Independent service auditor's assurance report on the description of controls, their design and implementation regarding development and operations of the software Hero Outbound as at 1 September 2018

ISAE 3402, type I

HeroBase A/S

CVR-no. 31 07 31 03

September 2018

Table of contents

Section 1: HeroBase A/S' statement

The accompanying description has been prepared for customers who have used HeroBase A/S' operating services related to the service 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, when obtaining an understanding of customers' information systems relevant to financial reporting.

HeroBase A/S confirms that:

(a) The accompanying description in Section 2 fairly presents HeroBase A/S' development and operations of the software Hero Outbound for customers as at 1 September 2018. The criteria used in making this statement were that the accompanying description:

(i) Presents how the system was designed and implemented, including:

- The type of services provided, when relevant
- The procedures, within both information technology and manual systems, by which those transactions are initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers
- Relevant control objectives and controls designed to achieve these objectives
- Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve the control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone
- Other aspects of our control environment, risk assessment process, information system and communication, control activities and monitoring controls that were relevant to processing and reporting customer transactions.

(ii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and implemented as at 1 September 2018. 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

Søborg, 1 September 2018

HeroBase A/S

Casper Langhoff
CEO

Kenny Andreasen
CTO & CIO

Section 2: HeroBase A/S' description of development and operations of the software 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 in the International Standard for Assurance Engagements on controls at a service organisation, ISAE 3402.

Additionally, the purpose of this description is to provide information on our information security code of practice which is applicable for our delivery of the product and service Hero Outbound to our customers.

The description comprises the control areas and controls regarding Hero Outbound, which 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 contact, 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 that incoming phone calls are 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 the centre to perform its 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 placed 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.

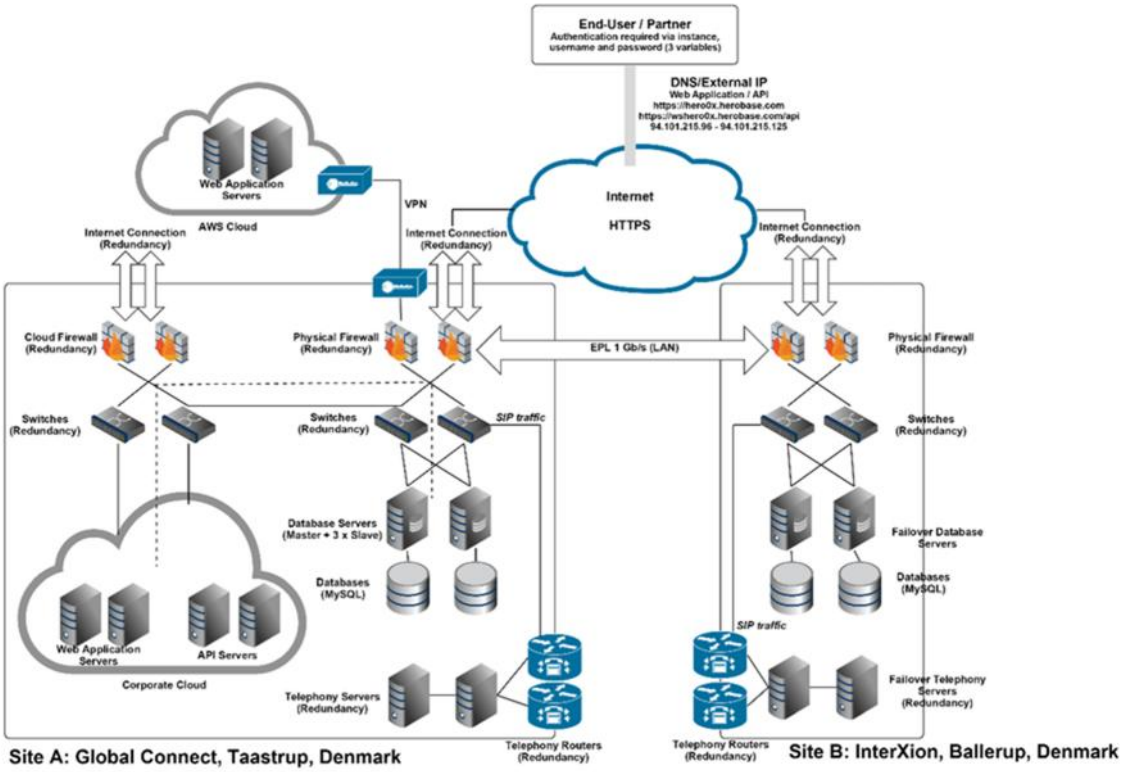

Fig. 1: The Hero Outbound platform, general infrastructure as at mid-2018.

We believe that by appealing to the everyday heroes by designing complete solutions for their workplaces, and by supplying solutions which turns 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. In conclusion, 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 data processor for a number 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 data processors, and we gladly express this in various connections. As a data processor we have furthermore ensured that we have processor agreements with all our customers on Hero Outbound who in this constellation are data controllers.

Information security management and security policy

HeroBase's general information security policy is prepared for the purpose of ensuring a continuous embedding of working methods, principles, and routines that comply with the determined security level.

The management approves the policy, which is signed by our CEO, and management is responsible for the policy being observed.

The information security policy must be observed in all regards and aims to ensure a secure and stable delivery of the product and service Hero Outbound, including compliance with relevant legislation, such that all significant risks of breakdowns, data theft, and data breaches are reduced.

The policy is reviewed and approved annually. The information security coordinator is the management's and information security committee's "auxiliary arm" in the daily embedding of the policy, and this ensures communication on an ongoing basis to all relevant parties. Additionally, all employees annually sign that they have read and comply with the policy and the associated information security code of practise.

Organisation of information security

Segregation of duties

We have a clear and well-defined organisation with segregation of duties, which entails that dependency on key persons is reduced as much as possible. In addition, segregation of duties has been introduced to areas where there is a risk of the occurrence of misuse of the company's data and information.

Contact with authorities

We have defined responsibility for contact with public authorities regarding topics pertaining to the area of information security.

Project management

We have defined the responsibility for HeroBase's project management model managing information security in all phases in an adequate manner, such that projects do not impact HeroBase's overall risk exposure to a negative degree. Information security is considered in all projects, regardless of their size.

Equipment and teleworking

We have a procedure for the use of mobile devices and home workplaces/remote workplaces. Minimum requirements have been defined for the protection of all devices, as well as access to business systems and data. All devices must be protected by antivirus and firewall. A number of system accesses to HeroBase's business systems require VPN access. These are issued and installed by HeroBase's IT department (approval by HeroBase's CTO, issuing and configuration of an employer in the IT department). VPN can be installed on PCs supplied and owned by HeroBase, but never on privately owned PCs.

Human resource security

We have defined a number of procedures that ensure security before, during and, if applicable, 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 conditions regarding confidentiality regarding their own, HeroBase's, and customers' matters. This is described in each employee's employment contract.

During employment it is ensured in cooperation between the employee, day-to-day leader, and the information security coordinator that the employee is kept up-to-date with, and complies with aspects regarding, information security.

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

In addition, a number of sanctions have been defined, in case 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, as well as 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 continually 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&I 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.

The development process is HeroBase's own method derived from an agile approach to development, SCRUM, and RUP. The development takes place in sprints, but not of an eternal, specified duration, as sprints are defined according to prioritised tasks in backlog.

On the basis of the classic project triangle consisting of time, scope, and resources, time is the factor that defines the objective for master releases with a release at least every 4 weeks, but we aim to make a master release every 3 weeks. Quality and marking tests as complete, however, are always to be considered

more important than the desire of making more frequent releases, as a zero-bug tolerance when new code is deployed for production overrides the desire of having new functions/features released quickly to customers.

Next to master releasees, hot fix releases are performed with corrections of distinct errors and significant inexpediencies. Significant errors and disclosed security weaknesses with the priority of 1 or 2 (cf. HeroBase's operations procedure) must always be handled as quickly as possible, and no later than within 3 working days.

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, and 10.

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 are 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.

Beneath please find in detail and chronological order how all cases are processed from creation, prioritisation, and approval, up through HeroBase's development flow.

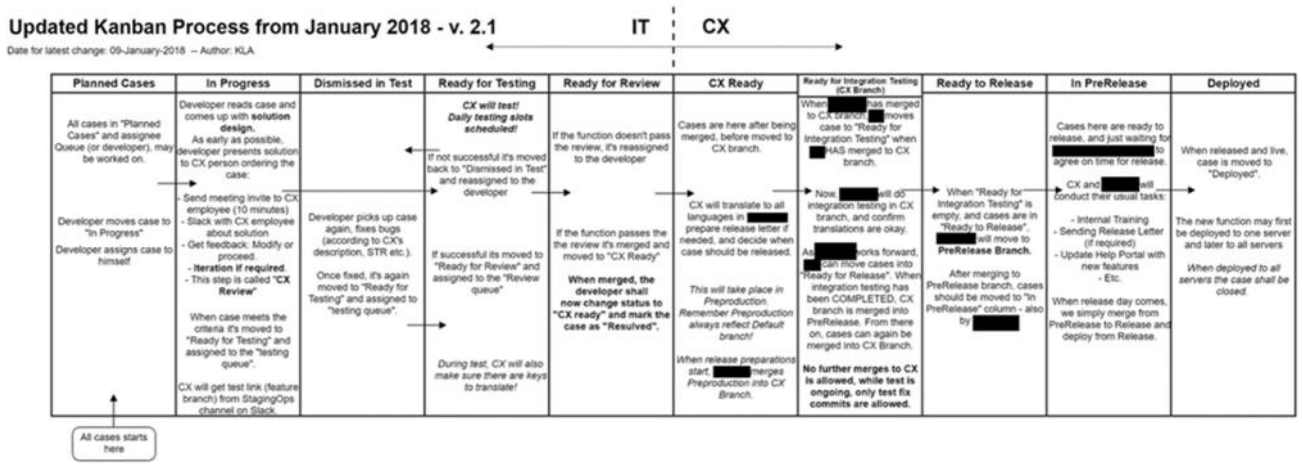

Fig. 2: Process and development model for Hero Outbound

HeroBase's release manager is the day-to-day responsible person for the process, and the process is evaluated every other week on a meeting between the release manager and HeroBase's CTO.

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.

Systems acquisition, development and maintenance

We have procedures that ensure secure change management in business supporting systems. The procedures prescribe i.a. that change logs are obtained and evaluated, and that changes are tested before they are released.

As all significant internal work processes are documented, the process documentation is updated where necessary, in connection with changes.

Please note that this section and the procedures referred to herein concern maintenance and changes in business supporting systems, not the solution Hero Outbound itself. Procedures and principles for changes in Hero Outbound are described in a previous, separate section.

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) gathering 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 after each operational issue where human action has been necessary to re-establish operations on parts of the platform.

Compliance

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. This is our first ISAE 3402 assurance report for the delivery of the product and service Hero Outbound, which is why this 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 data 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.

Section 3: Independent service auditor's assurance report on the description of controls and their design and implementation

To the management of HeroBase A/S, HeroBase A/S' customers, and their auditors.

Scope

We have been engaged to report on HeroBase A/S' description, presented in Section 2. The description, as confirmed by the management of HeroBase A/S' management, covers the company's processing of customer transactions in the company's software solution Hero Outbound as at 1 September 2018 as well as the design and operation of the controls related to the control objectives stated in the description.

We did not perform any procedures regarding the operating effectiveness of controls included in the description and, accordingly, do not express an opinion thereon.

Our opinion is issued with reasonable assurance.

HeroBase A/S' responsibility

HeroBase A/S is responsible for preparing the description (section 2) and accompanying statement (section 1) including the completeness, accuracy and method of presentation of the description and statement. Additionally, HeroBase A/S is responsible for providing the services covered by the description; stating the control objectives; and for the design, implementation and effectiveness of operating controls for achieving the stated control objectives.

REVI-IT A/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 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.

The firm 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.

REVI-IT A/S' responsibility

Based on our procedures, our responsibility is to express an opinion on HeroBase A/S' description (section 2) as well as on the design and implementation of the controls related to the controls objectives stated in that description. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by IAASB. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are suitably designed in all material respects.

An assurance engagement to report on the description and design of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed. An assurance engagement of this type also includes evaluating the overall

presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified by the service organisation, described in section 2.

As noted above, we did not perform any procedures regarding the operating effectiveness of controls included in the description and, accordingly, do not express an opinion thereon.

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

Limitations of controls at a service organisation

HeroBase A/S' description in section 2 is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the systems that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion were those described in HeroBase A/S' description in Section 2 and on the basis of this, it is our opinion that:

(a) the description of the controls, as they were designed and implemented as at 1 September 2018, is fair in all material respects

(b) the controls related to the control objectives stated in the description were suitably designed as at 1 September 2018 in all material respects

Intended users and purpose

This assurance report is intended only for customers who have made use of HeroBase A/S' development and operations of the software Hero Outbound and the auditors of these customers, who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves. This information serves to obtain an understanding of the customers' information systems, which are relevant for the financial reporting.

Copenhagen, 1 September 2018

REVI-IT A/S
State authorised public accounting firm

Henrik Paaske
State Authorised Public Accountant

Martin Brogaard Nielsen
IT Auditor, CISA, CIPP/E, CRISC, CEO