- to ensure that the instruction is legal in relation to the applicable personal data law regulation at any given time,
- ensuring that the instruction is appropriate in relation to this data processing agreement and the main service,
- ensuring that the data controller's users are up to date,
- to ensure that the necessary legal basis for processing the present,
- to comply with the obligation to inform data subjects about the exercise of their rights, responding to requests and verifying the identity of data subjects who wish to exercise their rights.

Section 2: Emply ApS' statement

The accompanying description has been prepared for data controllers, who has signed a data processing agreement with Emply ApS, and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with.

Emply ApS uses the following sub-suppliers and sub-processors, InterLogic Danmark ApS and GlobalConnect. This statement does not include control objectives and related controls at Emply ApS' sub-suppliers and sub-processors.

Emply ApS confirms that:

a) The accompanying description, Section 1, fairly presents how Emply ApS has processed personal data for data controllers subject to the Regulation throughout the period from 1 April 2022 to 31 March 2023. The criteria used in making this statement were that the accompanying description:

(i) Presents how Emply ApS' processes and controls were designed and implemented, including:

- The types of services provided, including the type of personal data processed
- The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete, and restrict processing of personal data
- The procedures used to ensure that data processing has taken place in accordance with contract, instructions or agreement with the data controller
- The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality
- The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation
- The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects
- The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed
- Controls that we, in reference to the scope of Emply ApS' services have assumed would be implemented by the data controllers and which, if necessary, in order to achieve the control objectives stated in the description, are identified in the description
- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data

(ii) Includes relevant information about changes in the Emply ApS' services in the processing of personal data in the period from 1 April 2022 to 31 March 2023;

(iii) Does not omit or distort information relevant to the scope of Emply ApS' services being described for the processing of personal data while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Emply ApS' services that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were, in our view, suitably designed and operated effectively throughout the period from 1 April 2022 to 31 March 2023. If

relevant controls with sub-suppliers were operationally effective and data controller has performed the complementary controls, assumed in the design of Emply ApS' controls as of 1 April 2022 to 31 March 2023. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 April 2022 to 31 March 2023.

c) Appropriate technical and organisational safeguards were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the Regulation.

Allerød, 21 July 2023

Emply ApS

Henrik Møller
CEO

Section 3: Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to Emply ApS' data processing agreement with customers

To: Emply ApS and their customers

Scope

We were engaged to provide assurance about a) Emply ApS' description, Section 1, of Emply ApS' services in accordance with the data processing agreement with costumers as data controllers throughout the period from 1 April 2022 to 31 March 2023 and about b) and c) the design and operating effectiveness of controls related to the control objectives stated in the Description.

Emply ApS uses the following sub-suppliers and sub-processors, InterLogic Danmark ApS and GlobalConnect. This statement does not include control objectives and related controls at Emply ApS' sub-suppliers and sub-processors.

We express reasonable assurance in our conclusion.

Emply ApS' responsibilities

Emply ApS is responsible for: preparing the Description and the accompanying statement, Section 2, including the completeness, accuracy, and the method of presentation of the Description and statement, providing the services covered by the Description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior and ethical requirements applicable to Denmark.

Grant Thornton is subject to the International Standard on Quality Control (ISQC 1) [1]and accordingly uses and maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Our responsibilities

Our responsibility is to express an opinion on Emply ApS' Description and on the design and operating effectiveness of controls related to the control objectives stated in that Description, based on our procedures.

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information", and additional requirements under Danish audit regulation, to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed and operating effectively.

An assurance engagement to report on the Description, design, and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its services and about the design and operating effectiveness of controls. The procedures selected

[1] ISQC 1, Quality control for firms that perform audits and reviews of financial statements, and other assurance and related services engagements.

depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not appropriately designed or 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 appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in Section 1.

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

Limitations of controls at a data processor

Emply ApS' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Emply ApS' services that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the *Management's statement* section. In our opinion, in all material respects:

(a) The Description fairly presents Emply ApS' services as designed and implemented throughout the period from 1 April 2022 to 31 March 2023;

(b) The controls related to the control objectives stated in the Description were appropriately designed throughout the period from 1 April 2022 to 31 March 2023; and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from 1 April 2022 to 31 March 2023.

Description of tests of controls

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

Intended users and purpose

This report and the description of tests of controls in Section 4 are intended only for data controllers who have used Emply ApS' services, who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with.

Copenhagen, 21 July 2023

Grant Thornton
State Authorised Public Accountants

Kristian Randløv Lydolph
State Authorised Public Accountant

Martin Brogaard Nielsen
Partner, CISA, CIPP/E, CRISC

Section 4: Control objectives, controls, tests, and results hereof

We conducted our engagement in accordance with ISAE 3000, assurance engagements other than audits or review of historical financial information.

Our test of the functionality has included the control objectives and attached controls, selected by management and which are stated in the control objectives A-I below. Our test has included the controls, we find necessary to establish reasonable assurance for compliance with the articles stated throughout the period from 1 April 2022 to 31 March 2023.

Our statement, does not apply to controls, performed at Emply ApS' sub-suppliers and sub-processors.

Further, controls performed at the data controller are not included in this statement.

We performed our test of controls at Emply ApS by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Emply ApS. The interviews have included questions about, how controls are performed.
Observation	Observing how controls are performed.
Inspection	Reading of documents and reports, including description of the performance of the control. This includes reading and assessment of reports and documents to evaluate whether the specific controls are designed in such a way, that they can the expected to be effective when implemented.
Re-performance	Re-performance of controls to verify that the control is working as assumed.

List of control objectives compared to GDPR-articles, ISO 27701, and ISO 27001/2

Below, control objectives are mapped against the articles in GDPR, ISO 27701 and ISO 270001/2.

Articles and points about main areas are written in bold.

Control activity	GDPR articles	ISO 27701	ISO 27001/2
A.1	5, 26, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*New scope compared to ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.11	**32**	**6.9.6.1**	12.6.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*New scope compared to ISO 27001/2*
B.15	**32**	**6.8**	11.1.1-6
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
C.9	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*New scope compared to ISO 27001/2*
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New scope compared to ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New scope compared to ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3	13.2.1, 13.2.2
G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*

Control activity	GDPR articles	ISO 27701	ISO 27001/2
H.2	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Control objective A - Instructions regarding processing of personal data

Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
A.1	Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure that personal data are only processed according to instructions. We have inspected that the procedures include a requirement to assess at least once a year the need for updates, including in case of changes in the data controller's instructions or changes in the data processing. We have inspected that procedures are up to date.	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	We have inspected that Management ensures that personal data are only processed according to instructions. We have inspected that a sample of personal data processing operations are conducted consistently with instructions.	No deviations noted.
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	We have inspected that formalised procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation. We have inspected that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation. We have inquired if data controllers was informed in cases where the processing of personal data was evaluated to be against legislation.	We have been informed that there have been no cases where the processing of personal data was considered to be in violation of legislation, wherefore we have not tested the effectiveness of the control. No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
B.1	Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure establishment of the safeguards agreed. We have inspected that procedures are up to date. We have inspected that the safeguards agreed on in a sample data processing agreements have been established.	No deviations noted.
B.2	The data processor has performed a risk assessment and based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller.	We have inspected that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. We have inspected that the risk assessment performed is up to date and comprises the current processing of personal data. We have inspected that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment. We have inspected that the data processor has implemented the safeguards agreed with the data controller.	No deviations noted.
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	We have inspected that, for the systems and databases used in the processing of personal data, antivirus software has been installed. We have inspected that antivirus software is up to date.	No deviations noted.
B.4	External access to systems and databases used in the processing of personal data takes place through a secured firewall.	We have inspected that external access to systems and databases used in the processing of personal data takes place only through a secured firewall. We have inspected that the firewall has been configured in accordance with the relevant internal policy.	No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
B.5	Internal networks have been segmented to ensure restricted access to systems and databases used in the processing of personal data.	We have inspected the network policy. We have inspected network diagrams and other network documentation to ensure appropriate segmentation.	No deviations noted.
B.6	Access to personal data is isolated to users with a work-related need for such access.	We have inspected that formalised procedures are in place for restricting users' access to personal data. We have inspected that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need. We have inspected that the technical measures agreed support retaining the restriction in users' work-related access to personal data. We have inspected that access is restricted to the employees' work-related need for a sample of users' access to systems and databases.	No deviations noted.
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	We have inspected that, for systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature. We have inspected that a sample of alarms were followed up on and that the data controllers were informed thereof as appropriate.	No deviations noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	We have inspected that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm. We have inspected that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email. We have inquired about the use of transport layer security.	No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
B.9	Logging has been established in systems, databases, and networks that support the processing of personal data. Log data are protected against manipulation, technical errors and are reviewed regularly.	We have inspected that formalised procedures exist for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data. We have inspected that logging of user activities in systems, databases or networks that are used to process or transmit personal data has been configured and activated. We have inspected that user activity data collected in logs are protected against manipulation or deletion. We have, by sample test, inspected that the content of log files is as expected, compared to the setup and that documentation exists regarding the follow-up performed and the response to any security incidents. We have inspected that documentation exists for the follow-up performed for activities carried by system administrators and others holding special rights.	No deviations noted.
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form. Such use only takes place to accomplish the data controller's purpose according to agreement and on the data controller's behalf.	We have inspected that formalised procedures exist for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. We have, by sample test, inspected that personal data included in development or test databases are pseudonymised or anonymised.	No deviations noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	We have inspected that formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans and penetration tests. We have inspected samples that documentation exists regarding regular testing of the technical measures established.	No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
		We have inspected that any deviations or weaknesses in the technical measures have been responded to in a timely and satisfactory manner.	
B.12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	We have inspected that formalised procedures exist for handling changes to systems, databases, or networks, including handling of relevant updates, patches, and security patches. We have, by sample test, inspected whether a selection of changes, made on service applications have been registered, assessed, prioritized, and implemented in the production environment, according to the Change Management procedure. We have inquired about the change management procedure for IT Operations.	We have inspected that for 13 of 13 change samples no documentation of approval was available. No further deviations noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	We have inspected that formalised procedures exist for granting and removing users' access to systems and databases using to process personal data. We have inspected that the user accesses granted have been authorised and that a work-related need exists for a sample of employees' access to systems and databases. We have – by sample test inspected resigned or dismissed employees to establish whether their access to systems and databases was deactivated or removed on a timely basis. We have inspected that documentation exists that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	No deviations noted.
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	We have inspected that formalised procedures exist to ensure that two-factor authentication is applied in the processing of personal data that involves a high risk for the data subjects.	No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
		We have inspected that users' access to processing personal data that involve a high risk for the data subjects may only take place by using two-factor authentication.	
B.15	Physical access safeguards have been established so as to only permit physical access by authorised persons to premises and data centres at which personal data are stored and processed.	We have inspected that formalised procedures exist to ensure that only authorised persons can gain physical access to premises and data centres at which personal data are stored and processed. We have inspected documentation that, throughout the assurance period, only authorised persons have had physical access to premises and data centres at which personal data are stored and processed.	We have inspected that two shared accounts were created with access cards to the office building which were not closed in a timely manner. No further deviations noted.
B.16	Backup copies of information software and system images are taken and tested regularly in accordance with an agreed backup policy.	We have inspected configuration of backup and we have inspected documentation for the setup. We have inspected that backup is monitored. We have inspected lists of backupfiles and we have inspected documentation for recovery test.	No deviations noted.

Control objective C - Organisational measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
C.1	Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	We have inspected that an information security policy exists that Management has considered and approved within the past year. We have inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No deviations noted.
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	We have inspected documentation of Management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the data processing agreements entered into. We have, by sample test, inspected that the requirements in data processing agreements are covered by the requirements of the information security policy for safeguards and security of processing.	No deviations noted.
C.3	The employees of the data processor are screened as part of the employment process.	We have inspected that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process. We have, by sample test, inspected that the requirements in data processing agreements for screening employees are covered by the data processor's screening procedures.	No deviations noted.

Control objective C - Organisational measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	We have, by sample test, inspected that employees appointed during the assurance period have signed a confidentiality agreement. We have, by sample test, inspected that employees appointed during the assurance period have been introduced to: • Information security policy. • Procedures for processing data and other relevant information.	No deviations noted.
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	We have inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etc. are returned. We have, by sample test, inspected that rights have been deactivated or terminated and that assets have been returned for employees resigned or dismissed during the assurance period.	No deviations noted.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	We have inspected that formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. We have, by sample test, inspected that documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality for employees resigned or dismissed during the assurance period.	No deviations noted.

Control objective C - Organisational measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	We have inspected that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data. We have inspected documentation that all employees who have either access to or process personal data have completed the awareness training provided.	No deviations noted.
C.8	The processor has assessed the need for a DPO and has ensured that the DPO has the adequate professional competence to perform their tasks and are involved in relevant areas.	We have inspected the assessment of the need for a DPO and ensured that the company has assessed the need for a DPO during the period.	No deviations noted.
C.9	The processor keeps a record of categories of processing activities for each data controller. Regularly – and at least annually – an assessment is made of whether the record of categories of processing activities for each controller should be updated.	We have inspected that the categories of processing contains the following information: • the name and contact details of the processor, and the data protection officer • the categories of processing carried out on behalf of each controller • where applicable, transfers of personal data to a third country or an international organisation • where possible, a general description of the technical and organisational security measures.	No deviations noted.

Control objective D - Return and deletion of personal data

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.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. We have inspected that the procedures are up to date.	No deviations noted.
D.2	Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.	We have inspected that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines. We have inspected that documentation exists that personal data are deleted in accordance with the agreed deletion routines in data processing agreements.	No deviations noted.
D.3	Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: • Returned to the data controller; and/or • Deleted if this is not in conflict with other legislation.	We have inspected that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data. We have inquired about the agreed deletion or return of data has taken place for terminated data processing sessions during the assurance period.	No deviations noted.

Control objective E – Storage of personal data

Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
E.1	Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements. We have inspected that the procedures are up to date.	No deviations noted.
E.2	Data processing and storage by the data processor must only take place in the localities, countries or regions approved by the data controller.	We have inspected that the data processor has a complete and updated list of processing activities stating localities, countries, or regions. We have, by sample test, inspected that documentation exists that the processing of data, including the storage of personal data, takes place only in the localities stated in the data processing agreement – or otherwise as approved by the data controller.	No deviations noted.

Control objective F – Use of sub-processors

Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
F.1	Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-data processing agreements and instructions. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions. We have inspected that procedures are up to date.	No deviations noted.
F.2	The data processor only uses sub-data processors to process personal data that have been specifically or generally approved by the data controller.	We have inspected that the data processor has a complete and updated list of sub-data processors used. We have, by sample test, inspected that documentation exists that the processing of data by the sub-data processor is stated in the data processing agreements – or otherwise as approved by the data controller.	No deviations noted.
F.3	When changing the generally approved sub-data processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-data processors used, this has been approved by the data controller.	We have inspected that formalised procedures are in place for informing the data controller when changing the sub-data processors used. We have inspected documentation that the data controller was informed when changing the sub-data processors used throughout the assurance period.	No deviations noted.
F.4	The data processor has subjected the sub-data processor to the same data protection obligations as those provided in the data processing agreement or similar document with the data controller.	We have inspected for existence of signed sub-data processing agreements with sub-data processors used, which are stated on the data processor's list. We have, by sample test, inspected that sub-data processing agreements include the same requirements and obligations as are stipulated in the data processing agreements between the data controllers and the data processor.	No deviations noted.

Control objective F – Use of sub-processors

Procedures and controls are complied with to ensure that only approved sub-data processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
F.5	The data processor has a list of approved sub-data processors.	We have inspected that the data processor has a complete and updated list of sub-data processors used and approved. We have inspected that, as a minimum, the list includes the required details about each sub-data processor.	No deviations noted.
F.6	Based on an updated risk assessment of each sub-data processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-data processor.	We have inspected that formalised procedures are in place for following up on processing activities at sub-data processors and compliance with the sub-data processing agreements. We have inspected documentation that each sub-data processor and the current processing activity at such processor are subjected to risk assessment. We have inspected documentation that information on the follow-up at sub-data processors is communicated to the data controller so that such controller may plan an inspection.	No deviations noted.

Control objective H – Rights of the data subjects

Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting, or restricting information on the processing of personal data to the data subject.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
H.1	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 inspected that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. We have inspected that procedures are up to date.	No deviations noted.
H.2	The data processor has established procedures as far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting or restricting or providing information about the processing of personal data to data subjects.	We have inspected 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. We have inquired if there have been requests by the data controller for assistance in handing out, correcting, deleting, or restricting or providing information about the processing of personal data to data subjects in the assurance period.	We have been informed that the data processor has not received requests from data controllers in relation to data subjects' rights, wherefore we have not tested the effectiveness of the control. No deviations noted.

Control objective I – Managing personal data breaches

Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
I.1	Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. We have inspected that procedures are up to date.	No deviations noted.
I.2	The data processor has established the following controls to identify any personal data breaches: • Awareness of employees • Monitoring of network traffic • Follow-up on logging of access to personal data.	We have inspected that the data processor provides awareness training to the employees in identifying any personal data breaches. We have inspected documentation that network traffic is monitored and that anomalies, monitoring alarms, large file transfers, etc. are followed up on. We have inspected documentation that logging of access to personal data, including follow-up on repeated attempts to gain access, is followed up on, on a timely basis.	No deviations noted.
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay after having become aware of such personal data breach at the data processor or a sub-data processor.	We have inquired if any personal data breaches have occurred in the assurance period.	We have been informed that no personal data breaches have occurred, wherefore we have not tested the effectiveness of the control. No deviations noted.
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency: • Nature of the personal data breach • Probable consequences of the personal data breach • Measures taken or proposed to be taken to respond to the personal data breach.	We have inspected that the procedures in place for informing the data controllers in the event of any personal data breach include detailed procedures for: • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach.	No deviations noted.

Control objective I – Managing personal data breaches

Procedures and controls are complied with to ensure that any personal data breaches may be responded to in accordance with the data processing agreement entered into.

No.	*Emply ApS' control activity*	*Grant Thornton's test*	*Result of test*
		We have inspected documentation that the procedures available support that measures are taken to respond to the personal data breach.	

Section 5: Supplementary information from Emply ApS

The following supplementary information has not been subject to the audit performed by Grant Thornton.

Based on Grant Thornton's identified nonconformities in the ISAE 3000 statement, Emply International A/S (hereinafter referred to as Emply) has the following additional information:

Under control activity B.12, Grant Thornton has found the following:

"We have inspected that for 13 of 13 change samples no documentation of approval was available. No further deviations noted."

To this, Emply states that Emply has a process where the approver of the change in question is not clearly stated. Emply has taken note of this and has adjusted the procedure accordingly.

Under control activity B.15, Grant Thornton has found the following:

"We have inspected that two shared accounts were created with access cards to the office building which were not closed in a timely manner."

Emply states that these two access cards have subsequently been closed, and it has been emphasized that the correct procedure for closing access cards will be followed in the future.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Henrik Basso Reichsthaler Møller
Underskriver 1
På vegne af: Emply ApS
Serienummer: e2bb9ab5-a11a-4b50-864e-8c58af066374
IP: 212.60.xxx.xxx
2023-08-07 07:56:08 UTC

Mit ID

Martin Brogaard Borup Nielsen
GRANT THORNTON,STATSAUTORISERET REVISIONSPARTNERSELSKAB
CVR: 34209936
Underskriver 2
Serienummer: 658bcd61-1988-4367-b3eb-215cfbbb49b0
IP: 82.192.xxx.xxx
2023-08-07 08:23:04 UTC

Mit ID

Kristian Lydolph
Underskriver 3
Serienummer: CVR:34209936-RID:43340328
IP: 62.243.xxx.xxx
2023-08-07 08:28:02 UTC

NEM ID