Independent service auditor’s assurance report

Assurance engagement in relation to compliance with
the EU General Data Protection Regulation (GDPR)
as at 17 December 2018

ISAE 3000

HeroBase A/S

CVR-no.: 31 07 31 03

December 2018

REVI-IT A/S • state authorised public accounting firm
Jens Kofods Gade 1 • DK-1268 Copenhagen K • Phone 3311 8100 • info@revi-it.dk • revi-it.dk • CVR-no. 3098 8531

Table of contents

HeroBase A/S' statement

This assurance report concerns HeroBase A/S' compliance with the EU General Data Protection Regulation (GDPR).

We confirm that we, in our opinion, in all material respects have complied with the aforementioned criteria as at 17 December 2018.

We furthermore confirm that auditor has had access to all information and material necessary for issuing the assurance report.

On the basis of this it is our assessment that we, in all material respects, have conducted appropriate operations and administration of our services.

Søborg, 17 December 2018

HeroBase A/S

Casper Langhoff
CEO

Kenny Andreasen
CTO & CIO

HeroBase A/S' system description of the solution Hero Outbound as well as internal controls

Introduction

The purpose of this description is to supply information to HeroBase's customers and their stakeholders (including auditors) regarding the requirements and contents of the EU General Data Protection Regulation ("GDPR"), as described by the framework of the International Standard for Assurance Engagements ISAE 3000, including the International Standard for Assurance Engagements on controls at a service organisation, ISAE 3402.

Additionally, the purpose of this description is to provide specific information on matters regarding the security of processing, technical and organisational measures, responsibility between data controllers (our customers) and processors (HeroBase), and how the solution Hero Outbound by means of functionality for e.g. supporting the rights of the data subjects support our customers (the data controllers) in relation to complying with GDPR as regards their activities in Hero Outbound. Thus, the description is applicable for our delivery of the product and service Hero Outbound to our customers.

The description concerns the matters related to Hero Outbound that cover the majority of our customers and are based on our standard delivery. Individual customer relations are not included in this description.

HeroBase and our software Hero Outbound

HeroBase is a Danish IT company based in Søborg. We develop, host, and supply software in the form of a SaaS solution to contact centres. Our core product is supplying the software Hero Outbound, which is supplied as a SaaS-solution, which means it is hosted in our own data centres and is based on a flexible and scalable subscription-based model.

Hero Outbound, which this assurance report concerns, is at the moment the largest product in our palette of solutions collected under the *Hero* brand. Other solutions include e.g. the marketing automation platform Hero Flows, and the advisory and sales training body Hero Academy. Hero is chosen as the umbrella term, as we with our solutions want to appeal directly to the end users of our software; when it comes to Hero Outbound, this for the most part means users and employees – also called agents – in contact centres – also called call centres. By supplying a fast, intuitive, efficient, and personal platform, we strive to be the preferred choice for the "everyday heroes", which the agents in the contact centres are dubbed internally in HeroBase.

We create the foundation for the most efficient contact centre

The name Hero Outbound has been chosen for the solution that for the moment is the leading solution, as it first and foremost focuses on direct sales/advisory work, also called outbound telemarketing. Though the term often has a negative connotation, telemarketing is yet a very efficient contact channel, as it provides the possibility of cultivating the personal contact between the agent and the person "on the other end of the line". Sales and customer contacts, which are established by means of canvassing, are in no way limited to outbound telemarketing alone. Emails and texts are a natural extension of the telephonic dialogue – either in connection with digital order approval, distribution of follow-up information, coordinating work, etc. In addition, Hero Outbound enables incoming phone calls to be answered "mixed" with the outgoing phone calls – typically when persons with a missed call on their phone call back, or in connection with inbound requests from potential customers due to campaigns etc.

Thereby, Hero Outbound can, even without products from the remaining palette of Hero solutions, constitute the only software necessary for many contact centres to perform their activities for the agents (sales, booking of meetings, fundraising, surveys etc.) and for leaders and administrators who organise and monitor the agents' work.

These ”activities” also include the action itself of placing a call or answering the phone. As a web application Hero Outbound is operated in a browser, and with a headset connected to the computer, phone calls can be placed and answered by means of the built-in call technology Hero Phone, which is based on the WebRTC framework. This means that no external phones or third-party solutions are necessary for performing the contact activities. If you want to make a call by means of an existing phone present at the work station – e.g. a SIP phone or a landline phone installed by the company – this can also be used along with Hero Outbound, as the application can connect to an external phone and keep the line open, whereby connection and speaking takes place via the external phone.

A central system among other business systems

Regarding integration, Hero Outbound offers a number of possibilities for integration with other solutions when it comes to data in and out of the platform; user creation; documentation of phone calls etc. Hero Outbound has a well-developed API, which customers can make use of at no additional cost. This REST-API allows access to the customer's Hero Outbound data according to rights on function and project level, defined by the customer itself, and allows retrieving, updating, and deleting logical entities. If the customer to a wider extent wants data pushed from Hero Outbound to external systems, instead of pulling data from our REST-API, the platform has built-in “triggers” – a kind of webhooks – where rules can be setup to perform certain actions when certain things occur in the system. Actions include, among other things, calls to external SOAP- or REST-APIs, whereby you can integrate Hero Outbound with all other systems without writing a single line of code – as long as you have an API that can be called from Hero's web servers (a limited IP range) with either XML or JSON-objects.

The above is a general description of Hero Outbound and a short description of some of the tools that the platform makes available. Regarding the customers on Hero Outbound, HeroBase wants to create a long-term customer relation, where the customer over time along with its customer experience manager starts using more and more parts of the platform, and where Hero Outbound is integrated to other key systems in the customer's business. We believe that this is possible through a technically strong and stable platform, where security and performance are given pride of place, with an engaged technical and customer-focused team behind this.

Technical setup and placement

Hero Outbound is a web application based on .NET (the primary language is C#) and with a front end based on e.g. JavaScript, Angular and REACT. The database technology is MySQL, and hosting is via the Danish data centres GlobalConnect (Taastrup) and InterXion (Ballerup). At the time of writing, a large part of AWS' (Amazon Web Services) solutions is being put into service. At first when it comes to storage of files in S3 instead of on virtual servers in Denmark. Later, also with a view to having databases in AWS' Aurora. The only AWS locations we have chosen services in, and where data thereby is located in, are AWS' Dublin site in Ireland and AWS' site in Frankfurt, and thereby no data in Hero Outbound leaves the EU. Telephony-wise, calling is operated by physical Linux servers with Freeswitch as a tele-operating system on top. Our infrastructure and architecture are designed in such a way that there is redundant failover equipment for everything from firewalls and switches to database and tele servers. Most of the equipment is also present in both data centres, which means that one location can resume operations if another location is impacted by reduced access or other problematic circumstances, internal as well as external.

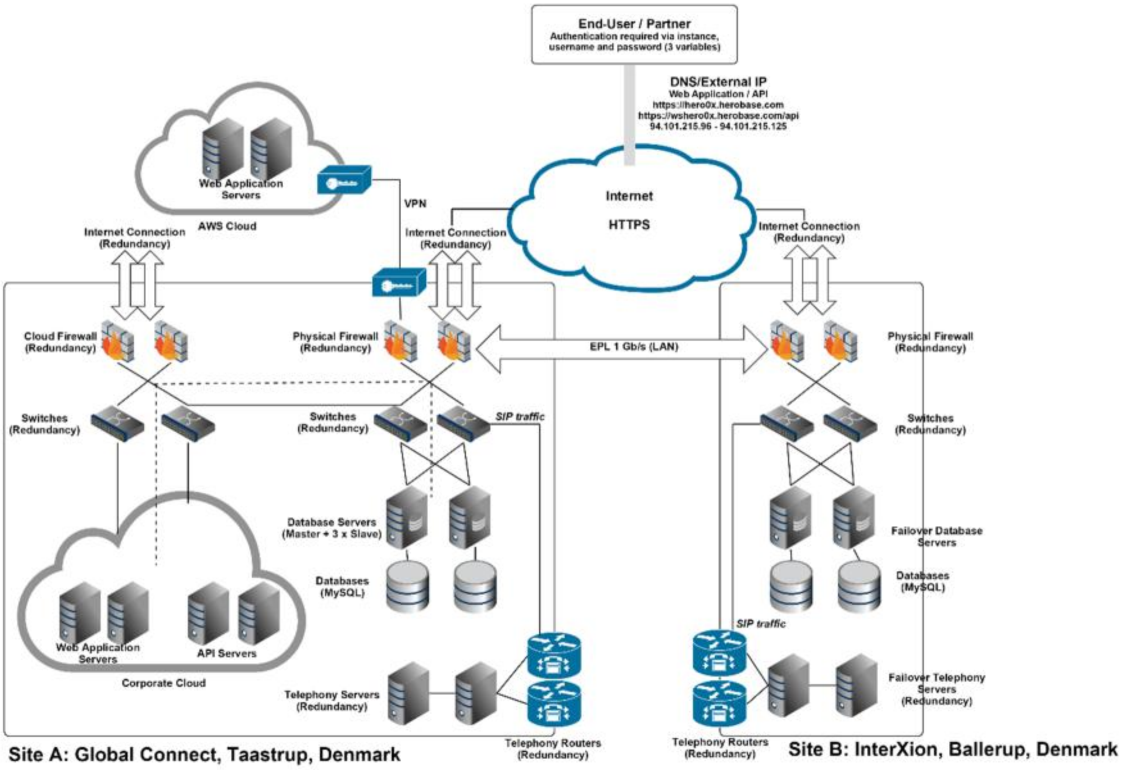
End-User / Partner
Authentication required via instance, username and password (3 variables)
DNS/External IP
Web Application / API
https://hero0x.herobase.com
https://wshero0x.herobase.com/api
94.101.215.96 - 94.101.215.125
Web Application Servers
AWS Cloud
VPN
Internet
HTTPS
Internet Connection (Redundancy)
Internet Connection (Redundancy)
Internet Connection (Redundancy)
Cloud Firewall (Redundancy)
Physical Firewall (Redundancy)
EPL 1 Gb/s (LAN)
Physical Firewall (Redundancy)
Switches (Redundancy)
Switches (Redundancy)
SIP traffic
Switches (Redundancy)
Database Servers (Master + 3 x Slave)
Failover Database Servers
Databases (MySQL)
Databases (MySQL)
SIP traffic
Web Application Servers
API Servers
Corporate Cloud
Telephony Servers (Redundancy)
Failover Telephony Servers (Redundancy)
Telephony Routers (Redundancy)
Telephony Routers (Redundancy)
Site A: Global Connect, Taastrup, Denmark
Site B: InterXion, Ballerup, Denmark

Fig. 1: The Hero Outbound platform, general infrastructure as at mid-2018.

We believe in appealing to the everyday heroes by designing complete solutions for their workplaces, and by supplying solutions which turn contact centres into competitive and efficient companies by optimising working time and the profitability of the centres' tasks, simultaneously with our adjustment of the platform to new, external requirements such as new requirements for payment solutions, contract documentation, GDPR etc. We believe that we have Northern Europe's best software for the industry, and we have international growth objectives based on a healthy and solid home market, where the close daily contact and long-term customer relation are in focus!

Organisation and responsibility

HeroBase employs 30 persons in Denmark, Sweden, Ukraine, Spain, and Lithuania. About half the employees are placed in Denmark and have their daily workplace at the office in Søborg.

The management consists of an ultimately responsible CEO, and below him a CTO with all technical responsibility as well as a CXO responsible for customer contact, customer relations, and support. In addition, a staff function with CFO as well as administration and HR.

The IT department, led by HeroBase's CTO, consists primarily of developers in a "devops" constellation, where two persons are dedicated to operations, optimising servers and infrastructure, monitoring and handling operational issues, but where all have operations as their first priority in case of technical issues on the platform. It is an objective that actual development, understood as improving existing features and developing new ones, constitutes 80 % of the department's time. The developers are organised in frontend and backend expertise, with a chief architect who makes the general decisions on language, technology, and new frameworks on the basis of a thorough analysis and in cooperation with HeroBase's CTO. In addition, a network administrator is responsible for network and telephony, whereas a project manager and tester has a close cooperation with HeroBase's other departments.

Management has the overall responsibility for IT security and that the company's general IT security policy is observed.

Next to the daily organisation based on function, a security organisation has been organised with an information security committee comprising key employees from various parts of HeroBase, including management, and an information security coordinator who has the daily, operational responsibility for a number of tasks defined in HeroBase's information security code of practise. The information security coordinator is additionally responsible for all employees being aware of the information security manual, including rules and procedures, helps them to access and understand it, and acting on and observing the rules. Finally, the responsibility for a variety of matters related to the business systems that support the daily work with supplying the product and service Hero Outbound is delegated to the system owners.

Risk management in HeroBase A/S

Risk management in HeroBase A/S is done for all areas connected with delivering the product and service Hero Outbound, and which thereby may have financial consequences for our customers. Risk analysis, assessment, and management are based on ISO 27005, and are based on impact analyses and vulnerability analyses at service level. Service is understood as business systems supporting the delivery of Hero Outbound as well as Hero Outbound in itself as a customer system.

The business in HeroBase answers the questions in the impact analysis, while the IT department in HeroBase performs the vulnerability analyses. Vulnerability analyses are reported at service level, but are based on assets, which are the physical and virtual sub-elements that altogether constitute the platforms or business systems. For instance, the service Hero Outbound has a number of dependent assets such as firewalls, switches, tele routers, web application servers, database servers, telephony servers etc. When reporting takes place at service level, it is also obvious that it is the "lowest common denominator" that defines e.g. maximum possible downtime. If a database server always can be taken over by a failover partner after boot and DNS change on five minutes, but if it in the utmost theory may take 15 minutes before a physical firewall will have been replaced by a booted and configuration-loaded redundant partner, it is obvious that it is these 15 minutes that will define the possible downtime.

Risk analyses are conducted as consequence and vulnerability analyses at least annually, after which the collected security overview is brought up for the information security committee and finally HeroBase's management, for the definition of further actions.

Generally on our control objectives, including rules and procedures as well as implemented controls

The most important thing in the supply of the product and service Hero Outbound is a stable and secure platform. It is a declared and management embedded promise that we would rather spend twice the time on solving a development task or another technical task than what was strictly necessary to solve the task, in order to ensure security and stability when we release updates to our customers.

To ensure that the supply chain can function, and that HeroBase at the same time can function as a competitive business, including achieving scalability over time, working procedures and processes connected with the supply of the product and service Hero Outbound are based on our information security code of practice, on top of which are defined procedures and controls with associated contingency plans etc.

Above all is our top-level information security policy, which is signed by HeroBase's CEO and which sets the framework for the information security work. This is valid for all employees and close cooperative partners (such as consultants).

The framework for the information security code of practice is ISO 27001, and the code of practice is classified according to the following control areas:

- Information security management and security policy
- Organisation of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

In addition, we have selected a number of procedures and policies within the framework of data security and GDPR, and we take our responsibility as processor for some of the country's largest companies extremely seriously. Up to the implementation of GDPR we have expanded our platform with a number of features that make it easier for our customers as data controllers to comply with the requirements imposed by e.g. GDPR. We would like to be considered *co*-data controllers to a higher extent than solely as processors, and we gladly express this in various connections. As a processor we have furthermore ensured that we have processor agreements with all our customers on Hero Outbound who in this constellation are data controllers.

GDPR and HeroBase's role and responsibility as a processor

GDPR is for everybody – but it is essential to understand how the specific parts of GDPR find use for each player depending on the type of organisation in question and how the organisation is subject to activities connected with the processing of data.

Naturally, HeroBase is the data controller for our own data. This means that we have performed data flow analyses for all processes in our business where personal data is stored or exchanged (internally or with a third party). The data flow analyses enable us to see exactly which types of data for which types of data subjects that are transferred or stored, and with which authority.

Additionally, as the provider of the software and solution Hero Outbound, HeroBase is the processor for all our customers. This means that we in our software Hero Outbound are hosting data that belongs to our customers as data controllers, and that we via our software provide a selection of tools and functionality that our customers – the data controllers – can use for working with the data. We only act on instruction from our customers and the framework for these instructions is defined in the contract between the customer and HeroBase as well as the associated processor agreement.

The articles 4-49 in GDPR thus find general use at HeroBase. But particularly relevant regarding HeroBase's role as processor is that we pay particular attention to the distinction between our own data and our customer's data. Data (and services – systems – wherein data is found) is classified and labelled according to this, and all technical and organisational measures – including internal procedures and training – are organised according to this distinction.

The following sections examine these measures and aspects in detail with a focus on HeroBase's role as a processor, i.e. measures that concern our processing of the data controllers' data, and how our software Hero Outbound is designed to support our customers as data controllers when it comes to the requirements that GDPR poses to data controllers.

Principles relating to processing of personal data

Hero Outbound is a generic and flexible platform that enables the input and entering of all sorts of data in principle. Campaign templates, fields (with associated attributes such as type of data, field validation, etc.) are defined, created and maintained by the customer itself that fully decides and is responsible for what data is input in, stored in, processed in, read out, and deleted from Hero Outbound.

HeroBase as a supplier neither accesses nor processes this data, unless we receive an explicit instruction from the data controlling customer for aiding with e.g. inputting data or rectifying/changing data in connection with the customer's campaign activities.

There is a data processing agreement between HeroBase and all customers. The contents and principles for this is specified in later sections.

Through procedures and regular training HeroBase has ensured that the classification of customer data and the associated processing principles are known by all employees.

Lawfulness of processing

If HeroBase receives instructions from the customer that are assessed to be contrary to current legislation or general sound principles for data processing, HeroBase will without undue delay bring this to the customer's attention.

HeroBase does not under any circumstances exchange or disclose the customer's data to third parties. An exception to this is situations where national special legislation requires that HeroBase provides information, e.g. if Danish authorities request data on certain phone calls as part of an investigation. In such cases the only personally identifiable data disclosed will be a phone number – no other personal data will be provided.

Additionally, as a part of our information security code of practice and information security procedures, HeroBase has defined responsibility for contact with relevant authorities, where this is required.

We have defined controls ensuring that customer data is not accessed by employees in other situations than helping the customer with support, or if separate instructions have been received from the customer.

Consent

By means of the previously mentioned customer-created campaign templates and field definitions, Hero Outbound facilitates that the customer can create fields in Hero Outbound for explicit documentation of consent and approval given by persons that are subject to sales, telemarketing, and communications activities through Hero Outbound – these persons are also called "leads".

Specifically, fields may be created for e.g. "URL for contest or homepage where the lead has given consent", "type of consent or approval given", "date and time for consent", "IP address (if available) from where the consent has been given", and similar.

The above-mentioned examples will typically be data that is present and with advantage can be input on the lead *before* processing via Hero Outbound.

In many cases the dialog that the lead is subject to will give rise to a need for further consent, approval, or accept (e.g. of an order) being registered. In these cases, corresponding fields can be created in Hero Outbound, such as channel-dependent approval for communication and marketing, continued interest in receiving digital communication, result of sales presentation and similar.

These consents, approvals, and accepts can be collected by entering data in fields, by sending a link to digital accept if answers are updated to Hero Outbound by means of the software's associated REST-API, or by recording verbal accept.

Processing of various categories of personal data

We have classified all data belonging to our customers as data controllers as "customer data". These are subject to the maximum security classification, and we thus do not have any lower security classification for Article 6 data than we have for Article 9 or 10 data.

We have a processor agreement with all our customers. When this is based on HeroBase's processor agreement template, we have asked the customer to account for what types of personal data (categorised according to Article 6, 9, 10, respectively 87) the customer intends to input and enter into Hero Outbound.

Every six months we take stock of whether there is an increasing tendency of indication of input/collection of Article 10 data, and if this is the case, we perform a design analysis of whether parts of our software should be restricted on category level to especially consider particularly sensitive data, e.g. by having customer administrators define on field level in campaign templates whether a field with the greatest likelihood will contain Article 6, 9, 10, or 87 data. However, at the time of writing we have not assessed this need to be present yet.

We are aware that Article 87 is not in essence a data category article on line with 6, 9, or 10, but a special condition regarding national identification number. However, we have decided to designate CPR-numbers as "Article 87 data" for interpretative reasons.

We have recognised that it is natural for a number of our customers that Article 9 data is present in Hero Outbound, as we have a relatively strong representation within the business sectors of insurance, unemployment funds, and trade unions.

Rights of the data subject

Hero Outbound registers all changes to data for a lead processed in our software, as well as all interactions with the lead in question.

As data controllers our customers can retrieve all leads input into and processed in Hero Outbound and see a full list of interactions with each lead.

As data controllers our customers can retrieve all leads input into and processed in Hero Outbound and see a full list of all data present on each lead.

As data controllers our customers can retrieve all leads input into and processed in Hero Outbound and see a full list of changes that has been made to data on each lead.

Thereby all processing activities are explicitly registered and are available to the customer directly in Hero Outbound's user interface.

As data controllers our customers can retrieve individual leads, block them for future contact, and/or delete all data present on each lead.

As data controllers our customers can retrieve individual leads and edit/rectify information on each lead.

As data controllers our customers can export the above-mentioned data, such that data can be transferred to a data subject; deleted from Hero Outbound, and that the data subject with its data can be moved to another system or service.

Thereby Hero Outbound supports our customers as data controllers when it comes to complying with the rights of the data subjects and as a starting point handling these efficiently and without undue delay.

General obligations as processor

We have procedures that ensure that we comply with our obligations as a processor and to the widest extent possible support our customers as data controllers in relation to the requirements that GDPR poses to them.

Our functions for supporting the rights of the data subjects, cf. the previous section, are collected on a few different pages in Hero Outbound that through module and rights management at the customer itself ensures our customers' possibility of allocating functional rights to using the functions according to a work-related need at the customer.

If HeroBase should receive an application directly from a data subject, instead of via the customer, HeroBase will within the framework of the legislation request further information from the data subject, and without undue delay forward the application or request to our customer. We have procedures for this that are communicated to and trained with our employees.

We have ensured processor agreements with sub-processors, including hosting and housing partners.

We have ensured that the requirements imposed by our customers on us through the contract and the processor agreement correspondingly are imposed on sub-suppliers and sub-processors.

Through regular training and campaigns we ensure awareness of significant areas within information security, data protection, as well as (but not limited to) GDPR.

We have procedures for data protection being part of the considerations and choices regarding design when Hero Outbound is changed and improved.

Acting according to instruction from our data controlling customers also include how long data is stored in Hero Outbound. Data is here understood as written data (numerical values, text strings and other entries – what traditionally is understood as data) and multimedia data (audio files from conversations that our customers have decided to record via Hero Outbound).

Instructions are given to HeroBase as processor through settings that the customer configures in Hero Outbound.

All leads belong to campaigns that belong to projects. Deletion rules for data can be defined on project level, such that all (or selected) data on leads closed with specific status automatically is deleted after "x" days.

These rules are executed on a nightly basis on Hero Outbound's database servers and delete data according to rules set up by our customers.

Data is stored on a backup for 7 days, after which data is also deleted from backup, and thereby after 7 days will be deleted from all database instances without the possibility of restore.

Security of processing, notification, and communication

We have established adequate technical and organisational measures, which are detailed in a later main section.

We have chosen ISO 27001 to be the information security framework that our information security code of conduct, procedures, and controls are based on.

We have procedures for managing information security incidents, including data breaches, as well as information security incidents.

We have procedures for notification to relevant authorities in cases where this is necessary , as well as notification to our customers as data controllers in case incidents or events concern these or might do so. This is done within set time limits that are defined in the processor agreements.

Data protection impact assessment

We have procedures for conducting data protection impact assessments (DPIA) in connection with the conduction of projects and development of Hero Outbound as software.

Data protection officer (DPO)

HeroBase has deselected having a data protection officer (DPO), cf. Article 37. The reason for the deselection is that HeroBase has a relatively insignificant amount of personal data for which HeroBase itself is the data controller of, and thus mainly has the role of being a processor and supplier of Hero Outbound. On the basis of this HeroBase does not systematically process personal data, just as it does not concern a large amount of sensitive or especially sensitive data.

Instead we have appointed and organised a full security organisation besides the usual operations organisation. The security organisation consists of an information security committee and an information security coordinator. The committee and the coordinator ensure embedding of the continual work with information security and additionally has a number of obligations defined by our information security code of conduct and procedures.

Transfer of personal data

All data in Hero Outbound belongs to our customers and HeroBase does not in any connection transfer, assign or exchange data with third parties. All exchange, output, and transfer of data is solely done by the customer itself by using functions in Hero Outbound or our associated REST-API.

Our hosting and housing partners, which we have sub-processor agreements with, only have data stored in the EU, cf. previous section. Data in Hero Outbound is thus never transferred to third countries, unless the customer decides to do this outside of the engagement with HeroBase.

Additionally, we have procedures concerning the portability of data, including management of physical media.

Technical and organisational measures

In this section we will elaborate on a number of matters regarding HeroBase's technical and organisational measures regarding the supply and operation of the software and solution Hero Outbound.

Human resource security

We have defined a number of procedures that ensure security prior to, during, and, if relevant, after employment.

Procedures concerning processes before a potential employment ensure that potential employees are screened and that relevant matters are checked within the framework of current legislation.

All employees must adhere to a number of terms regarding confidentiality about own, HeroBase's, and customers' matters. This is described in each employee's employment contract.

During employment it is ensured between the employee, the immediate manager, and the information security coordinator that the employee is kept up-to-date regarding and comply with aspects regarding information security.

We have procedures that ensure that employees at the termination of employment cannot cause damage to HeroBase or the system Hero Outbound by means of immediately removing rights to business systems and check this.

In addition, a number of sanctions have been defined for the event that the information security is breached or disregarded.

Asset management

All assets are defined with ownership, criticality, and technical dependencies such as services that are dependent on certain assets. Servers, systems, network etc. are documented and available for relevant technical personnel. At the introduction of new equipment and new systems, or at changes to architecture and infrastructure, relevant documentation is updated to ensure that this is always up-to-date.

The acceptable use of systems for employees has been defined, which i.a. includes guidelines for accessing, using, and exporting data. Data is considered categorised according to GDPR's categories for this purpose, and special procedures are applicable for certain types of data.

We have procedures concerning the management of portable devices, disposal of devices, as well as transport of portable, data-carrying devices, and for the classification and labelling of data. This means, for one thing, but is not limited to, that data solely must be stored in systems and on physical and virtual servers labelled and specified for the purpose. Customer data must not in principle be present anywhere else, including locally, on USB sticks, on other disks (flash drives), and similar. An exception to this is if a customer has requested in writing to be handed over data, or if it is necessary to transport data between two servers, and the transmission cannot occur via network.

If data is stored temporarily on such USB sticks, drives and similar, data must to the widest extent possible be anonymised or pseudonymised, and the physical device (including folders on it) must be password protected. As a rule, these devices must never be sent by regular mail to customers but must be transported by HeroBase's employees or picked up by the customer.

When physical servers are decommissioned, and data on hard disks no longer needs to be present on the drives in question, these disks must either a) be formatted in such a way that restore of data no longer is possible, b) be physically destroyed and the disks disposed of by employees in HeroBase's IT department, or c) both.

Access management

We have a string of procedures that ensure that access control and the allocation of rights occur in compliance with the established security level.

Only employees with a work-related need for having access to systems and data are granted access to the concerned business systems and associated data.

The heads of department are responsible for access rights being granted on the basis of a work-related need and in consideration of regulatory and contractual obligations.

We have a number of controls that ensure that this occurs on an ongoing basis, and that all access corresponds to the work-related needs in each function and for each employee.

We have defined a string of requirements for the protection of all devices (PCs, mobile phones, tablets) as well as passwords in all business systems. Employees are trained and checked regularly within these areas.

We have a number of procedures that ensure that only a group of privileged personnel has access to system administrator tools, central servers (e.g. domain controller), source code etc.

Production servers and other servers containing production data and customer data are only present in HeroBase's data centres and not at any office locations. Only specially trusted employees with a work-related need have access to the data centres. These accesses are assessed and inspected regularly.

Cryptography

We have procedures for the use of cryptography, including the generation and management of encryption keys and certificates.

This means, i.a., that Hero Outbound must have a valid SSL certificate, which HeroBase verifies, such that data exchange only occurs in a secure and encrypted manner (through HTTPS). SSL-certificates are managed solely by the IT department, where the application architect and network administrator are responsible for SSL certificates. No certificates may be acquired or issued bypassing these.

This requirement concerns access to Hero Outbound through the user interface and through API alike.

Physical and environmental security

Servers are only placed in data centres provided by suppliers who have been issued, and annually can show, assurance reports at the level of ISAE 3402.

HeroBase's office premises are subject to a number of procedures that secure the office as well as material and units stored at the office, regardless of servers only being placed in data centres.

This entails, i.a., procedures aimed at employees describing security measures for offices, common areas, and similar areas.

Operations security

Operating procedures and monitoring

We have operating procedures for the IT department's most significant duties, and these procedures are subject to versioning and change management.

We have defined the responsibility for ensuring that an assessment of the capacity requirements for critical IT systems is performed regularly.

Due to our size we cannot have a complete overlap on all functions, but cf. previous description we aim, by virtue of segregation of duties and thorough as well as continuous documentation and knowledge sharing, to avoid dependence on individuals. The IT department, led by HeroBase's CTO, consists primarily of developers in a "devops" constellation, where two persons are dedicated to operations, optimising servers and infrastructure, monitoring and handling operational issues, but where all have operations as the first priority in case of technical issues on the platform or information security issues.

All instances of Hero Outbound are monitored by means of monitoring tools. Thereby we monitor, among other things, access to servers, CPU/memory/disk I&O usage, similar for database servers, layers (in milliseconds) between master and slave databases, heavy SQL queries made by applications or directly by a client, and much more.

Critical levels and values are defined for all these monitoring areas. Alarms must trigger when these values are reached and must be sent to key employees either via email (for less critical alerts) or SMS (critical alerts).

Historical logs and events are regularly reviewed in a structured manner to perform improvements and optimisation.

We have procedures for backup besides continuous data replication, and the usability of backups for restore is regularly checked.

Development of Hero Outbound, management, and quality assurance

The development of Hero Outbound, including release of changes, occurs according to HeroBase's formalised and embedded development model.

Development occurs in development environments where code is branched from the main branch/"default". These development branches are connected with the staging database, where test data is found. Test data and production data are thus completely segregated, and customers' data must not be copied from master to staging without approval from HeroBase's CTO. If this permission is granted, it can and will only comprise configuration data in order to test and develop up against true, complex data in order to ensure the quality of the development, but it must and can never comprise data on the customer's prospects, employees or similar which are personally identifiable and can be categorised in accordance with GDPR's articles 6, 9, 10, and 87.

Function testing takes place in development branches (also called feature branches), after which code is merged to pre-production, on to CX branch, on to pre-release branch, on to release branch, from which code is finally deployed for production.

Integration testing with associated regression tests and happy flow testing takes place from CX branch, pre-release branch and/or release branch, where testing occurs in the master database, but on our own test data. Customers' personally identifiable data are thus not part of tests and are not accessed or viewed by HeroBase's employees in any of these test phases. Data in the master database on own accounts is created in such a way that it structurally looks like production data that customers work with, whereby data security, confidential processing, and simultaneous quality assurance are ensured and balanced.

Logging

We have procedures concerning the scope, processing, protection, and check of logging on various system types.

All logins and significant user actions in Hero Outbound are monitored and logged. The logging of significant user actions concerns i.a. data export, such that customer administrators have an overview over which users that access and export data.

All changes to data are registered.

All significant changes to configurations are registered.

These registrations are also available for customer administrators through visible logs in the user interface.

The logging level also comprises employees at HeroBase, whereby it is checked that these do not access customer data without a work-related need for this. This is checked and tested in a detailed manner on the basis of spot checks.

Communications security

We have procedures for network management and monitoring, including maintenance of network and network equipment.

Traffic on all connections and interfaces are monitored in relation to data volume over periods of time. Alarms have been set up that are triggered and sent to technical personnel in case of abnormalities (traffic spikes, significant delays between master databases and slave databases, and much else). Regarding tele connections, the amount of provider channels, the amount of server channels (Freeswitch channels), and amount of ongoing calls, amongst other things, are monitored, and max values for periods of time are logged.

This ensures ongoing, correct capacity management as well as a precaution against misuse.

In addition, as an extra layer of security against misuse we cooperate with fraud detection departments at all telecom operators that we use as sub-suppliers.

Exchange of information solely occurs by means of secure connections. If this occurs via the public Internet, data is encrypted (in principle by means of HTTPS). Systems that can communicate on internal connections (on internal IP address behind firewall – and between data centres via fibre connection, through which servers on various locations also can reach each other on internal IP address) use this method for data exchange via LAN.

Supplier relationships

In all cooperation agreements with suppliers we have defined security requirements and minimum requirements for the services provided to us by the supplier.

We have ensured that the matters we base our agreement on regarding the use of the product and service Hero Outbound in relation to customers are in accordance with our requirements to our suppliers.

We regularly, and at least annually, review the cooperation agreements, just as we obtain assurance reports for the entered agreements.

We have defined a responsibility for quarterly reviewing reports from the external service providers for operational equipment regarding events, issues, errors, crashes, and logging.

Information security incident and event management

The information security committee has defined procedures for information security incidents and events, which are embedded in HeroBase and which the management is responsible for being observed.

We define information security incidents as:

- The detection of successful external and unwanted intrusion in systems
- Finding customer data (hosted in the master database for Hero Outbound) online, where there is an obvious or strong suspicion that the publication of data has not occurred with the customer's approval and intent
- Finding data on current or former employees in HeroBase online, where publication of data has occurred without HeroBase's involvement or intent
- Finding other confidential business data online (according to the same directions) defined as customer contracts, revenue, or information which is classified as secret according to further definition by the information security committee

We define information security events as:

- Events that, if they had not been discovered, could have led to security incidents
- Situations where unintended data or information by accident (due to human error) has been sent to other recipients than the intended, and that it is assessed that this may entail damage or serious consequences for HeroBase

Procedures have been defined for both, which describe for employees and managers how they should act in case of incidents and events, including (but not limited to) collecting evidence and contact with authorities, if necessary.

All employees are aware of the instructions and have trained them.

Information security aspects of business continuity management

We have defined the responsibility for preparing emergency plans, contingency plans, and restore plans.

We have established adequate redundancy to meet the requirements for availability and the guarantees for uptime that we have agreed in contracts with our customers.

All technical employees have trained the plans.

Plans and procedures are regularly reviewed and in the wake of each operational issue where human action has been necessary to re-establish operations on parts of the platform.

Full transparency for data controllers

On the basis of a defined vision that our customers as data controllers must be able to acquire as much insight as possible regarding all matters related to potential platform use and security without approaching us as a software provider, we have made additional overviews and parameters visible for the customer in Hero Outbound.

We show a log of user actions that have led to the display of many leads' data at once on the screen and which might have led to an export of data. Performing this in Hero Outbound will in many cases just be a part of solving daily administrative tasks, but as the actions in theory could be the first step in inappropriate use of the system that ultimately could lead to a data breach, we believe in a preventive effect by making this information available to our customers' administrators.

We show a log of logins in the customer's Hero Outbound account containing user, time, and IP address.

We show overviews of changes to configuration on campaigns, including setup of the mentioned "triggers" that can send data from Hero to external systems.

We want ”privacy by design” to be a completely integrated part of Hero Outbound’s platform design and we have i.a. incorporated measures caused by GDPR in fundamental entities and concepts in our platform. As explained, all private individuals/data subjects (as well as other entities treated in Hero Outbound – e.g. companies) are represented as “leads”, and these always have a status (called LeadStatus) that Hero Outbound uses for managing the next action for the lead as well as for reporting purposes. When customers’ administrators at requests from data subjects delete their data completely by using the right to be forgotten, the lead has special status particularly for this, to clearly distinguish between these and other actions in the processing of leads. The extract beneath from the documentation of Hero Outbound’s REST-API exemplifies how these statuses have been made a fundamental part of the platform design in Hero Outbound.

```
/// <summary>
/// User request to clear info about him, all lead data is cleared from
the system according
/// </summary>
Anonymized = 610,

/// This status can be set by administrators to signal that the lead
/// should not be called, since it in corporate's DoNotCall list.
/// </summary>
DoNotCall = 700,
```

Compliance

This report has been prepared to supply in-depth information to our customers and their interested parties (including auditors) regarding the requirements and contents of the EU General Data Protection Regulation (“GDPR”). As part of checking our implementation and embedding of our technical and organisational measures, an ISAE 3402 assurance report has been prepared besides this present assurance report.

We regularly check that rules and procedures are observed, followed, and documented.

We ensure that we act in accordance with applicable legislation and furthermore that we adhere to the requirements posed to documentation by national legislation.

We ensure that personal data is protected and processed in accordance with the Data Protection Act and GDPR.

For years, we have used ISO 27001 as the framework of reference for information security in HeroBase and regarding the development and operations of Hero Outbound. The mentioned ISAE 3402 assurance report is our first ISAE 3402 assurance report for the delivery of the product and service Hero Outbound, which is why that is a type I assurance report. It has been embedded in the management that compliance with rules and procedures in our information security code of practice, including controls connected with rules and procedures, must be formalised, documented, and subject to annual audit by an independent external IT auditor, which is why we also in future will prepare ISAE 3402 (type II) assurance reports.

Complementary controls

Regarding our customers, HeroBase is responsible for delivering the services and the operations described in the contract concerning Hero Outbound between the customer and HeroBase.

Matters not comprised by the contract are the customer’s own responsibility.

Creation of users, protection of user information, and secure login procedures are the responsibility of the customer. The customer can by writing to HeroBase request the establishment of an IP lock on the customer’s Hero Outbound account, whereby login only will be possible from explicitly defined whitelisted IP addresses. HeroBase recommends our customers to do this to the extent it is possible for the customer, in order to protect the customer's data and activities in Hero Outbound.

Regarding data uploaded to Hero Outbound by the customer, it is a significant division of responsibility that the customer is the data controller, and HeroBase is the processor. Thus, HeroBase only acts according to instructions from the customer. In the contract or in the processor agreement that the customer provides HeroBase the customer gives an indication to HeroBase of what types/categories of data that the customer intends to upload to and process in Hero Outbound. A processor agreement must be established between HeroBase and the customer.

Regarding GDPR, HeroBase provides a string of functions on the platform Hero Outbound that enable the customer to comply with GDPR's requirements of data controllers. These functions include (but are not limited to) the possibility of retrieving data as well as a log of all interactions between agent and "subjects", the possibility of correcting data, the possibility of deleting data, and much more.

It is the customer's responsibility to have defined and embedded a procedure at the customer that ensures compliance with GDPR by i.a. complying with the requirements of response time regarding enquiries from private individuals/data subjects. HeroBase provides functions through the tool Hero Outbound, but cannot be held responsible for the customer's definition, embedding, and observation of procedures that are to ensure the customer's compliance.

Independent service auditor's assurance report on compliance with the EU General Data Protection Regulation (GDPR) as at 17 December 2018

To HeroBase A/S' management, the company's customers and their auditors

As agreed, we have reviewed HeroBase A/S' solution Hero Outbound in relation to compliance with the EU General Data Protection Regulation (GDPR) as at 17 December 2018.

Our opinion is issued with reasonable assurance.

The assurance report is intended solely for the use of the management of HeroBase A/S, their customers and their auditors for assessing the existing procedures, and must not be used for other purposes.

Management's responsibility

HeroBase A/S' management is responsible for implementing and ensuring the maintenance of procedures as required by the EU General Data Protection Regulation (GDPR).

Service auditor's responsibility

On the basis of the conducted work, it is our responsibility to express an opinion on whether the company complies with the requirements stated in the EU General Data Protection Regulation (GDPR).

We have conducted our work in accordance with ISAE 3000, Assurance engagements other than audits or reviews of historical financial information and additional requirements under Danish audit regulation in order to obtain reasonable assurance for our opinion.

REVI-IT A/S applies International Standard on Quality Control 1 and accordingly 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.

We have complied with the independence and other ethical requirements of the Code of Ethics for professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Our work comprised enquiries, observations as well as assessments and examination in spot checks of the information we have been provided.

Due to limitations in all control systems errors or fraud may occur, which might not be uncovered by our work. Also, the projection of our opinion on transactions in subsequent periods is subject to the risk of changes to systems or controls, changes to the requirements in relation to the processing of data or to the company's compliance with the described policies and procedures, whereby our opinion may not be applicable anymore.

Limitations in controls at a processor

HeroBase A/S' description is prepared to meet the common needs of a broad range of data controllers and their auditors and may not, therefore, include every aspect of Hero Outbound that each individual data controller may consider important according to their particular circumstances. Also, because of their nature, controls at a processor may not prevent or detect all breaches on personal data security. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a processor may become inadequate or fail.

Opinion

This opinion is formed on the basis of the understanding of the criteria accounted for in the assurance report's introductory section and which are based on the requirements in the EU General Data Protection Regulation (GDPR).

It is our opinion that HeroBase A/S' solution Hero Outbound in all material respects has met the criteria mentioned as at 17 December 2018.

Description of tests of controls

The specific controls tested, and the nature, timing and results of these tests are listed in the subsequent main section.

Intended users and purpose

This assurance report is intended only for customers who have used HeroBase A/S' solution Hero Outbound, and their auditors, who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves.

Copenhagen, 17 December 2018

REVI-IT A/S
State authorised public accounting firm

Henrik Paaske	Martin Brogaard Nielsen
State Authorised Public Accountant	IT Auditor, CISA, CIPP/E, CRISC, CEO

Control objectives, controls, tests, and related test controls

The following overview is provided to create an overview of the controls implemented by HeroBase A/S in relation to compliance with the EU General Data Protection Regulation (GDPR). Our testing of functionality comprised the controls that we considered necessary to provide reasonable assurance for compliance with the specified articles as at 17 December 2018.

The requirements evident directly from the EU General Data Protection Regulation (GDPR) or the Data Protection Act cannot be derogated from. However, it can be adjusted how the security is implemented, as the security requirements in GDPR in several respects are of more general and overall character that i.e. must consider purpose, nature of processing, category of personal data etc. In addition, there may be specific requirements in each customer contract that may have a scope extending beyond the general requirements of the Data Protection Act. If this is the case, these are not covered by the following.

Moreover, our assurance report does not apply to any controls performed at HeroBase A/S' customers, as the customers' own auditors should perform this review and assessment.

We performed our tests of controls at HeroBase A/S by taking the following actions:

Method	General description
Enquiry	Interview, i.e. enquiry with selected personnel at the company regarding controls
Observation	Observing how controls are performed
Inspection	Review and evaluation of policies, procedures, and documentation concerning the performance of controls
Re-performing control procedures	We have re-performed – or have observed the re-performance of – controls in order to verify that the control is working as assumed

2: Principles

Article	Control objective	Review performed	Test result
5 - Principles relating to processing of personal data	Procedures and controls are observed that ensure that collection, processing, and storage of personal data occurs in accordance with the principle for processing of personal data.	We have enquired about updated and management-approved written procedures for the processing of personal data that comprises principles for the processing of personal data, and we have inspected the procedures. We have enquired about regular control of compliance with the principles, and we have inspected the control.	No significant deviations noted.
6 - Lawfulness of processing	Procedures and controls are observed that ensure that only lawful processing of personal data takes place.	We have enquired about updated and management-approved written procedures for the processing of personal data, and we have inspected the procedures. We have enquired about legal base for processing personal data, and we have inspected the legal base. We have enquired about regular control of the processing taking place on a legislative basis, and we have inspected the control.	No significant deviations noted.
7 - Conditions for consent 8 - Conditions applicable to child's consent in relation to information society services	Procedures and controls are observed that ensure that the data subjects have given written consent for the processing of personal data.	We have enquired about functionality in the system for obtaining, managing, and documenting consent, and we have inspected the functionality.	We have observed that the company is not responsible for obtaining consent in connection with the processing of personal data, but that functions supporting obtainment of written consent is made available to data controllers. No significant deviations noted.
9 - Processing of special categories of personal data 10 - Processing of personal data relating to criminal convictions and offences	Procedures and controls are observed that ensure that processing of special categories of personal data only takes place in consideration of established criteria, conditions, and the necessary guarantees.	We have enquired about updated and management-approved written procedures for the processing of special categories of personal data, and we have inspected the procedures. We have enquired about legal basis for processing special categories of personal data, and we have inspected the legal basis. We have enquired about regular control of the processing taking place on a legislative basis, and we have inspected the control.	No significant deviations noted.

2: Principles

Article	Control objective	Review performed	Test result
11 - Processing which does not require identification	Procedures and controls are observed that ensure that storage, gathering and processing of information for identification of the data subject is maintained as long as identification is required.	*The company does not perform processing not requiring identification, whereby this item is not applicable.*	*Not applicable.*

3: Rights of the data subject

Article	Control objective	Review performed	Test result
12 - Transparent information, communication and modalities for the exercise of the rights of the data subject	Procedures and controls are observed that ensure that information on the processing of personal data can be supplied to the data subject in a transparent, easily accessible and comprehensible form.	*The company does not collect personal information as a data controller, whereby this item is not applicable.*	*Not applicable.*
	Procedures and controls are observed that ensure that the exercise of the rights of the data subject happens in a timely manner, including responding to the data subject's requests and providing a reason in case of refusals.	We have enquired about a procedure for the exercise of the rights of the data subject taking place in a timely manner. We have enquired about a control for securing observance of the company's procedure, and we have inspected the control.	No significant deviations noted.
13 - Information to be provided where personal data are collected from the data subject 14 - Information to be provided where personal data have not been obtained from the data subject	Procedures and controls are observed that ensure that the data subject has received the controller's contact information, information on the purpose of the processing of personal data, as well as information of any transfer of personal data to recipients, third countries, or international organisations.	*The company acts as a processor and it is not part of the company's services to collect personal information from data subjects, whereby this item is not applicable.*	*Not applicable.*

3: Rights of the data subject

Article	Control objective	Review performed	Test result
	Procedures and controls are observed that ensure that the data subject has received information of the right to insight, rectification, or deletion of personal data as well as restriction of the processing.	*The company does not collect personal data as a data controller, whereby this item is not applicable.*	*Not applicable.*
15 - Right of access by the data subject	Procedures and controls are observed that ensure that the data subject's right to insight in own registered personal data and the processing of this is observed.	We have enquired about a procedure for obtaining requests for insight from the data subjects, including notification to processors and recipients of the personal data, and we have inspected the procedure. We have enquired about a control for ensuring observance of the company's procedure, and we have inspected the control.	No significant deviations noted.
16 - Right to rectification 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing	Procedures and controls are observed that ensure that the data subject's right to rectification of own registered personal data is observed, including corrections at the recipients of the personal data.	We have enquired about a procedure for rectification of personal data, including notification to processors and recipients of the personal data, and we have inspected the procedure. We have enquired about a control for ensuring observance of the company's procedures, and we have inspected the control.	No significant deviations noted.
17 - Right to erasure ('right to be forgotten') 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing	Procedures and controls are observed that ensure that the data subject's right to erasure of own registered personal data is observed, including deletion at the recipients of the personal data.	We have enquired about a procedure for the erasure of personal data when the company receives a request from a data subject, and that processors are notified to delete personal data, and we have inspected the procedure. We have enquired about a control for ensuring observance of the company's procedures, and we have inspected the control.	No significant deviations noted.

3: Rights of the data subject

Article	Control objective	Review performed	Test result
18 - Right to restriction of processing 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing	Procedures and controls are observed that ensure that the data subject's right to restriction of processing of own personal data is observed, including restrictions at the recipients of the personal data.	We have enquired about a procedure for the restriction of personal data when the company receives a request from a data subject, and that processors are notified to restrict personal data, and we have inspected the procedure. We have enquired about a control for ensuring observance of the company's procedure, and we have inspected the control.	No significant deviations noted.
20 - Right to data portability	Procedures and controls are observed that ensure that the data subject's right to transferring own personal data to another controller is observed.	We have enquired about a procedure for data portability of personal data when the company receives a request from a data subject, and that processors are obligated to assisting the company, and we have inspected the procedure. We have enquired about a control for ensuring observance of the company's procedure, and we have inspected the control.	No significant deviations noted.
21 - Right to object 22 - Automated individual decision-making, including profiling	*N/A – the requirements are covered by the control objective in article 6.*	*Not applicable.*	*Not applicable.*
23 – Restrictions	*N/A – this is not relevant in relation to the control objective of an assurance report.*	*Not applicable.*	*Not applicable.*

4: Controller and processor

Article	Control objective	Review performed	Test result
24 - Responsibility of the controller	Procedures and controls are observed that ensure that the controller's technical and organisational measures for protecting the data subjects' rights and that the processing of personal data is approved by the controller.	We have enquired about a procedure that ensures that the company has implemented technical and organisational measures to protect the data subjects' personal data, including division of roles, password control, logging of activity etc., and we have inspected the procedure. We have enquired about a control for ensuring observance of the company's procedure, and we have inspected the control.	No significant deviations noted.
25 - Data protection by design and by default	Procedures and controls are observed that ensure that the requirements to data protection have been implemented by design and by default in the company's technical and organisational security measures.	We have enquired whether the company has decided on and has implemented data protection by design and by default, and that these are regularly checked, and we inspected controls for this.	No significant deviations noted.
26 - Joint controllers 27 - Representatives of controllers or processors not established in the Union	*N/A – these are not relevant in relation to the control objectives for an assurance report.*	*Not applicable.*	*Not applicable.*
28 - Processor 29 - Processing under the authority of the controller or processor	Procedures and controls are observed that ensure that the processing of personal data only occurs with reference to a contract or another legally binding document (processor agreement), and that the processing is only done by processors approved by the controller.	We have enquired about documentation for the company having entered processor agreements with its processors, and that these agreements comply with the regulation's requirements to processors, including sub-processors, and we have in spot checks inspected the documentation. We have enquired about periodic control for the processor agreements being updated, and we have inspected the control.	No significant deviations noted.

4: Controller and processor

Article	Control objective	Review performed	Test result
30 - Records of processing activities	Procedures and controls are observed that ensure that the company maintains a record over categories of processing activities performed on behalf of the controllers.	We have enquired about documentation for the company having prepared a record of all processing activities, and we have inspected the record. We have enquired about a control for the record being regularly updated and reviewed, and we have inspected the control.	No significant deviations noted.
31 - Cooperation with the supervisory authority	*N/A – this is not relevant in relation to the control objective of an assurance report.*	*Not applicable.*	*Not applicable.*
32 - Security of processing	Procedures and controls are observed that ensure that on the basis of an evaluation of risks, adequate technical and organisational security measures have been established to prevent accidental or illegal destruction, loss, change to, unauthorised disclosure of, or access to, personal data.	We have enquired about the preparation of a management-approved risk analysis, and we have inspected the risk analysis. We have enquired about the preparation of necessary procedures and technical measures, including i.a. change management, protection against unauthorised access to personal data, physical security, etc., and we have inspected the procedures. We have in spot checks inspected the implemented technical and organisational measures on the basis of the above-mentioned procedures. We have enquired about a control for periodic review of the company's risk picture and the associated technical and organisational measures, and we have in spot checks inspected the control.	We have observed that the company's risk analysis does not contain an overview of decisions on any mitigating actions performed on the basis of the risk assessment. In addition, we have observed that the risk analysis does not explicate how risks will impact the rights of the data subjects. We have observed the following in InterXions assurance report: - The outer physical perimeter security of one of the sub-supplier's data centres has in connection with ongoing construction work not been sealed, and the sub-supplier has in connection with this not implemented additional measures to mitigate the increased risk. Thus, generators and cooling system has been accessible without obstacle. - Monitoring of one of the sub-supplier's data centres has at inspection shown the wrong time stamp. The matter was remedied within 48 hours. - At present there is not a clear mapping between the company's identified risks, control objectives, and the control description. - No documentation is present for the company having

4: Controller and processor

Article	Control objective	Review performed	Test result
			received consultancy services from the Information Security Committee (INFOSEC), as the control description stipulates. - In connection with spot checks of user management, in 3 of 25 spot checks the process has not been documented in compliance with the company's procedure for this. No further significant deviations noted.
33 - Notification of a personal data breach to the supervisory authority 34 - Communication of a personal data breach to the data subject	Procedures and controls are observed that ensure that processor in case of personal data breaches can support the controller's obligation to timely and adequate notification to the supervisory authority as well as communication to the data subjects.	We have enquired about the company's procedure for managing personal data breaches, and we have inspected the procedure. We have enquired about periodic review of the procedure, and we have inspected the control.	No significant deviations noted.
35 - Data protection impact assessment	Procedures and controls are observed that ensure that processor has received the result of the controller's data protection impact assessment, before personal data is processed, and that a new data protection impact assessment is performed in case of changes to the risk that the processing activities constitute.	We have enquired about documentation for the management's assessment of the necessity of performing own impact assessments on all or parts of the data processing for each controller, and we have inspected the assessment. We have enquired about control for periodic review of the decision on a need for preparing impact assessments, and we have inspected the control.	We have observed that the company is not subject to requirements of performing an impact assessment for the entire processing. No significant deviations noted.

4: Controller and processor

Article	Control objective	Review performed	Test result
36 - Prior consultation	Procedures and controls are observed that ensure that processor has received the result of the controller's consultation at the supervisory authority, if the data protection impact assessment shows that the processing of personal data will entail a high risk due to lack of measures implemented by the controller to limit the risk.	*The company does not have processing activities giving rise to consultation at the Danish Data Protection Agency, whereby this item is not applicable.*	*Not applicable.*
37 - Designation of the data protection officer	Procedures and controls are observed that ensure that – in the cases where it is required – a data protection officer has been designated, who complies with the requirements of adequate competences, and who has been announced to the supervisory authority.	We have enquired about documentation for the management's assessment of the necessity of appointing a data protection officer, and we have inspected the assessment. We have enquired about periodic control of assessing the necessity of appointing a data protection officer.	No significant deviations noted.
38 - Position of the data protection officer	Procedures and controls are observed that ensure the data protection officer's position, including that a data protection officer does not receive instructions regarding the performance of his/her tasks, and that a data protection officer does not perform tasks or have other duties that can lead to a conflict of interests.	*The company is not subject to the requirement of appointing a data protection officer. The company has therefore deselected appointing a data protection officer, whereby this item is not applicable.*	*Not applicable.*

4: Controller and processor

Article	Control objective	Review performed	Test result
39 - Tasks of the data protection officer	Procedures and controls are observed that ensure that the data protection officer is aware of the scope of his/her tasks, is involved adequately and timely in all questions regarding protection of personal data, and reports directly to the management of the controller or of the processor.	*The company is not subject to the requirement of appointing a data protection officer. The company has therefore deselected appointing a data protection officer, whereby this item is not applicable.*	*Not applicable.*
40 - Codes of conduct 41 - Monitoring of approved codes of conduct 42 - Certification 43 - Certification bodies	*N/A – these are not relevant in relation to the control objective of an assurance report.*	*Not applicable.*	*Not applicable.*

5: Transfers of personal data to third countries or international organisations

Article	Control objective	Review performed	Test result
44 - General principle for transfers 45 - Transfers on the basis of an adequacy decision 46 - Transfers subject to appropriate safeguards 47 - Binding corporate rules 48 - Transfers or disclosures not authorised by Union law 49 - Derogations for specific situations 50 - International co-operation for the protection of personal data	Procedures and controls are observed that ensure that transfer of personal data to a third country or an international organisation only occurs, if the Commission has established that the third country, an area, or one or more specific sectors in this third country or the international organisation in question has an adequate level of protection.	We have enquired about transfer of personal data to third countries and we have inspected documentation for the company not transferring personal data to third countries.	No significant deviations noted.