



# revi-it

A safe society through compliance

## Assurance report

CVR No.: 31 43 07 47

# Emply ApS

Independent auditor's ISAE 3000 assurance report with reasonable assurance in connection with compliance with the Data Protection Regulation and affiliated data protection law in the role of data processor for the delivery of Emply ApS' SaaS solution throughout the period from 12 March 2020 to 31 March 2021

REVI-IT A/S | [www.revi-it.dk](http://www.revi-it.dk)

Højbro Plads 10, 1200 København K

CVR: 30 98 85 31 | Tel. 33 11 81 00 | [info@revi-it.dk](mailto:info@revi-it.dk)

[www.dpo-danmark.dk](http://www.dpo-danmark.dk) | [www.revi-cert.dk](http://www.revi-cert.dk)

May 2021

## Table of contents

Section 1:	Emply ApS' description .....	1
Section 2:	Emply ApS' statement.....	11
Section 3:	Independent auditor's ISAE 3000 assurance report with reasonable assurance on compliance with the General Data Protection Regulation (GDPR) and associated Data Protection law throughout the period from 12 March 2020 to 31 March 2021.....	13
Section 4:	Control objectives, controls, test and results hereof.....	16

## Section 1: Emply ApS' description

### Introduction

The purpose of this report is to supply information to Emply ApS' customers and their auditors, concerning the requirements in ISAE 3000, which is the international standard for assurance engagements about controls with the service provider.

The purpose of this description is to uncover the technical and organisational measures, involved in the operations 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 data processor) describing the primary requirements in connection with the role of data processor, combined with overall requirements in data processor agreements.

Furthermore, the description provides information about the controls, used to operate Emply ApS' SaaS solution, and how they are implemented.

### Description of Emply ApS

Emply ApS was founded in Copenhagen in 2020 by Michael Ahlstrøm and Gert Abildskov. The SaaS solution was developed to meet HR staffs' demands for modern solutions. The platform can be adapted to all companies regardless of line of business, size, organisational structure or HR processes, and no matter where in the world, the company may be located. Today Emply is available in more than 16 languages and is being used in more than 50 countries.

Emply ApS supplies in-house developed Software-as-a-Service, including 100% operations, service and support, consulting services and training. Emply adapt functionality and integrations on an ongoing basis so the system will always meet the customers' requirements as well as existing legislation and regulations.

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

### Business strategy / IT-security strategy

Emply ApS' strategy is that the required security must be integrated in the business, to prevent the company being exposed to unacceptable risks.

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

Maintenance and development of a high security level is a significant precondition, to Emply appearing trustworthy and reliable, both nationally and internationally.

To maintain Emply ApS' credibility, it must be ensured that information is processed with the necessary confidentiality and that complete, accurate and punctual processing of approved transactions is carried out.

Second only to the employees, IT-systems are regarded as Emply ApS' most critical resource. Therefore, operational reliability, quality, compliance with law and that the systems are user friendly, that is without inconvenient security measures, are of the utmost importance.

Efficient protection against threats to IT-security must be established, to secure Emplay ApS' image, employee security and working conditions, in the best way possible. The protection must be aimed at both natural, technical, and human-caused threats. All people are regarded to be possible causes to security breaches, in other words, no employee can be above the security regulations.

### **Our 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 function of the systems 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 Emplay's goal to maintain an information security level, that as a minimum:**

- complies with existing legislation
- observe good business practices
- meet 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 processor agreements are signed between customers and Emplay ApS.

We are responsible for the necessary technical and organisation 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. Emplay ApS' SaaS solutions are supported by a housing supplier (GlobalConnect) who will prepare 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 Emplay complies with the instructions in the signed data processor agreements.

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

- Information security policies
- Organising 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 with 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, 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.

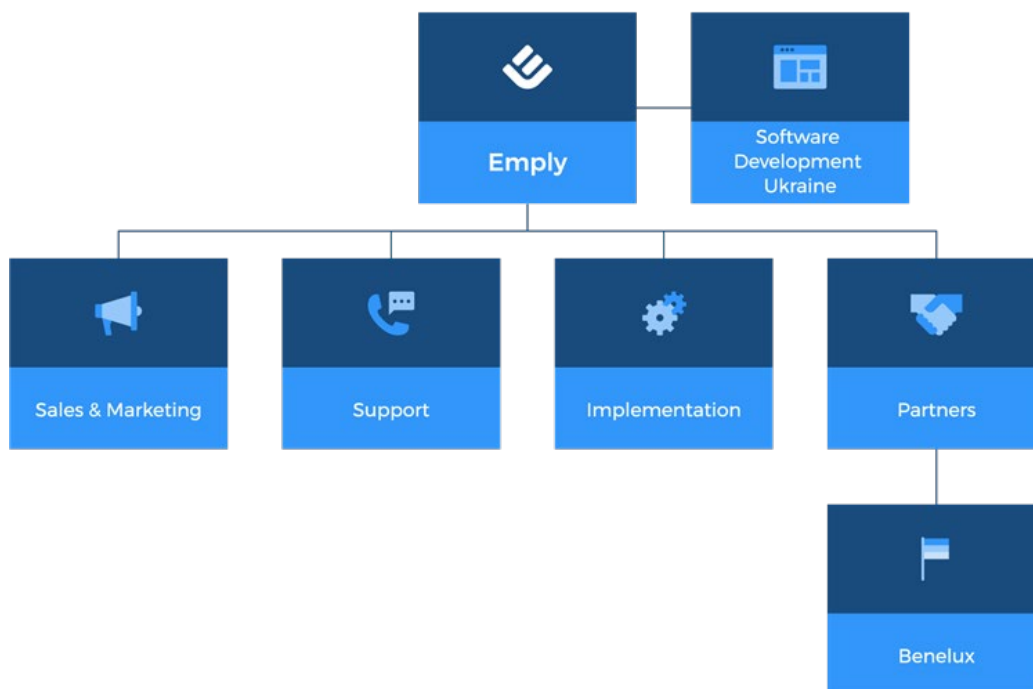
## Emply ApS' organisation and IT-security management

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 companies 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 the founders, Gert Abildskov and Michael Ahlstrøm.

## 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.

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

**Software Development Ukraine** is the department 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 Ukrainian developer to do it.

Emply ApS has made Gert Abildskov responsible for IT-security. Hence, the organisational embeddedness of IT-security is a natural part of 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 unit.

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 management.

## Physical security and supplier relationships

- *Datacentre*

GlobalConnect (previous Nianet) have an extensive security set-up and have implemented formal policies and process descriptions in contemplation of access control to systems, facilities, and datacentres.

- *Control by GlobalConnect:*

GlobalConnect annually prepare an ISAE 3402 assurance report concerning physical security and a ISAE 3000 about net- and information security.

- *Electricity and cooling*

The datacentre has been established according to Uptime Tier2- or Tier3-defiition. The datacentre is supplied by the local electricity distributor, through standby-generators and via UPS, ensuring a stable power supply, in case of breakdown of the public power supply.

Cooling of racks in the datacentre is done under raised floors. The cooling system pushes cool, filtered air up through the rack from underneath. GlobalConnect's datacentres most often use cubes, where cold air is circulated in "cold corridors" and hot air from the equipment is blown into the surrounding rooms, from where a cooling unit will absorb the heated air and via cooling water, heat outside units. All areas and racks have a temperature of maximum 25 degrees and a humidity of maximum 60%

- *Protection against water*

The datacentre has been built with raised floor level and equipped with water- and humidity detectors.

- *Fire prevention*

All areas, where GlobalConnect have Emply ApS' equipment, are build of fire-resistant materials.

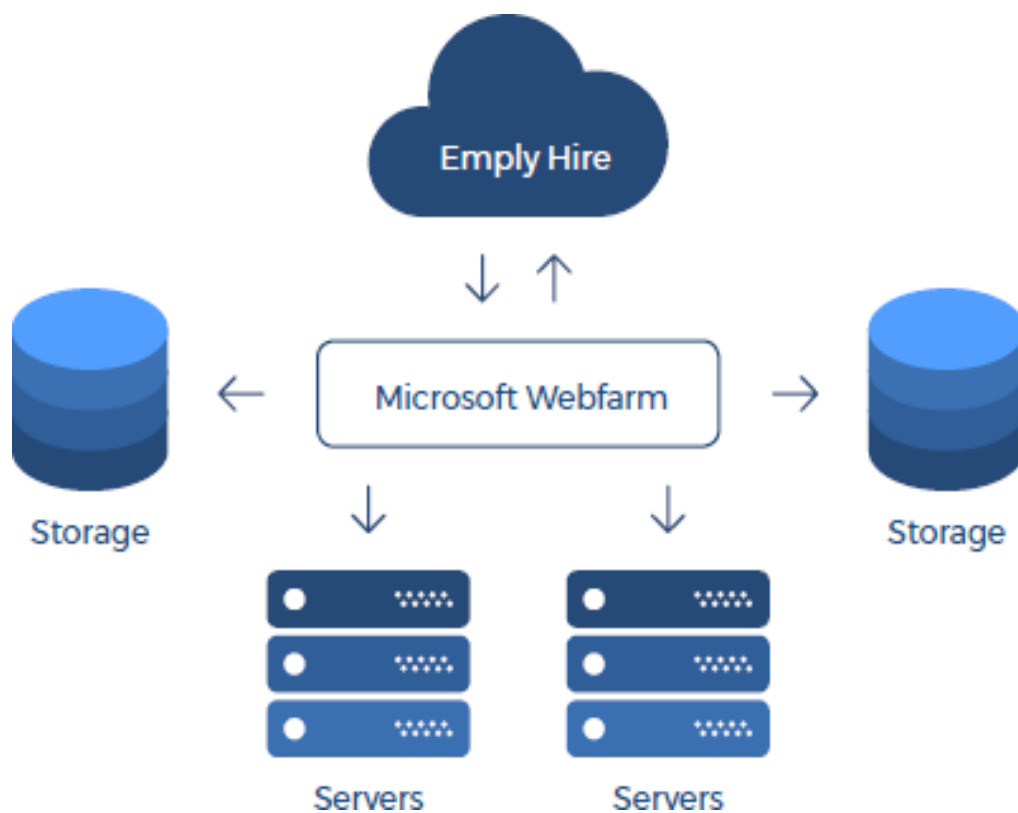
The datacentre is protected by Argonite- or Inergen facilities, connected to the fire alarm. Optical and ionizing smoke alarms are connected on both the ceiling and under the raised floor in the rooms. These are constantly monitoring the areas and will also sound audio-visual alarm. Automatically and monitored fire-extinguishing is also established. Furthermore, GlobalConnect will perform periodical service checks of the UPS, diesel generators, the fire-extinguishers, and the air-conditioning system.

- *Hardware setup*

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

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

The Emply 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 Emply ApS are saved and stored in multiple logfiles.





## Operational reliability

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

## Monitoring

The operational environment is monitored 24/7/365 via automatic service. Resources for servers (CPU, RAM, disc, network) are monitored. The monitoring also includes relevant IT-services, for example backup, accessibility for web and systems for customers, as well as 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 Emply 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 Emply ApS through the agreed support, either over the phone or via [support@emply.com](mailto:support@emply.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 log 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 exactly 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. Backup is established on a daily basis and saved via dedicated backup servers in the operational environment. Daily backups of customer databases are kept for 14 days and hereafter the latest backup of each month is being saved. Backups, older than 1 month is 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.

## Data protection

### *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 reestablished, 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 not the same as 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-depending 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 Emplý Datacentre (fire, water, or other) shutting down Emplý, partly or totally
- IT-incidents, affecting Emplý operations
- IT-incidents, affecting Emplý's infrastructure (virus outbreak or hacker attacks)
- IT-incidents, compromising Emplý with risk of data leak, where others unlawfully or unintended can gain access to Emplý's data or Emplý's customers' data

## Compliance with the role as data processor

It is Emplý 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 processor agreement
- Emplý's general agreement
- Emplý'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)

Emplý ApS' SaaS solution supports the customers' processes with HR. Emplý 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, Emplý ApS is the data processor, and the customer is the data controller.

## Data processor agreement

As data processor, Emplý has special responsibilities in the general data protection regulation, implemented in a data processor agreement. Among other things, Emplý 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
  - Article 32 – processing security
  - Article 33 – reporting data security incidents
  - 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, Emplay ApS is working with personal data, based on instructions from the customers, describing to what purpose, data can be used. Emplay ApS is responsible for ensuring that gathered data solely are being used for this purpose.

## Access to customer data

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

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

## Significant changes during the assurance period

No significant changes have been made during the assurance period.

## Customers' responsibilities (complimentary controls with the customers)

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.

## Section 2: Emplay ApS' statement

The accompanying description has been prepared for Emplay ApS' customers, who, in the role of data controllers have used Emplay 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.

Emplay ApS uses the following sub-suppliers, GlobalConnect, Paychex Deutschland GmbH (only for German customers) and Prodesse B.V. (only for Benelux customers). This statement does not include control objectives and related controls at Emplay ApS' sup-suppliers.

Emplay ApS confirm that:

- a) The accompanying description, Section 1, fairly presents Emplay ApS' SaaS solution which has processed personal data on behalf of data controller subject to the Regulation throughout the period from 12 March 2020 to 31 March 2021. The criteria used in making this statement were that the accompanying description:
  - (i) Presents how Emplay ApS' SaaS solution was 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 Emplay 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 Emplay ApS' SaaS solution in the processing of personal data throughout the period from 12 March 2020 to 31 March 2021

- (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 12 March 2020 to 31 March 2021. 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 12 March 2020 to 31 March 2021.
- 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

Glostrup, 25 May 2021

Emply ApS



Gert Abildskov

Direktør

## Section 3: Independent auditor's ISAE 3000 assurance report with reasonable assurance on compliance with the General Data Protection Regulation (GDPR) and associated Data Protection law throughout the period from 12 March 2020 to 31 March 2021

To Emply ApS' management, their customers in the role of data controllers and their auditors.

### Scope

We were engaged to provide assurance with reasonable assurance on Emply ApS' description in "Section 1" of Emply ApS' SaaS solution during the period from 12 March 2020 to 31 March 2021 about the design and effectiveness of controls related to the control objectives stated in the Description.

Emply ApS uses the following sub-suppliers GlobalConnect, Paychex Deutschland GmbH (only for German customers) and Prodesse B.V. (only for Benelux customers). This statement does not include control objectives at the sub-suppliers.

### 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 Code of Ethics for Professional Accountants issued by FSR - Danish Auditors (Code of Ethics for Professional Accountants), which are based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional conduct.

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 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 Emply ApS' SaaS solution 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

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' 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 12 March 2020 to 31 March 2021 in all material respects are true, and
- (b) The controls related to the control objectives stated in the Description, were appropriately designed throughout the period from 12 March 2020 to 31 March 2021, og
- (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 12 March 2020 to 31 March 2021.



## Description of tests of controls

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

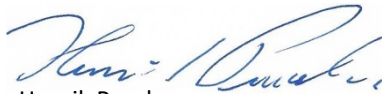
## Intended users and purpose

This report and the description of tests of controls in Section 4 are intended only for data controllers who have used Emplay 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, 25 May 2021

### **REVI-IT A/S**

State Authorised Public Accounting Company



Henrik Paaske

State Authorised Accountant



Christian H. Riis

Partner, CISA

## Section 4: Control objectives, controls, test and results hereof

The following overview is prepared to create a general view of the controls, implemented by Emply ApS to comply with the General Data Protection Regulation (GDPR) and associated data protection law. Our test of the functionality has included the controls, we find necessary to establish reasonable assurance for compliance with the articles stated throughout the period from 12 March 2020 to 31 March 2021.

Emply ApS uses the sub-suppliers GlobalConnect, Paychex Deutschland GmbH (only for Germany customers) and Prodesse B.V. (only for Benelux customers). This statement does not apply to controls, performed at the sub-suppliers.

The requirements, directly stated in the statutory regulation or the law, cannot be deviated from. However, the way security is implemented can be adjusted, as the safety requirements on multiple points are more of a general and overall nature, meant to address purpose, description of processing, the sort of personal data etcetera. Apart from this, specific customer contracts, may have special requirements beyond the general requirements of the Data Protection Law, in which case there are not included in the following.

Our statement does not apply to controls performed at Emply ApS' customers, as the customers auditors are to perform this control and assessment.

We performed our test of controls with Emply ApS, by one or more of 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 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 in regard 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 objective	GDPR-articles	ISO 27701	ISO 27001/2
A.1	5, 26, <b>28</b> , 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, <b>8.2.2</b>	<i>New area in relation to ISO 27001/2</i>
A.2	<b>28</b> , 29, 48	8.5.5, 6.15.2.2, <b>6.15.2.2</b>	18.2.2
A.3	<b>28</b>	<b>8.2.4, 6.15.2.2</b>	18.2.2
B.1	31, <b>32</b> , 35, 36	<b>5.2.2</b>	4.2
B.2	<b>32</b> , 35, 36	<b>7.2.5, 5.4.1.2, 5.6.2</b>	6.1.2, 5.1, 8.2
B.3	<b>32</b>	<b>6.9.2.1</b>	<b>12.2.1</b>
B.4	28 stk. 3; litra e, <b>32</b> ; <b>stk. 1</b>	<b>6.10.1.1, 6.10.1.2, 6.10.1.3</b> , 6.11.1.3	<b>13.1.2</b> , 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	<b>32</b>	<b>6.6</b>	9.1.1, 9.2.5
B.7	<b>32</b>	<b>6.9.4</b>	12.4
B.8	<b>32</b>	<b>6.15.1.5</b>	18.1.5
B.9	<b>32</b>	<b>6.9.4</b>	12.4
B.10	<b>32</b>	<b>6.11.3</b>	14.3.1
B.11	<b>32</b>	<b>6.9.6.1</b>	12.6.1
B.12	28, <b>32</b>	<b>6.9.1.2, 8.4</b>	12.1.2
B.13	<b>32</b>	<b>6.6</b>	9.1.1
B.14	<b>32</b>	<b>7.4.9</b>	<i>New area in relation to ISO 27001/2</i>
B.15	<b>32</b>	<b>6.8</b>	11.1.1-6
C.1	<b>24</b>	<b>6.2</b>	5.1.1, 5.1.2
C.2	<b>32, 39</b>	<b>6.4.2.2, 6.15.2.1, 6.15.2.2</b>	7.2.2, 18.2.1, 18.2.2
C.3	<b>39</b>	<b>6.4.1.1-2</b>	7.1.1-2
C.4	28, 30, <b>32, 39</b>	<b>6.10.2.3</b> , 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	<b>32</b>	<b>6.4.3.1, 6.8.2.5, 6.6.2.1</b>	7.3.1, 11.2.5, 8.3.1
C.6	<b>28</b> , 38	<b>6.4.3.1, 6.10.2.4</b>	7.3.1, 13.2.4
C.7	<b>32</b>	<b>5.5.3, 6.4.2.2</b>	7.2.2, 7.3
C.8	<b>38</b>	<b>6.3.1.1, 7.3.2</b>	6.1.1
D.1	6, 11, <b>13, 14</b> , 32	<b>7.4.5, 7.4.7, 7.4.4</b>	<i>New area in relation to ISO 27001/2</i>
D.2	6, 11, 13, 14, <b>32</b>	<b>7.4.5, 7.4.7, 7.4.4</b>	<i>New area in relation to ISO 27001/2</i>
D.3	13, <b>14</b>	<b>7.4.7, 7.4.4</b>	<i>New area in relation to ISO 27001/2</i>
E.1	13, 14, <b>28</b> , 30	<b>8.4.2, 7.4.7, 7.4.8</b>	<i>New area in relation to ISO 27001/2</i>
E.2	13, 14, <b>28</b> , 30	<b>8.4.2, 7.4.7, 7.4.8</b>	<i>New area in relation to ISO 27001/2</i>
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, <b>32</b> , 35, 40, 41, 42	5.2.1, <b>7.2.2, 7.2.6</b> , 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	<b>28</b>	<b>8.5.7</b>	15
F.3	<b>28</b>	<b>8.5.8, 8.5.7</b>	15
F.4	<b>33, 34</b>	<b>6.12.1.2</b>	15
F.5	<b>28</b>	<b>8.5.7</b>	15
F.6	<b>33, 34</b>	<b>6.12.2</b>	15.2.1-2

Control objective	GDPR-articles	ISO 27701	ISO 27001/2
<b>G.1</b>	15, 30, <b>44, 45</b> , 46, 47, 48, 49	<b>6.10.2.1, 7.5.1</b> , 7.5.2, 7.5.3, 7.5.4, <b>8.5.1</b> , 8.5.2, 8.5.3	13.2.1, 13.2.2
<b>G.2</b>	15, 30, <b>44, 45</b> , 46, 47, 48, 49	<b>6.10.2.1, 7.5.1</b> , 7.5.2, 7.5.3, 7.5.4, <b>8.4.2</b> , 8.5.2, 8.5.3	13.2.1
<b>G.3</b>	15, 30, <b>44, 45</b> , 46, 47, 48, 49	<b>6.10.2.1, 7.5.1</b> , 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
<b>H.1</b>	12, <b>13, 14</b> , 15, 20, 21	<b>7.3.5, 7.3.8, 7.3.9</b>	<i>New area in relation to ISO 27001/2</i>
<b>H.2</b>	12, <b>13, 14</b> , 15, 20, 21	<b>7.3.5, 7.3.8, 7.3.9</b>	<i>New area in relation to ISO 27001/2</i>
<b>I.1</b>	<b>33, 34</b>	<b>6.13.1.1</b>	16.1.1-5
<b>I.2</b>	<b>33, 34</b> , 39	6.4.2.2, <b>6.13.1.5, 6.13.1.6</b>	16.1.5-6
<b>I.3</b>	<b>33, 34</b>	<b>6.13.1.4</b>	16.1.5
<b>I.4</b>	<b>33, 34</b>	<b>6.13.1.4</b> , 6.13.1.6	16.1.7

## Control objective A – Instruction regarding processing of personal data

Procedures and controls are performed to ensure that instructions regarding processing of personal data are in compliance with data processor agreement

No	Processor's control activity	Auditor's test	Auditor's test result
A.1	<p>There are written procedures containing requirements that processing of personal data may only occur on the basis of an instruction.</p> <p>Regularly – and at least annually – an assessment is made of whether the procedures should be updated.</p>	<p>We have inspected the information security policies to make sure, that it has been decided to follow instructions from data controller.</p> <p>We have inspected the policy and ensured that this has been updated, during the period.</p>	No deviations found.
A.2	The processor only performs the processing of personal data evident from the instruction from the controller.	We have inspected the information security policy, and – by sample test – ensured that this complies with data processor agreement.	No deviations found.
A.3	The processor immediately notifies the controller if an instruction according to the processor is contrary to the General Data Protection Regulation or data protection provisions in other EU law or the Member States' national legislation.	We have inquired into, whether there have been instructions during the period, that the data controller has considered to be unlawful.	<p>We have been informed, that there have been instructions during the period, that the data controller has considered to be unlawful.</p> <p>No deviations found.</p>

## Control objective B – Technical measures

Procedures and controls are observed to ensure that the processor has implemented technical measures for ensuring relevant security of data processing.

No	Processor's control activity	Auditor's test	Auditor's test result
B.1	<p>There are written procedures containing requirements on the establishment of agreed security measures for the processing of personal data in accordance with the agreement with the controller.</p> <p>Regularly – and at least annually – an assessment is made of whether the procedures should be updated.</p>	<p>We have inspected the information security policy and ensured, that compliance with agreements have been decided upon.</p> <p>We have inspected that procedures are updated.</p>	No deviations found.
B.2	The processor has performed a risk assessment and on the basis of this, has implemented the technical measures assessed to be relevant in order to achieve adequate security, including establishing the security measures agreed with the controller.	<p>We have inspected the risk analysis and ensured, that this has been updated, during the period.</p> <p>We have inspected, that risk assessment is updated and includes the actual processing of personal data.</p>	No deviations found.

No	Processor's control activity	Auditor's test	Auditor's test result
B.3	For the systems and databases, used for processing personal data, antivirus is implemented and regularly updated.	We have – by sample test – inspected the implementation of antivirus and – by sample test – ensured that this is configured according to internal policies.  We have inspected, that antivirus software is updated.	No deviations found.
B.4	External access to systems and databases used for the processing of personal data occurs through a secured firewall.	We have – by sample test – inspected firewalls and also by sample test, ensured that this has been correctly configured.	No deviations found.
B.5	Internal networks are segregated in order to ensure restriction of access to systems and databases used for the processing of personal data.	We have – by sample test – inspected network documentation to ensure adequate segmentation.	No deviations found.
B.6	Access to personal data is isolated to users with a work-related need for this.	We have – by sample test – inspected accesses and – by sample test – ensured that this is based on a work-related need.	No deviations found.
B.7	For the systems and databases, used for processing personal information, system surveillance with alarms, has been established.	We have – by sample test – inspected monitoring of network components and – by sample test – ensured that these are configured in compliance with internal policy.	No deviations found.
B.8	By transmission of personal data via the internet and by email, efficient encryption is used.	We have – by sample test – inspected the encryption of transmissions, and – by sample test – ensured that the encryption is configured in compliance with internal policy.	No deviations found.
B.9	Logging in systems, databases and networks have been established.	We have – by sample test – inspected the established logging and – by sample test – ensured that this is implemented in compliance with internal policy.	No deviations found.
B.10	Personal information used for development, test or similar, are always in pseudonymised or anonymised form. Usage is only in order to perform the controller's purpose according to agreement and on its behalf.	We have inspected the information security policy and ensured that access to personal data is based on a work-related need.  We have – by sample test – inspected development projects during the period and ensured that access to personal data has been based on work-related needs.	No deviations found.
B.11	The established technical measures are regularly tested by means of vulnerability scans and penetration tests.	We have inspected, that the company has performed vulnerability tests during the period.  We have inspected the ongoing monitoring of vulnerabilities.	No deviations found.

No	Processor's control activity	Auditor's test	Auditor's test result
B.12	Changes to systems, databases, and networks are made in accordance with established procedures that ensure maintenance by means of relevant updates and patches, including security patches.	We have – by sample test – inspected changes during the period and – by sample test - ensured that these are in compliance with the policy.	No deviations found.
B.13	There is a formal procedure for allocating and revoking user accesses to personal data. Users' accesses are regularly reviewed, including that rights still can be justified by a work-related need.	We have inspected, that formal procedures have been established for creating and deleting of users' access to systems and databases, used for processing personal data.  We have – by sample test – inspected the creation and deletion of accesses during the period, and – by sample test – ensured that this follows procedures.  We have inquired into ongoing control of accesses.	No deviations found.
B.14	Access to systems and databases, in which personal data is processed, which entails a high risk for the data subjects, occurs as a minimum by means of two factor authentications.	We have – by sample test – inspected accesses and – by sample test – ensured that this is performed by means of two-factor authentication.	No deviations found.
B.15	Physical access security has been established such that only authorised persons can gain physical access to premises and data centres in which personal data are stored and processed.	We have inspected lists of key cards.	No deviations found.

## Control objective C – Organisational measures

Procedures and controls are observed that ensure that the processor has implemented organisational measures for ensuring relevant security of data processing.

No	Processor's control activity	Auditor's test	Auditor's test result
C.1	<p>The processor's management has approved a written information security policy, which has been communicated to all relevant stakeholders, including the processor's employees. The information security policy is based on the performed risk assessment.</p> <p>Regularly – and at least annually – an assessment is made of whether the information security policy should be updated.</p>	<p>We have inspected, that information security policy is present, and has been updated during the period.</p> <p>We have inspected documentation that the information security policy has been communicated to the relevant stakeholders, including the processor's employees.</p>	No deviations found.
C.2	<p>The processor's management has ensured that the information security policy is not contrary to entered processor agreements.</p>	<p>We have – by sample test – inspected data processing agreements and – also by sample test ensured that the information security policy is in compliance with the agreements.</p>	No deviations found.
C.3	<p>The processor's employees are checked in connection with employment.</p>	<p>We have – by sample test – inspected employments during the period and ensured that the procedure for employment has been followed.</p>	No deviations found.
C.4	<p>At employment, employees sign a confidentiality agreement. In addition, the employee is introduced to the information security and procedures regarding data processing as well as other relevant information in connection with the employee's processing of personal data.</p>	<p>We have – by sample test – inspected employments during the period and – by sample test – ensured that new employees have signed a non-disclosure agreement and have been introduced to the information security policy.</p>	No deviations found.
C.5	<p>At the termination of employment, a procedure has been implemented at the processor ensuring that the user's rights are deactivated or terminated, including that assets are returned.</p>	<p>We have inspected procedures, ensuring that terminated employees' access rights are deactivated or deleted upon termination, and that assets, such as key cards, laptops, mobile phones etcetera, are being returned.</p> <p>We have – by sample test – inspected terminations during the period and by sample test ensured that accesses have been terminated and assets returned.</p>	No deviations found.



No	Processor's control activity	Auditor's test	Auditor's test result
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, that the company has hired a Data Protection Officer.	No deviations found.

## Control objective D – Return and deletion of personal data

Procedures and controls are observed that ensure that personal data can be deleted or returned if agreed with the controller.

No	Processor's control activity	Auditor's test	Auditor's test result
D.1	<p>There are written procedures containing requirements that storage and deletion of personal data occurs in accordance with the agreement with the controller.</p> <p>Regularly – and at least annually – an assessment is performed of whether the procedures should be updated.</p>	<p>We have inspected that formal procedures for storage and deletion of personal data have been established, according to the agreement with the data controller.</p> <p>We have inspected that the procedures have been updated.</p>	No deviations found.
D.2	Specific requirements to the data processor's storage period and deletion routines have been agreed upon.	We have – by sample test – inspected data processor agreements and – by sample test - ensured that storage periods have been agreed upon.	No deviations found.
D.3	<p>At the end of the processing of personal data for the controller, data is according to the agreement with the controller:</p> <ul style="list-style-type: none"> <li>Returned to the controller, and/or</li> <li>Deleted, when not in conflict with other legislation.</li> </ul>	We have – by sample test – inspected data processor agreements, terminated during the period and – by sample test - ensured that data has been returned or deleted .	No deviations found.

## Control objective E – Storage of personal data

Procedures and controls are observed that ensure that the processor only stores personal data in accordance with the agreement with the controller.

No	Processor's control activity	Auditor's test	Auditor's test result
E.1	<p>There are written procedures containing requirements that storage of personal data only occurs in accordance with the agreement with the controller.</p> <p>Regularly – and at least annually – an assessment is made of whether the procedures should be updated.</p>	<p>We have inspected, that formalized procedures have been established, to ensure that storage and processing of personal data, only is performed in compliance with data processor agreements.</p>	No deviations found.
E.2	<p>The processor's processing including storage must only take place at the locations, in the countries, or the territories approved by the controller.</p>	<p>We have inspected, that the processor has a general and updated list of processing activities, including locations, countries, or regions.</p> <p>We have - by sample test – inspected data processor agreements and – by sample test - ensured that processing only takes place on agreed locations.</p>	No deviations found.

## Control objective F – Use of sub-processors

Procedures and controls are observed that ensure that only approved sub-processors are used and that the processor when following up on their technical and organisational measures for protection of the rights of the data subjects and the processing of personal data ensures adequate security of data processing.

No	Processor's control activity	Auditor's test	Auditor's test result
F.1	<p>There are written procedures containing requirements to the processor at the use of sub-processors, including requirements on sub-processor agreements and instruction.</p> <p>Regularly – and at least annually – an assessment is made of whether the procedures should be updated.</p>	<p>We have inspected, that formalized procedures for the use of sub-data processors have been established, including requirements about sub-data processor agreements and instructions.</p> <p>We have inspected, that the procedures are updated.</p>	No deviations found.
F.2	<p>The processor solely uses sub-processors for the use of processing of personal data that are specifically or generally approved by the controller.</p>	<p>We have – by sample test – inspected data processor agreements and – by sample test – ensured that the data processor only uses sub-data processors for processing of personal data.</p>	No deviations found.

No	Processor's control activity	Auditor's test	Auditor's test result
F.3	In case of changes to the use of generally approved sub-processors, the controller is informed in a timely manner in order to be able to raise objections and/or withdraw personal data from the processor. In case of changes to the use of specifically approved sub-processors, this is approved by the controller.	We have inquired into, whether there has been a change in the use of sub-data processors during the period.	We have been informed, that there have been no changes in the use of sub-data processors during the period.  No deviations found.
F.4	The processor has subjected the sub-processor to the same data protection obligations as those stated in the processor agreement or the like with the controller.	We have – by sample test – inspected data processor agreements and sub-processor agreements and – by sample test - ensured that both the data processor and the sub-processor has been subjected to same or similar obligations.	No deviations found.
F.5	The processor has a list of approved sub-processors.	We have inspected the data processor agreement and ensured, that sub-data processors are included in the agreement.	No deviations found.
F.6	On the basis of an updated risk assessment of each sub-processor and the activity taking place at this sub-processor, the processor performs periodic follow-up on this at meetings, inspections, review of assurance report, or similar.  The controller is informed about the follow-ups with the sub-processor.	We have inspected the procedure of inspection with the sub-processors, and we have ensured that the sub-processor has been inspected and reviewed.	No deviations found.

## Control objective G – Transfer of personal data to third countries

Procedures and controls are observed that ensure that the processor only transfers personal data to third countries or international organisations in accordance with the agreement with the controller on the basis of a valid ground for transfer.

No	Processor's control activity	Auditor's test	Auditor's test result
G.1	There are written procedures containing requirements that the processor only transfers personal data to third countries or international organisations in accordance with the agreement with the controller on the basis of	We have inspected data processor agreements and ensured that transfers to third countries have been handled.  We have inspected data location.	We have been informed, that data are not being transferred to third countries and we find this plausible, based on our tests.  No deviations found.
G.2	The data processor may only transfer personal data to third countries or international organisations according to instructions from the controller.	We have inspected data processor agreements and ensured that transfers to third countries have been handled.	We have been informed, that data are not being transferred to third countries and we find this plausible, based on our tests.  No deviations found.
G.3	In connection with transfer of personal data to third countries or international organisations, the processor has assessed and documented that there is a valid basis for transfer.	We have inspected data location.	We have been informed, that data are not being transferred to third countries and we find this plausible, based on our tests.  No deviations found.

## Control objective H – Rights of the data subjects

Procedures and controls are observed that ensure that the processor can assist the controller with handing over, correcting, erasing, or the restriction of and providing information about the processing of personal data to the data subject.

No	Processor's control activity	Auditor's test	Auditor's test result
H.1	There are written procedures containing requirements that the processor must assist the controller in relation to the rights of the data subjects.  Regularly – and at least annually – an assessment is made of whether the procedures should be updated.	We have inspected, that formalized procedures have been established, for the data processor's assistance to the controller in relation to the rights of the data subjects.  We have inspected that the procedures are updated.	No deviations found.
H.2	The processor has established procedures that to the extent agreed permits timely assistance to the controller in relation to handing over, correcting, erasing, or the restriction of and providing information about the processing of personal data to the data subject.	We have inquired into, whether there have been requests during the period.	We have been informed, that there have been no requests during the period, wherefore we have not been able to test the procedures.  No deviations found.

## Control objective I – Managing personal data breaches

Procedures and controls are observed that ensure that any personal data breaches can be managed in accordance with the entered processor agreement.

No	Processor's control activity	Auditor's test	Auditor's test result
I.1	<p>There are written procedures containing requirements that the processor must inform the controller in case of personal data breaches.</p> <p>Regularly – and at least annually – an assessment is made of whether the procedures should be updated.</p>	<p>We have inspected, that formalized procedures have been established, including requirements that controller must be notified in case of security breaches.</p> <p>We have inspected that the procedure is updated.</p>	No deviations found.
I.2	The processor has established controls for identification of possible personal data breaches.	We have inspected that processor offers awareness training to employees, related to identification of possible personal data breaches.	No deviations found.
I.3	In case of personal data breaches, the processor has notified the data controller without further delay, after finding out that a personal data breach has occurred that the processor or a sub-processor	We have inquired into, whether personal data breaches have occurred during the period.	<p>We have been informed, that there have been no personal data breaches during the period, wherefore we have not been able to test the efficiency of the procedures in this area.</p> <p>No deviations found.</p>
I.4	<p>The data processor has established procedures for assisting the controller at the controller's notification to the Danish Data Protection Agency (Datatilsynet):</p> <ul style="list-style-type: none"> <li>• The type of personal data breach</li> <li>• Probable consequences of the personal data breach</li> <li>• Measures taken or suggested to be taken in order to manage the personal data breach.</li> </ul>	We have inspected, that procedures for notifying the controller in case of data breaches, have been established.	No deviations found.