



revi-it

Building a safe society through compliance

Assurance report

Emply ApS

ISAE 3000 with assurance about information security and measurements pursuant to data processing agreements with customers throughout the period 1 April 2021 to 31 March 2022.

July 2022

REVI-IT A/S | www.revi-it.dk
Højbro Plads 10, 1200 København K
CVR: 30 98 85 31 | Tel. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

Table of contents

Section 1:	Emply ApS' description of processing activities for the supply of Emply ApS' SaaS solution	1
Section 2:	Emply ApS' statement	11
Section 3:	Independent auditor's ISAE 3000 assurance report with reasonable assurance on information security and measures according to the data processing agreements with customers throughout the period 1 April 2021 to 31 March 2022	13
Section 4:	Control objectives, controls, test, and results hereof	16

Disclaimer:

The English version of this report was translated from Danish for the convenience of the reader. This translation has not been reviewed or approved by REVI-IT A/S' auditors. In all legal matters, please refer to the Danish version.

Section 1: Emply ApS' description of processing activities for the supply of Emply ApS' SaaS solution

The purpose of the present description is to provide information to Emply ApS' customers and their auditors concerning the requirements of ISAE 3000, which is the international auditing standard for assurance reports about controls with the service provider.

The purpose of this description is a mapping of the technical and organisational measurements, involved in the operation of Emply ApS' Software-as-a-Service solutions (SaaS solution).

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

Further, the description provides information about the controls, used in the operation of Emply ApS' SaaS solution, including how they are implemented.

Description of Emply ApS

Emply was founded in Copenhagen in 2010. The SaaS solution was developed to service HR-employees' need of a modern solution. The platform can be adapted to all companies, regardless of line of business, size, organisational structure, or HR working procedures and no matter where the company is situated. Today, Emply is available in more than 16 languages and is being used in more than 50 countries.

Emply ApS supplies proprietary Software-as-a-Service, which includes 100% operation, service and support, consulting services and training. Emply supplies adjustments of functionality and integrations, on an ongoing basis, so the systems meet customers' demands as well as current legislation and regulations.

Emply ApS' SaaS solution is today supplied to both private and public companies. The solution is operated in Denmark and handled as a private cloud solution with GlobalConnect in Glostrup. Emply ApS is operating the solution and GlobalConnect "only" supplies housing, electricity, access to the Internet and the backup solution.

Business strategy / IT-security strategy

It is Emply's strategy that the necessary security must be integrated in the business, avoiding unnecessary risks for the company.

The purpose of the security policy is furthermore to indicate to everybody with a relation to Emply, that the use of information and information systems is subject to standards and guidelines.

Maintaining and developing a high security level is essential for Emply appearing reliable, both nationally and internationally.

In order to maintain Emply ApS' credibility, it must be ensured that information is being handled with the necessary confidentiality and that complete, precise, and punctual processing of approved transactions is being performed.

Second only to our employees, IT-systems are regarded as Emply ApS' most critical resource. We therefore put great effort in operational reliability, quality, observing legislative requirements, and that the systems are user friendly.

An efficient protection against IT-security treats must be created, assuring Emply ApS' image and the security, and working conditions of the employees. The protection must be aimed at both natural, as well as technical and man-made treats. Everybody is considered to be a possible cause of security breaches, i.e., no employee is excepted from the security rules.

The goals are therefore to:

- Obtain high operational reliability, with maximum availability factor and minimized risk of major breakdowns and loss of data - ACCESSIBILITY
- Obtain correct systems functions with a minimized risk of manipulation of and malfunction of both data and systems – INTEGRITY
- Obtain confidential processing, transferring and storage of data - CONFIDENTIALITY
- Obtain a mutual security between the parties involved – AUTHENTICITY
- Obtain guarantee of mutual and ascertainable contact – NON-REPUDIATION

It is Emply's goal to maintain an information security level, that as a minimum:

- complies with existing legislation
- observe good business practices
- meets customers' wishes, requirements and expectations to a professional supplier

The Danish Data Protection Act and EU's general data protection regulation form the legal frame of personal data processing in IT-service. Data processing agreements are signed between customers and Emply ApS.

We are responsible for the necessary technical and organisational measures, to ensure that the personal data are processed in a secure and adequate way.

To ensure a consistent supply, meeting the best standards of the businesses, we have chosen to support the operation of our SaaS solutions with an auditing process, enabling us to meet the requirements of ISAE 3000. Emply ApS' SaaS solutions are supported by a housing supplier (GlobalConnect) who will provide an ISAE 3402 assurance report.

The audit is repeated once a year and the assurance report will be presented to existing customers, as well as potential new customers. The assurance report must contribute to customers' (data controller) control, as to whether Emply complies with the instructions in the signed data processing agreements.

Within the following areas of IT-security strategy, Emply ApS has used methods to implement the relevant measures:

- Information security policies
- Organizing the IT-security
- HR security
- Means of access
- Physical security and supplier relationships
- Operations security
- Network security
- Development environment
- Security incident management
- Emergency management
- Compliance with the role of data processor (compliance)

Risk management in Emply ApS

It is our policy that risks, because of the company's activities, must be uncovered or limited to such a level, that the company is able to maintain normal operations.

Emply has established procedures for risk assessment of the business. That ensures that the risks linked to services supplied by us, are minimized to an acceptable level.

Risk assessment is performed periodically, as well as upon changes in existing system or when new systems are implemented. The risk assessment is part of the IT-security officer's responsibilities.

Information security policy

Emply management is responsible for IT-security and hereby we ensure that the general requirements and scope for IT-security is complied with. IT-security policies must be reviewed at least once a year.

Emply ApS' IT-security policy has been established with reference to the above and applies to all employees and all supplies. In case of failures or security breaches in our operational environment, the failure/security breach will be repaired immediately. A fixed procedure is followed to ensure transparency as well as preventive and corrective actions.

All servers, storage and network units are documented in Emply ApS. In there we log all system changes. Configuration files for network units (firewall, routers, switches and similar) are stored and accessible.

Security policy is prepared, to give all employees a common set of rules. That way, we obtain a stable operating environment and a high security level. Both policies, procedures and the operational basis is improved on an ongoing basis.

Emply ApS' organisation and IT-security management

In January 2021, Emply was bought by Lessor Group, the market leader in software for pay-, HR-, time recording and duty schedule solutions for small and big compagnies in Denmark, Sweden, and Germany. Lessor employs 180 people, and more than 65,000 companies now use one or more systems, provided by Lessor Group.

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

Emply ApS' organisational structure

Management is responsible for the daily operations of both organisation and IT.

Sales & Marketing is the department managing all communication with customers in connection with sales, software demonstrations, trade shows, tenders, and the execution of orders.

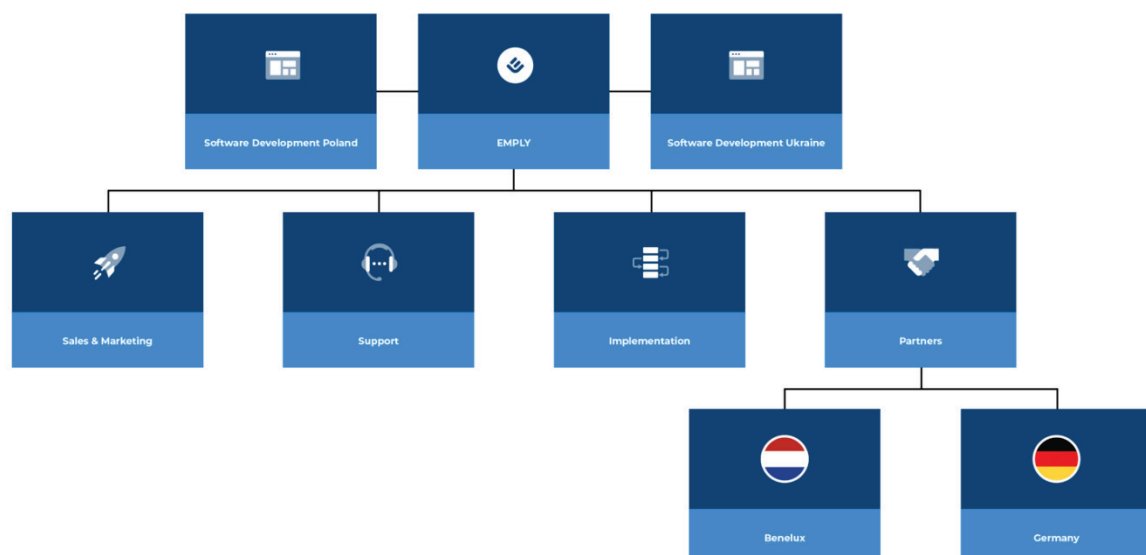
Support is the department that provides high-level support to all our customers.

Implementation is the department ensuring that all new customers have a positive experience when they come to us

Partners is the department ensuring that Emply can sell and distribute outside Denmark.

Software Development Ukraine and Poland are the departments developing Emply software. Ukraine is solely developing and testing software. Data processing is performed in Denmark. Upon special tasks, such as recreation of databases etcetera, Emply can – if agreed with customer – authorize a Polish developer's access to solving customer related tasks.

Emply ApS' IT-security is placed within Lessor Groups' security organisation. The organisational framework of IT-security is a natural part of the management's responsibilities.



HR-security

Emply ApS' employees are essential for the business. It is important to maintain and increase our competencies so we can adapt to customers' needs. We work with yearly KPI targets enabling us to pull together as a team.

Emply ApS use our own inhouse-developed SaaS solution. New employees go through an introduction to all areas of Emply. Both old and new employees study Emply ApS' policies and procedures. This applies to all employees.

Every Emply employee sign a non-disclosure agreement, also including the processing of customers' data. Emply ApS' employees have, to a limited extent, an opportunity to work from other facilities.

Access

Only authorized Emply users/employees have access to the Emply systems. The allocation of access to the operating environment is performed according to purpose. Rights and access to information are based on work-related needs, to enable the individual to perform best possible.

Access management is done by Emply's management.

Physical security and supplier relationships

Supervision of Global Connect:

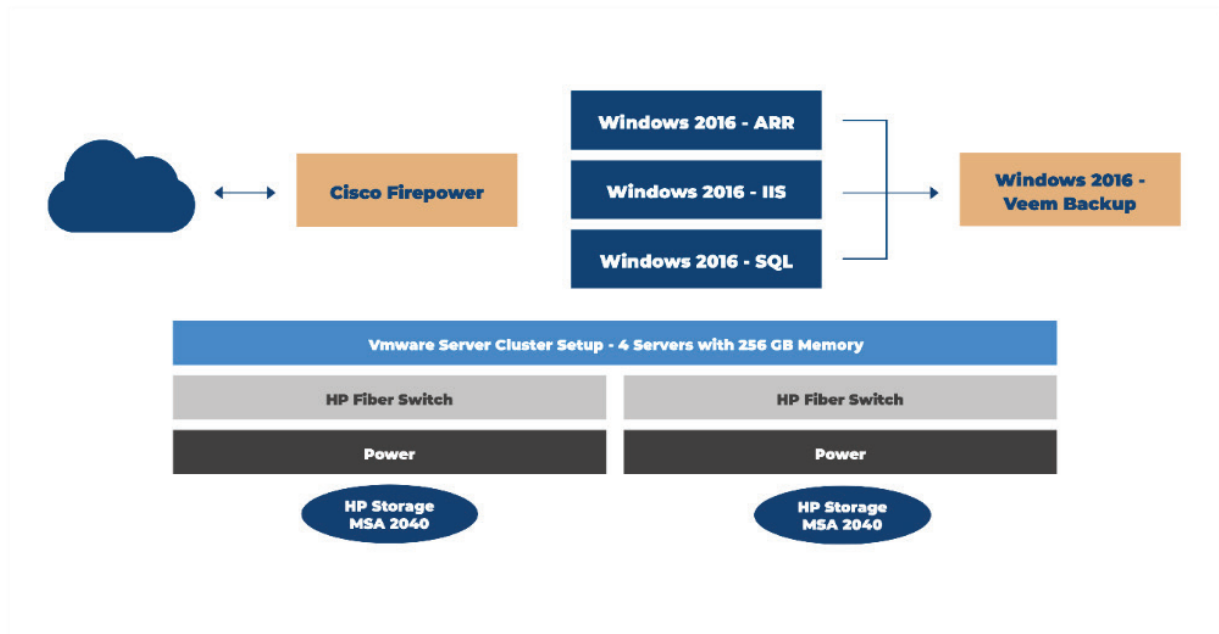
Global Connect provides, on a yearly basis, an ISAE 3402 assurance report, and an ISAE 3000 report on net- and information security.

Hardware setup

Emply is provided as a private cloud-service, run on a virtual Microsoft webfarm. The application is being hosted on multiple virtual machines. The individual virtual machine is running on a VMware cluster-solution. The VM cluster solution is run on six physical servers and all data are stored in an SD-storage system.

The Emply SaaS solution is built with Microsoft.Net. All customers use different SCL-databases to ensure a stable and secure software solution. The Emply solution is furthermore watched by multiple software solutions, to obtain a stabile production environment.

The Emplý solution contains several integrations, such as SSO (Single Sign-on), ADFS, two-factor authentication and more extended webservice APIs in both SOAP and RES. All transactions in Emplý ApS are saved and stored in multiple logfiles.



Operational reliability

Operational tasks are performed by Emplý ApS at set intervals. Furthermore, Emplý ApS will perform controls, maintenance, and management of all servers.

Monitoring

The operational environment is monitored 24/7/365 via automated service. Recourses for servers (CPU, RAM, disc, network) and accessibility. The monitoring also includes relevant IT-services, such as backups, accessibility to web, and systems for customers and internal use.

The primary monitoring is done internally within the operational environment, but to cover the external accessibility too, we have established remote monitoring.

Errors are being reported directly to Emplý ApS, whereupon the error will be investigated. In case of critical error on servers or services, the operator on duty will be notified directly.

Customers, experiencing operational problems, must contact Emplý ApS through the agreed support, either over the phone or via support@emplý.com.

We are open for inquiries Monday-Thursday from 8:30am-16:30pm and Friday from 8:30am to 15:30pm.

Logging

Logging is a valuable tool for monitoring, handling, and investigation. Since logs contain a lot of different information, we can divide it into two levels:

- System log: Emply ApS has developed their own system for monitoring of errors.
- User log: All Emply customers have access in the system to see which activities, they have made. They can search for activities via customer's own users, specific dates, projects etcetera.

Backup

The purpose of backup is to ensure, that the customer's data can be recreated accurately and fast, to avoid unnecessary delay. Backups are made on different levels, such as virtual servers, configurations, and data. All Emply customers have their own database, to ensure a speedy and easy restoring via backup.

All customers' databases are being saved encrypted in Veem Backup Solution. The backup service is provided by Global Connect. Backup is established on a daily basis and stored via dedicated backup servers in the operating environment. Hereafter the latest backup is stored for a month. Backups, 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 that service packs from suppliers are implemented to protect the systems against down-time and unauthorized access, and that the implementation is performed in a controlled manner.

Maintenance of Windows operating systems and appurtenant backend systems from Microsoft, is managed by Microsoft's build-in WSUS (Windows Service Update Service) where security- and critical patches are automatically installed in set intervals.

Communication security

Data lines and network security

The connection with the operational environment consists of 2 independent fibre lines. If the primary line should break down, traffic is automatically transferred via the secondary. As soon as the primary has been re-established, the traffic is again routed through this.

The firewall is rule-based and has a basic "deny-all" traffic rule. On this, a ruleset has been established, allowing specific protocols against a given server group. The firewall has a build-in "Load Balancer" used to ensure the distribution of the total traffic to different servers.

Finally, the firewall is performing an inspection of data packets (IDS). Automated scanning and blocking of traffic are based on state of vulnerability and is updated daily.

Development environment

When developing software, Emplay ApS uses dedicated test environments, from where the software can be processed for developing and testing. These environments are different from the ones used by Emplay ApS' customers.

Security incident management

Emplay ApS has established procedures for incident management and deviations reports, including security breaches.

The procedures ensure that data collection and documentation are performed systematically providing a solid basis for subsequent evaluation.

Management is responsible for defining and coordinating a structured process, ensuring a suitable reaction to security incidents

Emergency management

Emplay ApS' IT-contingency plan is to ensure that the IT-dependent business critical processes in Emplay can be restored and are functional after a critical incident directly or indirectly has hindered normal operations for a period of time. This to ensure a stable operation of Emplay.

The IT-contingency plan must be activated, when one or more incidents disturb or interrupt critical parts of Emplay for a longer period and the failing of IT-systems to restore during normal operations and troubleshooting with the agreed timeframe, which is 2 hours within normal working hours and 4 hours outside working hours.

The plan describes the handling of 4 scenarios:

- Physical incidents in Emplay Datacentre (fire, water, or other) shutting down Emplay, partly or totally
- IT-incidents, affecting Emplay operations
- IT-incidents, affecting Emplay's infrastructure (virus outbreak or hacker attacks)
- IT-incidents, compromising Emplay with risk of data leak, where others unlawfully or unintended can gain access to Emplay's data or Emplay's customers' data

Compliance with the role as data processor

It is Emplay ApS' management who is responsible for ensuring that all relevant legal and contractual requirements are identified and correctly observed. Relevant requirements could for instance be:

- EU General Data Protection Regulation
- Danish data protection law
- Data processing agreement
- Emplay's general agreement
- Emplay's user conditions

The presence of the above agreements and other relevant documents ensure compliance with relevant legal and contractual requirements.

EU General data protection regulation (GDPR)

Emply ApS' SaaS solution supports the customers' processes with HR. Emply ApS does not own the data, gathered by the customers, and stored in the SaaS solution, but solely develop and operates the SaaS solution, used by the customers to perform the necessary data processing. According to the General Data Protection Regulation and the Danish Data Protection law, Emply ApS is the data processor, and the customer is the data controller.

Data processing agreement

As data processor, Emply has special responsibilities in the general data protection regulation, implemented in a data processing agreement. Among other things, Emply ApS must:

- Keep records of which categories of data being processed
- Describe the technical and organisational measures, established to safeguard the personal data
- Contribute to meeting the customer's obligations connected with the data subjects' rights (according to Chapter 3 in the AU General Data Protection Regulation)
- Provide expert knowledge to the customer to ensure compliance with Article 32-34
 - o Article 32 – processing security
 - o Article 33 – reporting data security incidents
 - o Article 34 – informing data subjects about personal data security breaches
- Inform the customer about name and contact details of sub-data processors
- Ensure that potential requirements from the customer is also imposed on the sub-data processor

As data processor, Emply ApS is working with personal data, based on instructions from the customers, describing to what purpose, data can be used. Emply ApS is responsible for ensuring that gathered data solely are being used for this purpose.

Access to customer data

The Emply solution is a SaaS solution, operated by Emply ApS. Test and releases are managed by Emply itself. Therefore, Emply ApS is fully responsible for the processing of customers' data. Generally, Emply employees have no access to customers' data, unless specified tasks require this. It is solely Emply's support department and management, who have access to customer data.

All Emply ApS' employees have signed a non-disclosure agreement, focused on how we at Emply handle customer's data.

Significant changes during the assurance period.

No significant changes have been made during the assurance period.

Complementary controls with the data controller

This chapter describes the general aspects of Emplay ApS' SaaS solution, which means that the individual customer's agreement is not being considered.

Emplay ApS is not responsible for access rights, including granting, changing and deletion, in relation to the customers' individual users and their access to the SaaS solution. The customer themselves are obliged to ensure the necessary controls related to this control objective.

The data controllers are also under the following obligations:

- To ensure, that personal information is up to date
- To ensure, that the instruction is legal, according to the current personal data legislation
- To ensure, that the instruction is appropriate, according to this data processing agreement and the main service
- To ensure, that the data controllers' users are up to date
- To ensure that the required authorization for data processing is present
- To comply with the duty of disclosure towards the data subjects on the exercising of their legal rights
- To handle requests and control the identity of the data subjects, who wish to exercise their rights

Section 2: EmPLY ApS' statement

The accompanying description has been prepared for EmPLY ApS' customers, who, in the role of data controllers have used EmPLY ApS' SaaS solution 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 sub-suppliers Lessor, Interlogic and Global Connect. This statement does not include control objectives and related controls with EmPLY ApS' sup-suppliers and sub-data processors. Certain control objectives in the description can only be achieved, if the sup-supplier's controls, as assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by sup-suppliers.

A few of the control objectives, stated in EmPLY ApS' description in Section 1 of EmPLY ApS' SaaS solution, can only be achieved if the complimentary controls with customers are adequately designed and function effectively with the controls with EmPLY ApS. The statement does not include the suitability of the design and functionality of these complementary controls.

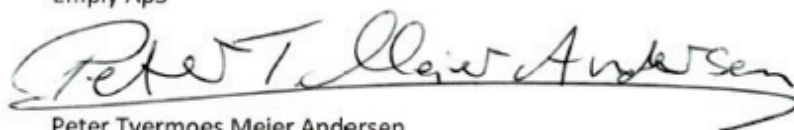
EmPLY ApS confirm that:

- a) The accompanying description, Section 1, fairly presents how EmPLY ApS has processed personal data on behalf of the data controller throughout the period from 1 April 2021 til 31 March 2022. The criteria used in making this statement we that the accompanying description:
 - (i) Presents how EmPLY ApS' processes and controls related to data protection were designed and implemented, including:
 - The type of services provided, including the type of personal data processed
 - The processes in both IT- 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' SaaS solution 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 data processor Emply ApS' SaaS solution for the processing of personal data throughout the period from 1 April 2021 to 31 March 2022.
- (iii) Does not omit or distort information relevant to the scope of Emply ApS' SaaS solution, 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' SaaS solution, 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 2021 to 31 March 2022, if relevant controls with sup-suppliers were operationally effective and data controller has performed the complementary controls, assumed in the design of Emply ApS throughout the period from 1 April 2021 to 31 March 2022.
- 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 2021 to 31 March 2022.
- 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.

Copenhagen, 4 July 2022

Emply ApS



Peter Tvermoes Meier Andersen
Direktør

Section 3: Independent auditor's ISAE 3000 assurance report with reasonable assurance on information security and measures according to the data processing agreements with customers throughout the period 1 April 2021 to 31 March 2022

To Emply ApS and Emply ApS' customers in the role of data controllers.

Scope

We were engaged to provide assurance with reasonable assurance on Emply ApS' description in "Section 1" of Emply ApS' SaaS solution according to data processing agreements with their customers, in the role of data controller throughout the period of 1 April 2021 to 31 March 2022 and b+c) about the design and functionality of controls related to the control objectives, stated in the description.

Emply uses the sup-suppliers and sub-data processors Lessor, Interlogic and Global Connect. This statement does not include control objectives and related controls with Emply ApS' sub-suppliers and sub-data processors. Certain control objectives in the description can only be achieved, if the sub-data processors controls, assumed in the design of Emply ApS' controls, are adequately designed, and functioning effectively together with the related controls with Emply ApS.

A few of the control objectives, stated in Emply ApS' description in Section 1 of Emply ApS' SaaS solution can only be achieved if the complementary controls with the customers are adequately designed and functioning effectively together with the controls with Emply ApS. This statement does not include the suitability of the design and functionality of these complementary controls.

Our opinion is expressed with reasonable assurance.

Emply ApS' responsibilities

Emply ApS is responsible for the preparing of the Description and the accompanying statement in "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.

REVI-IT A/S is subject to the International Standard on Quality Control (ISQC 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 Emplý 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 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

Emplý ApS' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of Emplý ApS' SaaS solution, 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' SaaS solution, as designed, and implemented throughout the period 1 April 2021 to 31 March 2022 in all material respects are true, and
- (b) that the controls related to the control objectives stated in the Description, in all materials aspects were adequately designed throughout the period from 1 April 2021 to 31 March 2022, to provide a high degree of security, that the control objectives stated in the description would be achieved, if controls with sup-suppliers were operationally effective, and if data controllers has designed and implemented the complementary controls, as assumed in the design og Emply ApS' controls during the period from 1 April 2021 to 31 March 2022, and
- (c) that 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 fra 1 April 2021 to 31 March 2022.

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' SaaS solution, 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, 4 July 2022

REVI-IT A/S

State Authorised Public Accounting Company



Christian H. Riis
Partner, CISA



Michael Marseen
State Authorised Public Accountant

Section 4: Control objectives, controls, test, 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 2021 to 31 March 2022.

Our statement, does not apply to controls, performed at Emplay 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 Emplay ApS by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Emplay 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 be 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 27001/2.

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	<i>New scope compared to ISO 27001/2</i>
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	<i>New scope compared to ISO 27001/2</i>
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	<i>New scope compared to ISO 27001/2</i>
D.1	6, 11, 13, 14, 32	7.4.5, 7.4.7 , 7.4.4	<i>New scope compared to ISO 27001/2</i>
D.2	6, 11, 13, 14, 32	7.4.5, 7.4.7 , 7.4.4	<i>New scope compared to ISO 27001/2</i>
D.3	13, 14	7.4.7 , 7.4.4	<i>New scope compared to ISO 27001/2</i>
E.1	13, 14, 28, 30	8.4.2, 7.4.7, 7.4.8	<i>New scope compared to ISO 27001/2</i>
E.2	13, 14, 28, 30	8.4.2, 7.4.7, 7.4.8	<i>New scope compared to ISO 27001/2</i>
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

Control activity	GDPR articles	ISO 27701	ISO 27001/2
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	<i>New scope compared to ISO 27001/2</i>
H.2	12, 13, 14 , 15, 20, 21	7.3.5, 7.3.8, 7.3.9	<i>New scope compared to ISO 27001/2</i>
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	Test performed by REVI-IT A/S	Result of test
A.1	<p>Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inspected, that formalized procedures ensuring that processing of personal data only is performed according to instructions, are established.</p> <p>We have inspected, that the procedures are updated.</p>	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	We have by sample test, inspected that processing of personal data is performed according to the 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 inquired, into whether the data processor has received instructions, that in the data processor's opinion infringes the Regulation or other European Union or member state data protection provisions.	<p>We have been informed, that the data processor has not received instructions, that in the data processor's opinion infringes the Regulation or other European Union or member state data protection provisions, therefore we have not tested the effectiveness of the relevant processes.</p> <p>No deviations noted.</p>

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	Test performed by REVI-IT A/S	Result of test
B.1	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inspected, that formalized procedures, ensuring that the agreed security measures are being established, are present.</p> <p>We have inspected, that the procedures are updated.</p>	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 the risk assessment performed, is updated, and includes the processing of personal data in question.	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.	<p>We have, by sample test, inspected the implementation of antivirus and ensured, that this has been configured according to the internal policies.</p> <p>We have inspected, that antivirus software has been updated.</p>	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, by sample test, inspected firewalls, and by sample test ensured that these are configured according to the internal policy.	No deviations noted.
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 network charts and other network documentation to ensure adequate segmentation.	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	Test performed by REVI-IT A/S	Result of test
B.6	Access to personal data is isolated to users with a work-related need for such access.	<p>We have inspected that formalised procedures are in place for restricting users' access to personal data.</p> <p>We have, by sample test, inspected new employees and by sample test, ensured that accesses are based on a work-related need.</p> <p>We have inspected lists of accesses.</p>	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 by sample test, inspected monitoring of network components and by sample test ensured, that these are configured according to internal policy.	No deviations noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	We have by sample test inspected the encryption of transmissions and by sample test ensured, that the encryption is configured according to internal policy.	No deviations noted.
B.9	<p>Logging has been established in systems, databases, and networks.</p> <p>Logon data are protected against manipulation and technical errors and are reviewed regularly.</p>	We have by sample test, inspected the logging established, and by sample test ensured that this is implemented according to internal policy.	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, by sample test, inspected that personal data in development and 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 by sample test inspected that documentation exists for ongoing tests of the established technical measures.	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	Test performed by REVI-IT A/S	Result of test
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 by sample test inspected changes during the period and by sample test ensured that these follow the internal change procedure.	No 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.	<p>We have inspected that formalised procedures exist for granting and removing users' access to systems and databases used to process personal data.</p> <p>We have by sample test inspected, that employees' access to systems and databases have been approved and that they are based on a work-related need.</p> <p>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.</p> <p>We have inspected that documentation exists, that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.</p>	No deviations noted.
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 documentation that a procedure for managing access to data centres exists.	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	Test performed by REVI-IT A/S	Result of test
C.1	<p>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.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.</p>	<p>We have inspected that an information security policy exists that has been approved within the past year.</p> <p>We have inspected of documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.</p>	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 by sample test inspected data processing agreements and by sample test ensured that the information security policy is according to the agreements.	No deviations noted.
C.3	The employees of the data processor are screened as part of the employment process.	We have by sample test, inquired about screening of new employees.	<p>We have observed that compliance with the screening procedure has not been documented.</p> <p>No further deviations noted.</p>
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.	<p>We have by sample test inspected that new employees during the assurance period, have signed a non-disclosure agreement.</p> <p>We have by sample test inspected whether new employees during the assurance period have been introduced to relevant procedures.</p>	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	Test performed by REVI-IT A/S	Result of test
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.	<p>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.</p> <p>We have by sample test inspected, that rights have been deactivated or terminated.</p> <p>We have inquired into the return of assets during the assurance period.</p>	<p>We have observed that compliance with the return of assets procedure can not be documented.</p> <p>No further deviations noted.</p>
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, 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.
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.	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 documentation, that the DPO has been involved in relevant tasks during the assurance period.	No deviations noted.
C.9	The processor keeps a record of categories of processing activities for each data controller.	We have inspected that lists exist, that management has processed and approved within the last year.	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	Test performed by REVI-IT A/S	Result of test
D.1	<p>Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	We have inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller.	No deviations noted.
D.2	Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.	We have by sample test, inspected terminated data processing agreements during the period and by sample test ensured that requirements exist of storage- and deletion routines.	No deviations noted.
D.3	<p>Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been:</p> <ul style="list-style-type: none"> • Returned to the data controller; and/or • Deleted if this is not in conflict with other legislation. 	We have, by sample test, inspected that documentation exists that 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	Test performed by REVI-IT A/S	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.	We have inspected that formalised procedures exist for only storing and processing personal data in accordance with the data processing agreements.	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.	<p>We have inspected that the data processor has a complete and updated list of processing activities stating localities, countries, or regions.</p> <p>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.</p> <p>We have inspected documentation of back-up.</p>	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	Test performed by REVI-IT A/S	Result of test
F.1	<p>Written procedures exist which include requirements for the data processor when using sub-data processors, including requirements for sub-data processing agreements and instructions.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have inspected that formalised procedures are in place for using sub-data processors, including requirements for sub-data processing agreements and instructions.</p> <p>We have inspected that procedures are up to date.</p>	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	Test performed by REVI-IT A/S	Result of test
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.	<p>We have inspected that the data processor has a complete and updated list of sub-data processors used.</p> <p>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.</p>	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 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.	<p>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.</p> <p>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.</p>	No deviations noted.
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.	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 by sample test, inspected the supervision of sub-data processors during the assurance period.	No deviations noted.

Control objective G – Transfer of personal data to third countries

Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.

No.	Emply ApS' control activity	Test performed by REVI-IT A/S	Result of test
G.1	Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.	<p>We have by sample test inspected data processing agreements and by sample test ensured that transfer to third countries have been addressed.</p> <p>We have inquired into, whether the data processor transfers data to third countries.</p>	<p>We have been informed, that personal data are not transferred to third countries or international organisations, and we find this probable based on our test actions.</p> <p>No deviations noted.</p>
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	<p>We have by sample test, inspected data processing agreements and by sample test ensured, that transfer to third countries have been addressed.</p> <p>We have inquired into whether the data processor transfers data to third countries.</p>	<p>We have been informed, that personal data are not transferred to third countries or international organisations, and we find this probable based on our test actions</p> <p>No deviations noted.</p>
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	<p>We have by sample test, inspected data processing agreements and by sample test ensured, that transfer to third countries have been addressed.</p> <p>We have inquired into, whether the data processor transfers data to third countries.</p>	<p>We have been informed, that personal data are not transferred to third countries or international organisations, and we find this probable based on our test actions.</p> <p>No deviations noted.</p>

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	Test performed by REVI-IT A/S	Result of test
H.1	<p>Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>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.</p> <p>We have inspected that procedures are up to date.</p>	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 inquired into whether the data processor has received requests from the data controller, related to the rights of the data subjects.	<p>We have been informed, that the data processor has not received any requests from the data controller, related to the data subjects' rights, wherefore we have not tested the efficiency of the data processor's procedures.</p> <p>No deviations noted.</p>

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	Test performed by REVI-IT A/S	Result of test
I.1	<p>Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>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.</p> <p>We have inspected that procedures are up to date.</p>	No deviations noted.
I.2	The data processor has established the following controls to identify any personal data breaches:	We have inspected that the data processor provides awareness training to the employees in identifying any personal data breaches.	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.	<p>We have inspected that the data processor has a list of security incidents disclosing whether the individual incidents involved a personal data breach.</p> <p>We have inquired into whether personal data security breaches have occurred during the period.</p>	<p>We have been informed, that no personal data security breaches have occurred during the period, wherefore we have not been able to test the efficiency of the data processor's procedures.</p> <p>No deviations noted.</p>
I.4	<p>The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency:</p> <ul style="list-style-type: none"> • 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 documentation that the procedures available support that measures are taken to respond to the personal data breach.	No deviations noted.