# Assurance report

## emagine

Independent auditor's ISAE 3000 assurance report on information security and measures pursuant to compliance with the EU General Data Protection Regulation (GDPR) in the role of data controller for emagine's services supported by ProManagement throughout the period from 1 March 2022 to 28 February 2023

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

May 2023

Table of Contents

# Section 1: emagine Consulting A/S' (hereinafter referred to as "emagine") description of services supported by ProManagement

## Introduction

The purpose of this document is to inform emagine's Clients and auditors about emagine's controls and compliance measures implemented to secure general compliance of emagine's services with legislative requirements such as GDPR.

Furthermore, this document will outline specific security aspects related to the processing of data in the engagement between emagine and the customers, including a high-level description of how emagine's systems and processes support the rights of the registered individuals.

## Our Services

emagine services are all related to helping customers acquire IT and Business consultants according to the customer's specific requirements. Services are delivered directly in all the countries where emagine operates, except for nearshore services which are supplied out of our locations in Poland and offshore services in India.

In addition to these services focusing individual consultants, emagine delivers Managed Services to a number of customers in several custom-made service offerings.

Customers place a request with emagine to supply a number of consultant CV's eligible for the specific request, and after interviewing the relevant candidates' contracts between the customer and emagine as well as between emagine and the consultant are agreed and executed.

In direct support of the consultant deliveries, emagine will register the delivered hours, follow-up on quality and invoice the services rendered.

All of the above-mentioned services are supported by and registered in an internally developed ERP system named ProManagement (PM). For all process steps the required controls and implementation of the registered individuals' rights are supported by IT functionality.

General compliance with legislative requirements is reported and controlled by specific individuals appointed in the organization and audited by external professionals yearly.

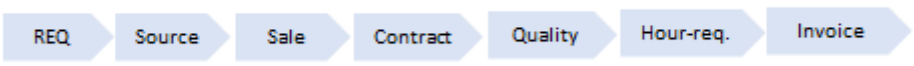
## GDPR – conditions for collection and processing personal data

### Purpose of processing

emagine stores and processes information relating to Freelance contractors and their professional career.

As defined and communicated in our privacy policies, emagine only store and process data with the sole purpose of providing the consultant with a new contract with one of our customers. The purpose of processing has been recorded in the record of processing (ROPA).

Given that this is the only purpose for which we process data and given that the data we process is not harvested in any way but entered individually by each consultant after the consultant's explicit approval of our terms and conditions for processing the data, emagine operates a very strict data processing chain:




The data provided by each registered individual may be refined by emagine's Sourcing team in order to produce a standardized consultant's profile that can be later on presented to the prospect Client and for a specific project. This happens always in cooperation with the consultant.

Given the fact that all data processed is stored and processed within one single system, PM, producing the DPIA (Data Processing Impact Assessment) is a matter of mapping data volumes to the processing activity and any related IT security measures implemented to protect and preserve the data being processed.

The ROPA (Register of Processing Activities) in fact constitutes a list of the above processing steps, the data involved, the departments involved in the processing and is held and maintained in the GDPR framework implemented in emagine.

## Legal Basis for processing personal data

Each of the processing steps in the emagine value chain regarding the registered individuals' personal data operates on the basis of the Art. 6 (1) b) GDPR – contractual necessity. For limited instances, the additional basis is Art. 9 (2) b) GDPR – legal obligation as authorised in Union or Member State law (for example, in case of processing criminal records), considering the sole main purpose of the data processing that is facilitating a new professional contract between individual freelance consultant and end Client. Documentation of the ROPA is held in the implemented GDPR framework, and relevant legal bases has been recorded in the record of processing.

Before registering in emagine's database, one is informed that registering involves a mandate for emagine to find clients requests that match one's profile (contractual necessity). Upon registration, the registered individuals have all been referred to and accepted the emagine Privacy Policy outlining the data processing performed in emagine. The acceptance of terms and conditions communicated to emagine through the sign-up process is stored and maintained for all registered individuals.

## Processing of the different categories of personal information

The registered individuals in emagine's systems only register personal information related to their professional careers, and the data is only processed in the internal emagine ERP system PM.

For a very limited number of individual consultants, emagine's customers require emagine to verify personal data relating to criminal convictions and offences, such us criminal records. If needed, this data is processed manually in an encrypted and Access Controlled file-share. emagine engages in such verification only if the Client is mandated by the law to check the candidate's criminal record before the final decision on engaging the pre-selected candidate in a project and awarding the contract. This applies, for example, to Clients from the banking industry. The data is processed only for verification purpose and is deleted immediately after such verification. emagine does not store such records, nor transfer it to the Clients.

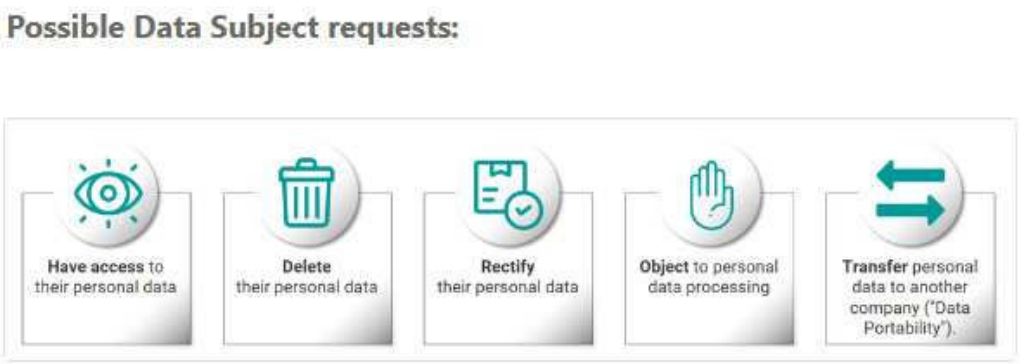
## The registered rights

The registered individuals' rights are preserved in the fact that all registered individuals may access, change, and control the processing of the data registered with emagine through our self-service portal: https://cv.it-consultant.com/.

Sourcing team main objective is to keep consultant data accurate and up to date. Automatic and manual deletion schemes are in place. Consultant may always contact Sourcing team with any question regarding his/her profile.

Additionally, we have the processes defined for handling data subject requests, and the registered individuals may send such request to a dedicated e-mail address published in our Privacy Policy available on our website.

Emagine's employees are aware how to react in case of data subject requests. Internal manual is available in our Intranet:




## General obligations as a controller

Contract with data processors

In general, emagine secures that all vendors and partners interacting with emagine and may potentially be processing or storing data has entered into a data processing agreement with emagine and/or holds external audit certifications to document their compliance. (ISO27001/ISAE3402)

The following processors are most relevant for processing of data stored in our system PM:

- DocuSign Inc.,
- HubSpot Inc.,
- Microsoft Inc.

Data processing agreements are continuously reviewed to ensure that they are up to date.

## Risk assessment

To ensure compliance with data protection regulation and in order to address potential risks to the rights and freedoms of data subjects, our internal ERP system PM have been built with the principle of privacy by design and default from the very beginning.

emagine continuously evaluates the appropriateness of the measures adopted to address the following main risks to the data subjects (candidates in our database and enrolled consultants):

- Risks stemming from unauthorized access, disclosure, or data breach, such as:
  - identity theft,
  - fraud or other type of financial loss,
  - inappropriate use of personal data (e.g., repurposing by other party after data breach).
- Risks stemming from inaccurate or incomplete personal data, such as:
  - incorrect or lack of assignment matches. i.e., loss of opportunity.
- Risks to the fairness principle, such as:
  - Lack of transparency about the use of personal data,
  - Difficulty in accessing or updating personal information,
  - Loss of control over personal information.

Apart from the “usual” mitigating measures adopted, such as encryption at rest and in transit, access controls (e.g., MFA when logging into PM), or staff manuals and training, the main principle of the structure of our ERP and our operations is to give as much control as possible to the data subject, starting from the moment of data collection and registration in the system, through enabling profile update and development, constant contact with the recruitment team, and establishing adequate retention schemes and automated deletion routines.

Similarly, the main risk factors have been assessed and addressed accordingly. The following risk factors have been found applicable to the processing activities in question:

- Processing personal data on a large scale (Risk level: 1),
    - this criterion being determined by the number of data subjects concerned (as a specific number and as a proportion of the relevant population), by the duration of the data processing activity and by the geographical extent of the processing activity,
- Matching or combining different sets of personal data (Risk level: 1)
- Processing highly personal data such as criminal convictions (Risk level: 1)
    - Important note: this happens in a very limited scope and without storing data, nevertheless, it needs to be counted as a risk factor.
- Evaluating data subjects (Risk level: 1).

On a risk scale 0-14 and taking into account the technical and organizational measures implemented and described further in this document, we estimate that risk to the data subjects is medium and properly addressed. emagine continues to monitor data protection risks and is committed to implementing new measures if there is any significant change to the processing activities, or a change in the interpretation of the law, acclaimed good practices or standards.

The ongoing monitoring and review of data subjects' risks, and adequacy of mitigation measures is assured and added to the Compliance yearly wheel.

## Data protection officer (DPO)

Our analysis indicates that emagine is not obliged to appoint a (Group) DPO under GDPR, since the premises of art. 37.1 GDPR are not fulfilled in our case. A local DPO has been appointed in Germany in accordance with local regulation (§ 38 Federal data Protection Act (BDSG)).

DPO's tasks and responsibilities have been assigned accordingly to the employees of emagine's Compliance and Legal departments. Technical and organizational measures have been implemented to ensure security, confidentiality, and integrity of candidates', consultants', and employees' data.

emagine regularly examines the need to designate a DPO and monitors data protection authorities' interpretations and local requirements.

## Transfer of personal information

As a rule, emagine does not transfer personal data outside the EU. Clients', consultants', and candidates' personal data is made available within the companies constituting emagine in the EU. Each Group entity is a joint data controller, and the legal basis for sharing the data within emagine is the legitimate interest (Article 6(1) f) of the GDPR).

## Compliance Obligations

emagine continuously develop Group compliance programme, and deploy the following standards which are regularly audited by external professionals:

- ISAE3000 GDPR
- ISAE3402 Operations
- ISO14001 (Poland, Denmark, Norway, in progress – the whole Group)
- ISO9001 (Poland, Denmark, Norway, in progress – the whole Group)
- ISO 27001 (currently Germany, France, UK, planned - certification of the whole Group)
- TISAX (Germany)

## Polices and processes in support of emagine's Information Security Management

### Information Security policies and operations:

emagine implemented the following written policy framework to govern compliance to the scope of the Information Security Management System implemented.

Policies in the framework:

- Information Security Policy
- Access Control Policy
- Physical Security Policy
- Internet Acceptable Use Policy
- Cloud Computing Policy
- Teleworking Policy
- Social Media Policy
- Security Breach Policy
- Security Incident and Event Management Policy

Procedures implemented to support the policy framework:

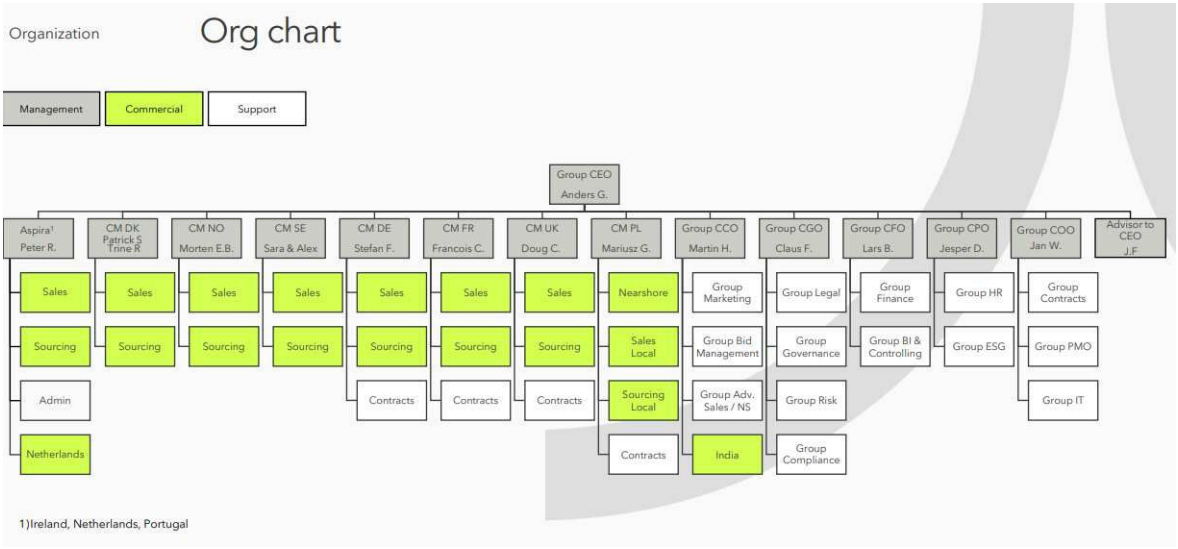
- Asset Handling Procedure
- Information Labelling Procedure
- Change Management Procedure

All policies and procedures are reviewed once a year and updated by the Compliance Team. Employees are obligated to report any procedural discrepancies to the management of emagine. The updated policy framework is approved by CEO.

## Organization of information security

### Internal Organization

To ensure consistency of the management of Information Security, IT security, and the inherited risk to Business Operations that rely on processing information assets, emagine implemented an organizational structure based on role segregation, clear accountability rules, governance of business development including IT change projects, and a sustainable and effective risk mitigating control environment.




The CEO is ultimately accountable for Information Security in emagine.

The COO role is responsible for management of Information Security in emagine. The COO is a member of the CxO group accountable for setting the directions and articulating targets for Business Development, Information and IT Security, and the day-to-day Business Operation. The CxO group meetings are set to discuss and decide on all principal questions regarding Information and IT security.

The COO and IT Director are accountable for the IT Operation, IT Security level, Change Advisory Board, and the IT teams. Representatives on the Change Advisory Board meetings are the business and IT change manager. Security events are logged on an ongoing basis and reported to the CxO group on the CxO group meetings.

All activities including daily work in emagine are based on written security policies, including the IT policy, with off-set in the ISO 27001 standard, and the Employee Handbook to govern Information Security. The COO will, based on risk assessment minimum once a year or as consequence of major change, review and if necessary, update all implemented security policies and procedures to ensure sustainable compliance to external obligations, legal requirements, and contracts.

It is the responsibility of the employee's daily manager to communicate the updated content of the policies that relates to the work to be carried out on department level, ensure that procedures are followed, and risk mitigation controls documented. It's also the responsibility of the individual employee to report to the management of emagine if policies and procedures are not followed. Employees must as part of the onboarding procedure to all levels of the organization be trained in information security.

*Information security roles and responsibilities*

We have a clearly defined organization structure (see above). All information security responsibilities are defined and allocated. Comprehensive descriptions of roles and responsibilities are in place regarding all major roles, starting from management through the operations and support functions. At the same time, we have processes to handle key staff dependencies.

*Segregation of duties*

Overlapping duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisations' assets.

*Teleworking*

emagine's employees have the possibility of remote work in specified cases. We have implemented Policy and supporting security measures to protect information accessed, processed, and stored at teleworking sites. The equipment allowed for teleworking usage has been defined. Portable devices are protected with logon and encryption. Virtual Private Network (VPN) must be used each time when connecting from remote site. Two-factor authentication is required when a connection comes from an unusual site.

## Human resource security

### Prior to employment

*Screening*

We have procedures in place governing recruitment of employees and collaboration with externals ensuring that we recruit the right candidate based on background and skills. We have descriptions of roles and responsibilities for employees and employee categories to ensure that all employees are aware of their responsibilities. When joining the company, all employees are reviewed, and a registration form is followed.

*Terms and conditions of employment*

General terms of employment, including confidentiality regarding internal and customer matters, are de- scribed in each employee's employment contract where terms of all areas of the employment, including termination and sanctions in case of potential security breaches, are laid down.

During employment

*Management responsibilities*

In connection with employment, the new employee signs a contract. The contract states that the employee must observe the current policies and procedures. Moreover, it is clearly defined as part of the contract material what the employee's responsibilities and role comprise.

*Disciplinary process*

General terms of employment, including confidentiality about customer relationships, are described in each employee's employment contract, in which matters relating to all aspects of the employment, including termination and penalties in case of security breaches, are specified.

*Termination or change of employment responsibilities.*

In the event of termination of employment, we have a thorough procedure which must be observed to ensure that the employees return all relevant assets, including portable media, etc. and to ensure that all employees' access to buildings, systems and data are revoked. The overall responsibility for securing the performance of all controls related to the termination process lies with the company's COO.

## Asset management

*Inventory of assets*

Managing the assets of emagine uniquely identifying software, servers, physical infrastructure, cloud solutions, and laptops is being done by having them inventoried and controlled in the configuration and by change management processes. The documentation is a core component in managing information security and is continuously updated and reviewed by the IT Department.

*Ownership of assets*

All production systems are hosted in Microsoft Azure. Central network devices, servers, peripherals, systems, and data are controlled by system administrators in emagine.

Asset protection and security is the accountability of the COO ensuring and overseeing clear ownership and classification of information asset.

*Acceptable use of assets*

Acceptable use of the assets is elaborated in the Employee Handbook as part of the onboarding procedure, and in our internal policies.

*Return of assets*

Offboarding procedure is in place and includes returning emagine's assets and revoking the provisioned role-based access rights to accommodation, systems, and information.

*Management of removable media*

emagine's internal IT department is accountable for secure configuration and maintenance of company's portable equipment, such as laptops, mobile phones and similar. Such protection is mandatory and includes necessary updates for media carrying data when new security measures are introduced.

*Disposal of media*

Reuse or disposal of all physical equipment carrying information assets erased or destroyed is enabled and handled only by the IT department. Hardware is destroyed by certified external company.

## Access Control

*Access control policy*

Access control is governed by the emagine's Access Control Policy and the IS-Policy, which outline the requirements for granting, modifying, and revoking access rights to our systems and data. The policies are reviewed at least once a year.

*Access to network and network services*

We have implemented process and controls to restrict access to our network, systems, and data to authorized individuals only.

*User registration and de-registration*

Users accounts are registered and unregistered in accordance with the formal procedure we have in place and implemented to enable assignment of access rights.

*User access provisions*

Access provisioning process has been established and is followed for each user. Based on our controls, it is the accountability of the business line manager to request provisioning and withdrawal of standard role-based access rights on behalf of the employee, with the target to limit access to information. The access is assigned and revoked by the IT team as requested by the business line manager, after IT team validation. All provisioning of access rights is segregated by duties.

*Management of privileged access rights*

Privileged access rights are granted in a restricted and controlled manner to the authorized personnel only. Such access is reviewed on a regular basis.

*Management of secret authentication information of users*

Initial password allocation and further requirements are controlled through emagine's Access Control Policy. As a rule, all personal logons are only known by the individual employee.

*Review of user access rights*

The review of access rights is done at least once a year and is the accountability of the business line manager.

*Removal or adjustment of access rights*

Access rights are removed and adjusted immediately upon user's termination of employment at emagine or upon change of the role and thus the needed adjustment of the access scope.

We have defined procedure for external party users to our information assets ("Just-in-time").

*User responsibilities*

*Use of secret authentication information*

All users must follow emagine's practices and password requirements as described in emagine's Access Control Policy. Users are required to keep their authentication information secret and are instructed never to share their passwords with anyone. Such requirements are also highlighted by regular information security trainings.

## Cryptography

*Policy on the use of cryptographic controls*

The use of cryptography in emagine is governed by the Encryption Policy and Cloud Computing Policy. It is the accountability of the COO to oversee and approve the cryptographical standard implemented. Information assets must be encrypted in transit and at rest. Connectivity communication to emagine is 256 Bit encrypted on a randomized set of proprietary Firewall ports in a VPN architecture. Where information is to be transferred over a public network such as the internet TLS encryption must be used. All databases are encrypted with a key stored in a 'safe box' solution.

## Physical and environmental security

*Physical security perimeter*

We have defined and used security perimeters to distinguish and appropriately protect areas where either sensitive or critical information can be stored. Our Physical Security Policy is applicable in this regard and for overall physical security on our premises.

*Physical entry control*

The physical building and access points are anti-theft protected with window and door locks, cameras, and access control mechanisms in two levels.

The first level of access control mechanism is the requirement of access key card and visitor registration including validation of identification artefact in the staffed reception area at the entrance to the building. The second level is applied at emagine's accommodation facilities entrance and consists of access key card, badge, and biometric control.

*Securing offices, rooms, and facilities*

Physical security of our offices, rooms and facilities has been designed and applied accordingly. PL Nearshoring Centre is subject to additional internal procedures (higher security level) due to the nature of the work, and there are additional access control systems installed compared to other emagine offices.

*Protection against external and environmental threats*

We have designed and applied physical protection against natural disasters, malicious attacks, or accidents.

Visitors are monitored by emagine's employee, and they are never left unattended, including 3rd party service suppliers.

Maintenance and support plans are in place for the building security facilities. Written procedures are in place for issuing access permission and withdrawal thereof. Fire detection alarms and enlightened escape routes are in place. Evacuation plans, test and service plans and procedures are updated and available. Physical and environmental security is the responsibility of the Facilities Office Managers.

*Equipment sitting and protection*

Physical infrastructure and local servers are protected in locked rooms inside the premises to limit the risks of environmental hazards such as heat, fire, smoke, water, dust and vibrations, and unauthorized access. Locked cabinets, for example for laptop storage, are available and in usage.

*Supporting utilities (security of supply)*

We have an uninterruptible power supply (UPS) secured and in use.

*Cabling security*

All cabling is secured in a manner that prevents unauthorized access or tampering. Access to cabling is limited to authorized personnel only. Cabling is regularly inspected to ensure that it remains secure and in good shape.

*Equipment maintenance*

All equipment is regularly maintained in line with manufacturer recommendations and company policies.

*Removal of assets*

Assets are only removed from the premises with the prior approval management. Asset removal is documented and recorded.

*Security of equipment and assets off-premises*

Security has been applied to off-site assets considering the different risks of working outside the organization's premises.

*Secure disposal or re-use of equipment*

All equipment is disposed of or re-used in a manner that is secure and complies with company policies and relevant legislation.

All items of equipment containing storage media are verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use.

*Clear desk and clear screen policy*

Computer screen lock is mandatory when computers are not in active use and attended by employees. Clear desk policy for paper files and removable storage media is enforced.

## Operations security

*Change management*

emagine has implemented a change management process to ensure that changes to our systems and infrastructure that might affect information security are made in a controlled manner.

Changes are made as agreed with emagine business areas and are properly planned according to the in-house conditions. Changes are only made based on a qualification of the project, the complexity and assessment of effects on other systems. Moreover, a process is followed regarding development and testing, as well as acceptance by the business stakeholders.

In case of fundamental changes to the underlying systems operating our environment, we always ensure as a minimum that:

- All changes are discussed, prioritized, and approved by management
- All major changes are tested
- All major changes are approved before deployment
- All major changes are deployed at a specific time as agreed with the business
- Fall-back planning is performed, ensuring that the changes can be rolled back or cancelled in case they fail to be operational

Our environment is logically segregated and divided into several environments whereby we ensure that deployed changes may be tested before deployed into production

*Capacity management*

We monitor and adjust the utilization of our systems and infrastructure to ensure that we have sufficient capacity to meet business demands. This includes performance monitoring, capacity planning and resource allocation to ensure that our systems can handle the expected workload.

*Control against malware*

We have implemented detection prevention and recovery controls to protect against malware. User awareness is kept up-to-date and raised via regular information security trainings.

*Event logging*

We maintain logs recording user activities exceptions, faults, and information security events. These logs are securely stored and monitored regularly.

*Protection of log information*

We take measures to protect logging facilities and log information from tampering an unauthorized access.

*Administrator and operator logs*

We maintain logs of system administrator and system operator activities to monitor and detect any potential misuse of privileges or unauthorized access. These logs are kept protected and reviewed.

*Clock synchronization*

Clock synchronization is an important aspect of operational security control. It ensures that all relevant systems and devices within the organization have accurate time stamps, which is critical for event logging, correlation, and investigation.

All relevant information processing system within our organization have been synchronised through the use of single reliable time source.

*Installation of software on operational systems*

We have procedures in place to monitor and control the installation of new and unauthorized software on operational systems.

*Management of technical vulnerabilities*

We are proactively identifying and addressing vulnerabilities in our systems and applications. This includes internal assessments and testing to identify potential weaknesses, prioritizing vulnerabilities based on risk and developing and implementing plans to remediate those vulnerabilities in a timely manner.

## Communications security

*Network security management*

A physical topology separating infrastructure networks has been implemented, and all logins to management network segments require 2 factor authentication. Production networks may only be accessed from specific IP-addresses under IT Security governance.

We have set up monitoring and logging of network traffic followed and managed by our operations department.

Granting remote VPN connection with Multi Factor Authentication system access follows the formal procedure of access provisioning, after whitelisting and contracting the specific services, including 3rd party vendors.

*Segregation of networks*

Groups of information services users and information systems are segregated on networks. Use of portable devices is segregated from internal network and all access is governed via VPN connections.

## Information security incident management

*Responsibilities and procedures*

We have established clear responsibilities and procedures for information security incident management to ensure a quick, effective, and orderly response to information security incidents. This includes defining roles and responsibilities for incident response team, as well as procedure for incident identification, assessment, and response.

We have defined a separate policy for security breaches involving personal data, so as to take appropriate steps that are proportionate to the data subjects' risks.

Technical measures are implemented to automatically detect and report any incidents, discrepancies, or deviations from normal operations of services. Designated members of the IT team monitor the potential threats on a regular basis. Moreover, all employees are obliged to report any potential incident, and they are informed about the channels they should use. This is especially the case for the incidents that cannot be detected by the technical and automated tools.

*Reporting information security events*

Information security incidents are being reported internally through designated channels as quickly as possible. Our data processors are obliged under the data processing agreements in place to report security events relevant to their processing in a timely manner allowing emagine as a data controller for evaluation and response, as well as reporting to the authorities if needed in due time.

*Reporting security weaknesses*

Employees and Clients using emagine's information systems and services are encouraged to inform the IT or Compliance team about any security weakness they may identify from their own observations. Such reports are assessed on CAB meetings and given priority if needed.

*Assessment of and decision on information security events*

Information security events are assessed, and it is decided if they are to be classified as information security incidents. This includes evaluating the potential impact of the incident and determining the root cause of the incident. Monitoring and assessment of events and potential information security breaches is processed in a weekly CAB meeting revisiting all events from the operations-log and securing RCA and mitigations are being implemented.

*Response to information security incidents*

Our Incident Response Team follows established procedures for responding to information incidents, including containing the incident to prevent further damage, collecting evidence, and restoring affected systems and data to a secure state. Should the operational staff determine a possible information security breach, the Information Security Incident response procedure will be initiated.

*Learning from information security incidents*

After an information security incident has been resolved, a post-incident review is conducted to identify any possible lesson learned and areas of improvement. Depending on the scale and impact of the incident, the post-review evaluates the effectiveness of incident response procedures, potential gaps in security controls and provides a suggestion whether an update of incident response procedure is needed.

## Information security aspects of business continuity management

*Planning information security continuity*

The needs and requirements for information security continuity in case of various adverse events, such as internet local power failure, internet failover, emergency re-location etc., have been evaluated and decided upon. The aim of our business continuity planning is to restore full operational status, i.e., the availability and integrity of core services, as quickly as possible, following any business activity interruption.

*Implementing information security continuity*

Data protection and Business continuity is implemented to meet a strategic target of recovering business functionality within 3 hours and with a potential data loss minimized to 15 min. Processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented, and maintained.

*Verify review and evaluate information security continuity*

We verify on a regular basis the established and implemented information security continuity controls to ensure that they are valid and effective during adverse situations.

## Changes during the period

Throughout the period of 1. March 2022 to 28. February 2023, we have undergone the following significant changes:

- Infrastructure topology was updated to M354 E5 Security and all communication protocols were updated to VPN and MFA protocols,
- The System platform PM was upgraded according to overall Roadmap releasing Request-Module, Sourcing-Module, and new Integrated CRM functionality.

# Section 2: emagine Consulting A/S' (hereinafter referred to as "emagine") statement

The accompanying description has been prepared for customers, who have used emagine's services supported by ProManagement, and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the customers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with.

emagine uses the following supplier and processor: Microsoft Inc. This statement does not include control objectives and related controls at emagine's suppliers and processors.

emagine confirms that:

a) The accompanying description, Section 1, fairly presents how emagine's services supported by ProManagement has been has processed personal data in accordance with the Regulation throughout the period from 1 March 2022 to 28 February 2023. The criteria used in making this statement were that the accompanying description:

   (i) Presents how emagine's processes and controls were designed and implemented, including:

   - The types of services provided, including the type of personal data processed
   - The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete, and restrict processing of personal data
   - The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality
   - The procedures supporting in the event of breach of personal data security that the data controller may report this to the supervisory authority and inform the data subjects
   - The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed
   - Controls that we, in reference to the scope of emagine's services supported by ProManagement are identified in the description
   - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data

   (ii) Includes relevant information about changes in the scope of emagine's services supported by ProManagement in the processing of personal data during the period from 1 March 2022 to 28 February 2023;

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

b) The controls related to the control objectives stated in the accompanying description were, in our view, suitably designed and operated effectively throughout the period from 1 March 2022 to 28 February 2023. The criteria used in making this statement were that:

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

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

   (iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 March 2022 to 28 February 2023.

c) Appropriate technical and organisational safeguards were established and maintained sound data processing practices and relevant requirements for data processing in accordance with the Regulation.

Copenhagen, 9 May 2023
emagine

Anders Gratte
CEO

# Section 3: Independent auditor's ISAE 3000 assurance report on compliance with the General Data Protection Regulation (GDPR)

To: emagine Consulting A/S (hereinafter referred to as "emagine") and their customers

## Scope

We were engaged to provide assurance about a) emagine's description, Section 1, of emagine's services supported by ProManagement in accordance with their compliance with the EU General Data Protection Regulation (GDPR) throughout the period from 01. March 2022 to 28. February 2023 and about b+c) the design and operating effectiveness of controls related to the control objectives stated in the Description. emagine uses the following suppliers and processors, Microsoft Inc. This statement does not include control objectives and related controls at emagine's suppliers and processors.

We express reasonable assurance in our conclusion.

## emagine's responsibilities

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

## Grant Thornton's independence and quality control

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

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

## Auditor's responsibilities

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

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

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

An assurance engagement to report on the Description, design, and operating effectiveness of controls at a data controller involves performing procedures to obtain evidence about the disclosures in the data controller's description of emagine's services supported by ProManagement and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data controller and described in Section 1.

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

## Limitations of controls at a data controller

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

## Opinion

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

(a) The Description fairly presents emagine's services supported by ProManagement as designed and implemented throughout the period from 1 March 2022 to 28 February 2023;

(b) The controls related to the control objectives stated in the Description were appropriately designed throughout the period from 1 March 2022 to 28 February 2023; and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period from 1 March 2022 to 28 February 2023.

## Description of tests of controls

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

## Intended users and purpose

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

Copenhagen, 9 May 2023

**Grant Thornton**
State Authorised Public Accountants

Kristian Randløv Lydolph
State Authorised Public Accountant

Basel Rimon Obari
Executive director, CISA, CISM

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

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

Our test of the functionality has included the control objectives and attached controls, selected by management and which are stated in the control objectives below. Our test has included the controls, we find necessary to establish reasonable assurance for compliance with the articles stated throughout the period from 1 March 2022 to 28 February 2023.

Our statement, does not apply to controls, performed at emagine's suppliers and processors.

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

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

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

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

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

Articles and points about main areas are written in bold.

| GDPR articles | ISO 27701 | ISO 27001/2 |
|---|---|---|
| **5, 26, 28, 29, 30, 32, 40, 41, 42, 48** | 8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2** | *New scope compared to ISO 27001/2* |
| **28, 29, 48** | 8.5.5, 6.15.2.2, **6.15.2.2** | 18.2.2 |
| **28** | **8.2.4, 6.15.2.2** | 18.2.2 |
| **31, 32, 35, 36** | **5.2.2** | 4.2 |
| **32, 35, 36** | **7.2.5, 5.4.1.2, 5.6.2** | 6.1.2, 5.1, 8.2 |
| **32** | **6.9.2.1** | **12.2.1** |
| **28 stk. 3; litra e, 32; stk. 1** | **6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3 | **13.1.2**, 13.1.3, 14.1.3, 14.2.1 |
| **32** | 6.6.1.2, 6.10.1.3 | 9.1.2, 13.1.3, 14.2.1 |
| **32** | **6.6** | 9.1.1, 9.2.5 |
| **32** | **6.9.4** | 12.4 |
| **32** | **6.15.1.5** | 18.1.5 |
| **32** | **6.9.4** | 12.4 |
| **32** | **6.11.3** | 14.3.1 |
| **32** | **6.9.6.1** | 12.6.1 |
| **28, 32** | **6.9.1.2, 8.4** | 12.1.2 |
| **32** | **6.6** | 9.1.1 |
| **32** | **7.4.9** | *New scope compared to ISO 27001/2* |
| **32** | **6.8** | 11.1.1-6 |
| **24** | **6.2** | 5.1.1, 5.1.2 |
| **32, 39** | **6.4.2.2, 6.15.2.1, 6.15.2.2** | 7.2.2, 18.2.1,18.2.2 |
| **39** | **6.4.1.1-2** | 7.1.1-2 |
| **28, 30, 32, 39** | **6.10.2.3**, 6.15.1.1, 6.4.1.2 | 7.1.2, 13.2.3 |
| **32** | **6.4.3.1, 6.8.2.5, 6.6.2.1** | 7.3.1, 11.2.5, 8.3.1 |
| **28, 38** | **6.4.3.1, 6.10.2.4** | 7,3.1, 13.2.4 |
| **32** | **5.5.3, 6.4.2.2** | 7.2.2, 7.3 |
| **38** | **6.3.1.1, 7.3.2** | 6.1.1 |
| **6, 8, 9, 10, 15, 17, 18, 21, 28, 30, 32, 44, 45, 46, 47, 48, 49** | 6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6 | *New scope compared to ISO 27001/2* |
| **6, 11, 13, 14, 32** | **7.4.5**, **7.4.7**, 7.4.4 | *New scope compared to ISO 27001/2* |
| **6, 11, 13, 14, 32** | **7.4.5**, **7.4.7**, 7.4.4 | *New scope compared to ISO 27001/2* |
| **13, 14** | **7.4.7**, 7.4.4 | *New scope compared to ISO 27001/2* |
| **13, 14, 28, 30** | **8.4.2, 7.4.7, 7.4.8** | *New scope compared to ISO 27001/2* |
| **13, 14, 28, 30** | **8.4.2, 7.4.7, 7.4.8** | *New scope compared to ISO 27001/2* |
| **6, 8, 9, 10, 17, 18, 22, 24, 25, 28, 32, 35, 40, 41, 42** | 5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7 | 15 |
| **28** | **8.5.7** | 15 |
| **28** | **8.5.8**, 8.5.7 | 15 |
| **33, 34** | **6.12.1.2** | 15 |
| **28** | **8.5.7** | 15 |
| **33, 34** | **6.12.2** | 15.2.1-2 |
| **15, 30, 44, 45, 46, 47, 48, 49** | **6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3 | 13.2.1, 13.2.2 |
| **15, 30, 44, 45, 46, 47, 48, 49** | **6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3 | 13.2.1 |
| **15, 30, 44, 45, 46, 47, 48, 49** | **6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3 | 13.2.1 |
| **12, 13, 14, 15, 20, 21** | **7.3.5, 7.3.8, 7.3.9** | *New scope compared to ISO 27001/2* |
| **12, 13, 14, 15, 20, 21** | **7.3.5, 7.3.8, 7.3.9** | *New scope compared to ISO 27001/2* |
| **33, 34** | **6.13.1.1** | 16.1.1-5 |
| **33, 34, 39** | 6.4.2.2, **6.13.1.5, 6.13.1.6** | 16.1.5-6 |
| **33, 34** | **6.13.1.4** | 16.1.5 |
| **33, 34** | **6.13.1.4,** 6.13.1.6 | 16.1.7 |

# ISO 27001/2

## A.5 Information security policies

### A.5.1 Management direction for information security

Control objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 5.1.1 | *Policies for information security*<br><br>A set of policies for information security is defined and approved by management, and then published and communicated to employees and relevant external parties. | We have inspected the information security policy and ensured that it contains relevant information.<br><br>We have inspected the risk assessment. | We have observed that the risk assessment does not take in the risk for the data subjects in mind.<br><br>No further deviations noted. |
| 5.1.2 | *Review of policies for information security*<br><br>The policies for information security are reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability adequacy and effectiveness. | We have inspected that the information security policy has been reviewed during the period.<br><br>We have inspected documentation that management has approved the risk evaluation | No deviations noted. |

# A.6 Organisation of information security

## A.6.1 Internal organisation
Control objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 6.1.1 | *Information security roles and responsibilities*<br>All information security responsibilities are defined and allocated. | We have inspected the organization chart.<br>We have inspected the guidelines for information security roles and responsibilities. | No deviations noted. |
| 6.1.2 | *Segregation of duties*<br>Confliction duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisations' *assets*. | We have inspected the organization chart.<br>We have inspected lists of employees, and ensured that the employees are divided according to functions and roles | No deviations noted. |

## A.6.2 Mobile devices and teleworking
Control objective: To ensure the security of teleworking and use of mobile devices

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 6.2.2 | *Teleworking*<br>Policy and supporting security measures are implemented to protect information accessed, processed, and stored at teleworking sites. | We have inspected documentation for the use of VPN. | No deviations noted. |

# A.7 Human resource security

## A.7.1 Prior to employment
Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 7.1.1 | *Screening*<br><br>Background verification checks on all candidates for employment is being carried out in accordance with relevant laws, regulations and ethics and are proportional to the business requirements, the classification of the information to be accessed and the perceived risks. | We have inquired into the procedure for employment of new employees and the security measures needed in the process.<br><br>We have, by sample test, inspected documentation for of screening new employees during the period. | We have been informed that for seven samples out of ten new employees, that documentation for screening has been deleted in accordance with the controller's retention scheme.<br><br>No further deviations noted. |
| 7.1.2 | *Terms and conditions of employment*<br><br>The contractual agreements with employees and contractors are stating their and the organisation's responsibilities for information security. | We have, by sample test, inspected a selection of contracts with employees and consultants in order to determine whether these are signed by the employees.<br><br>We have, by sample test, inspected that the onboarding process has been followed during the period. | No deviations noted. |

| A.7.2 During employment<br>Control objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 7.2.1 | *Management responsibility*<br>Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation. | We have inquired about procedure concerning establishing requirements for employees and partners.<br>We have inquired into whether management has required that employees observe the IT-security policy | No deviations noted. |
| 7.2.2 | *Information security awareness education and training*<br>All employees of the organisation and where relevant contractors, are receiving appropriate awareness education and training and regular updates in organisational policies and procedures as relevant for their job function. | We have inquired about procedures to secure adequate training and education (awareness training).<br>We have inspected documentation for activities developing and maintaining security awareness with employees. | No deviations noted. |
| 7.2.3 | *Disciplinary process*<br>There is a formal and communicated disciplinary process in place, to act against employees who have committed an information security breach. | We have inspected sanctioning guidelines and ensured that the employees can be sanctioned. | No deviations noted. |

| A.7.3 Termination and change of employment<br>Control objective: To protect the organisation's interests as part of the process of changing or terminating employment | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 7.3.1 | *Termination or change of employment responsibility*<br>Information security responsibilities and duties that remain valid after termination or change of employment have been defined, communicated to the employee or contractor, and enforced. | We have inquired about employees and contractors' obligation to maintain information security in connection with termination of employment.<br>We have, by sample test, ensured that confidentiality is enforced in regard to employees. | No deviations noted. |

## A.8 Asset management

### A.8.1 Responsibility for assets
Control objective: To identify organisational assets and define appropriate protection responsibilities

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 8.1.1 | *Inventory of assets*<br>Assets associated with information and information processing facilities have been identified and an inventory of these assets has been drawn up and maintained. | Vi have inspected records of assets and ensured that relevant assets have been identified. | No deviations noted. |
| 8.1.2 | *Ownership of assets*<br>Assets maintained in the inventory are being owned. | We have inspected record of asset ownership and ensured that relevant assets have an assigned owner. | No deviations noted. |
| 8.1.3 | *Acceptable use of assets*<br>Rules for the acceptable use of information and of assets associated with information and information processing facilities are being identified, documented, and implemented. | We have inquired about asset use guidelines, and we have inspected the guidelines. | No deviations noted. |
| 8.1.4 | *Return of assets*<br>All employees and external party users are returning all the organisational assets in their possession upon termination of their employment contract or agreement. | We have inquired into the procedure for securing the return of assets delivered, and we have inspected the procedure.<br>We have inspected the return of assets during the period, in order to ensure that the procedure has been followed. | No deviations noted.. |

| A.8.3 Media handling<br>Control objective: To prevent unauthorised disclosure, modification, removal, or destruction of information stored on media | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 8.3.1 | *Management of removable media*<br>Procedures have been implemented for the management of removable media in accordance with the classification scheme adopted by the organisation. | We have inspected the guidelines for removable media, and we have inspected documentation for the implementation. | We have been informed that there has been no removal of media in the period and therefore we have not been able to test the effectiveness of the company's procedures.<br>No deviations noted. |
| 8.3.2 | *Disposal of media*<br>Media are being disposed of securely when no longer required using formal procedures. | We have inquired about media disposal guidelines.<br>We have inquired about destroyed equipment during the period. | We have been informed that there has been no disposal of media in the period and therefore we have not been able to test the effectiveness of the company's procedures.<br>No deviations noted. |

# A.9 Access control

## A.9.1 Business requirements of access control
Control objective: To limit access to information and information processing facilities

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 9.1.1 | *Access control policy*<br>An access control policy has been established, documented, and reviewed based on business and information security requirements. | We have inquired into the policy of managing access control in order to establish whether it is updated and approved. | No deviations noted. |
| 9.1.2 | *Access to network and network services*<br>Users are only being provided with access to the network and network services that they have been specifically authorized to use. | We have inquired about managing access to networks and network services, and we have inspected the solution.<br>We have inspected list and users and inspected documentation for work-related need for access. | No deviations noted. |

| A.9.2 User access management<br>Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services. | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 9.2.1 | *User Registration and de-registration*<br>A formal user registration and de-registration process has been implemented to enable assignment of access rights. | We have inquired into the procedure for user registration and de-registration, and we have inspected the procedures.<br>We have, by sample test, inspected documentation for user registration and de-registration of users during the period. | No deviations noted. |
| 9.2.2 | *User access provisioning*<br>A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services | We have inspected the procedure for access control.<br>We have, by sample test, inspected documentation for user registration during the period. | No deviations noted. |
| 9.2.3 | *Management of privileged access rights*<br>The allocation and use of privileged access rights have been restricted and controlled. | We have inquired about procedures for allocation of user rights, use and limitation of privileged access rights.<br>We have inspected list of administrators for selected servers that process personal data. | No deviations noted. |
| 9.2.4 | *Management of secret-authentication information of users*<br>The allocation of secret authentication information is controlled through a formal management process. | We have, by sample test, inspected implementation of password requirements. | No deviations noted. |
| 9.2.5 | *Review of user access rights*<br>Asset owners are reviewing user's access rights at regular intervals | We have inquired into review of user access during the period. | We have observed that user review only includes review of a list of users, and it does not include review of logical accesses.<br>No further deviations noted. |

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 9.2.6 | *Removal or adjustment of access rights*<br><br>Access rights of all employees and external party users to information and information processing facilities are being removed upon termination of their employment contract or agreement or adjusted upon change. | We have inquired into procedures about discontinuation and adjustment of access rights.<br><br>We have, by sample test, inspected a list of resigned employees and we have inspected whether their access rights have been removed. | No deviations noted. |

| A.9.3 User responsibilities<br>Control objective: To make users accountable for safeguarding their authentication information | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 9.3.1 | *Use of secret authentication information*<br><br>Users are required to follow the organisations' s practices in the use of secret authentication information. | We have inspected the policy for passwords.<br><br>We have, by sample test, inspected password and by sample test ensured that it is implemented in accordance with the guidelines. | No deviations noted. |

## A.10 Cryptography

A.10.1 Cryptographic controls
Control objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 10.1.1 | *Policy on the use of cryptographic controls*<br>A policy for the use of cryptographic controls for protection of information has been developed and implemented. | We have, by sample test, inspected transmission over the internet, and by sample test ensured the transmission is secure. | We have observed that one out of three samples of transmissions over the internet use an expired certificate.<br>We have observed that two out of three samples of transmissions over the internet support a deprecated cryptographic protocol.<br>No further deviations noted. |

## A.11 Physical and environmental security

A.11.1 Secure areas
Control objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 11.1.1 | *Physical security perimeter*<br>Security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information. | We have inspected the policy for physical security.<br>We have inspected documentation for implementation of the policy. | No deviations noted. |
| 11.1.2 | *Physical entry control*<br>Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access. | We have inspected the policy for physical security.<br>We have inspected documentation for implementation of the policy.<br>We have inspected offices and ensured that access to offices is restricted. | No deviations noted. |

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 11.1.3 | *Securing offices, rooms, and facilities*<br>Physical security for offices rooms and facilities has been designed and applied. | We have inspected the policy for physical security.<br>We have inspected documentation for implementation of the policy. | No deviations noted. |
| 11.1.4 | *Protection against external and environmental threats*<br>Physical protection against natural disasters, malicious attack or accidents has been designed and applied. | We have inspected documentation for protection against external and environmental threats. | No deviations noted. |

| A.11.2 Equipment<br>Control objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 11.2.1 | *Equipment sitting and protection*<br>Equipment is sited and protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access. | We have inquired into the procedure concerning placement and protection of equipment.<br>We have inspected selected equipment. | No deviations noted. |
| 11.2.2 | *Supporting utilities (security of supply)*<br>Equipment is protected from power failures and other disruptions caused by failures in supporting utilities. | We have inspected documentation for test of UPS during the period. | No deviations noted. |
| 11.2.3 | *Cabling security*<br>Power and telecommunications cabling carrying data or supporting information services are being protected from interception | We have inspected the protection of selected power and telecommunications cabling in order to stablish whether the cables are protected from interception. | No deviations noted. |

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 11.2.4 | *Equipment maintenance*<br>Equipment is being correctly maintained to ensure its continued availability and integrity. | We have, by sample test, inspected service reports concerning maintenance of selected equipment, in order to determine whether the equipment has been maintained in compliance with the supplier's recommendations. | No deviations noted. |
| 11.2.5 | *Removal of assets*<br>Equipment information or software is not taken off-site without prior authorization. | We have inspected the policy for asset removal.<br>We have inquired about removal of equipment and assets. | We have been informed that there has been no removal of assets in the period and therefore we have not been able to test the effectiveness of the company's procedures.<br>No deviations noted. |
| 11.2.6 | *Security of equipment and assets off-premises*<br>Security has been applied to off-site assets considering the different risks of working outside the organisation's premises. | We have inspected the policy for acceptable use.<br>We have inquired about securing of equipment and assets outside the company's premises. | No deviations noted. |
| 11.2.7 | *Secure disposal or re-use of equipment*<br>All items of equipment containing storage media have been verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use. | We have inspected the procedure for secure disposal or re-use of equipment.<br>We have inquired about destroyed equipment during the period. | We have been informed that there has been no removal of media in the period and therefore we have not been able to test the effectiveness of the company's procedures.<br>No deviations noted. |
| 11.2.9 | *Clear desk and clear screen policy*<br>A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities has been adopted. | We have inquired into the policy of tidy desk and clear screen.<br>We have inspected documentation for enforced screen saver. | No deviations noted. |

# A.12 Operations security

## A.12.1 Operational procedures and responsibilities
Control objective: To ensure correct and secure operation of information processing facilities

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 12.1.2 | *Change management*<br>Changes to the organisation business processes information processing facilities and systems that affect information security have been controlled. | We have, by sample test, inspected changes during the period, and by sample test ensured that the procedure has been followed. | No deviations noted. |
| 12.1.3 | *Capacity management*<br>The use of resources is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained. | We have, by sample test, inspected capacity alerts. | No deviations noted. |

## A 12.2 Protection from malware
Control objective: To ensure that information and information processing facilities are protected against malware

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 12.2.1 | *Control against malware*<br>Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness. | We have., by sample test, inspected implementation of controls against malware. | No deviations noted. |

| A.12.4 Logging and monitoring<br>Control objective: To record events and generate evidence | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 12.4.1 | *Event logging*<br>Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed. | We have, by sample test, inspected servers and by sample test ensured that event logging has been implemented. | No deviations noted. |
| 12.4.2 | *Protection of log information*<br>Logging facilities and log information are being protected against tampering and unauthorized access. | We have, by sample test, inspected servers, and by sample test ensured that only administrators have access to logs. | No deviations noted. |
| 12.4.3 | *Administrator and operator logs*<br>System administrator and system operator activities have been logged and the logs are protected and regularly reviewed. | We have, by sample test, inspected servers, and by sample test ensured that administrator activity is logged. | No deviations noted. |
| 12.4.4 | *Clock synchronization*<br>The clocks of all relevant information processing systems within an organisation or security domain have been synchronised to a single reference time source. | We have, by sample test, inspected implementation of NTP. | No deviations noted. |

| A.12.5 Control of operational software<br>Control objective: To ensure the integrity of operational systems | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 12.5.1 | *Installation of software on operational systems*<br>Procedures are implemented to control the installation of software on operational systems. | We have, by sample test, inspected servers that processes personal data, and by sample test ensured that the servers are updated on a regular basis. | No deviations noted. |

| A.12.6 Technical vulnerability management<br>Control objective: To prevent exploitation of technical vulnerabilities | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 12.6.1 | *Management of technical vulnerabilities*<br>Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. | We have inspected vulnerability rapports during the period. | No deviations noted. |

## A.13 Communications security

### A.13.1 Network security management
Control objective: To ensure the protection of information in networks and its supporting information processing facilities

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 13.1.3 | *Segregation of networks*<br>Groups of information services users and information systems are segregated on networks. | We have, by sample test,, inspected network components and by sample test ensured that the network is separated. | No deviations noted. |

## A.15 Supplier relationships

### A.15.1 Information security in supplier relationships
Control objective: To ensure protection of the organisation's assets that are accessible by suppliers

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 15.1.1 | *Information security policy for supplier relationships*<br>Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets have been agreed with the supplier and documented. | We have inspected policies for supplier relations.<br>We have inspected a list of suppliers. | No deviations noted. |
| 15.1.2 | *Addressing security within supplier agreements*<br>All relevant information security requirements are established and agreed with each supplier that may access process store communicate or provide IT infrastructure components for the company's information. | We have inspected list of processors.<br>We have, by sample test, inspected data processor agreements. | No deviations noted. |

| 15.2 Supplier service delivery management<br>Control objective: To maintain an agreed level of information security and service delivery in line with supplier agreements | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 15.2.1 | *Monitoring and review of third-party services*<br>Organisations are regularly monitoring review and audit supplier service delivery. | We have inspected documentation for review of vendors during the period. | No deviations noted. |

# A.16 Information security incident management

| A.16.1 Management of information security incidents and improvements<br>Control objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 16.1.1 | *Responsibilities and procedures*<br>Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents. | We have inquired about the responsibilities and procedures of information security incidents, and we have inspected documentation for the distribution of responsibilities.<br>Further, we have inspected the procedure for handling information security incidents. | No deviations noted. |
| 16.1.2 | *Reporting information security events*<br>Information security events are being reported through appropriate management channels as quickly as possible. | We have inquired into guidelines for reporting information security events and weaknesses, and we have inspected the guidelines.<br>We have, by sample test, inspected that information security events have been responded to, in accordance with the documented procedures. | No deviations noted. |

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 16.1.3 | *Reporting security weaknesses*<br><br>Employees and contractors using the organisation's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services. | We have inspected the procedure for reporting incidents, and we have ensured that employees are required to report incidents. | No deviations noted. |
| 16.1.4 | *Assessment of and decision on information security events*<br><br>Information security events are assessed, and it is decided if they are to be classified as information security incidents. | We have, by sample test, inspected the ongoing control of incidents during the period. | No deviations noted. |
| 16.1.5 | *Response to information security incidents*<br><br>Information security incidents are responded to in accordance with the documented procedures. | We have inquired about information security incidents during the period. | We have been informed that there have not been any incidents during the period, and we have therefore not been able to test the effectiveness of the controllers' procedures.<br><br>No deviations noted. |
| 16.1.6 | *Learning from information security incidents*<br><br>Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents. | We have inquired about information security incidents during the period. | We have been informed that there have not been any incidents during the period, and we have therefore not been able to test the effectiveness of the controller's procedures.<br><br>No deviations noted. |

# A.17 Information security aspects of business continuity management

## A.17.1 Information security continuity
Control objective: Information security continuity should be embedded in the organisation's business continuity management systems

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 17.1.1 | *Planning information security continuity*<br><br>Requirements for information security and the continuity of information security management in adverse situations e.g., during a crisis or disaster has been decided upon. | We have inquired about the preparation of a contingency plan to ensure the continuation of operations in the event of crashes and the like, and we have inspected the plan. | No deviations noted. |
| 17.1.2 | *Implementing information security continuity*<br><br>Processes procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented, and maintained. | We have inquired about procedures to ensure that all relevant systems are included in the contingency plan, and we have inspected that the contingency plan is properly maintained. | No deviations noted. |
| 17.1.3 | *Verify review and evaluate information security continuity*<br><br>The established and implemented information security continuity controls are verified on a regular basis to ensure that they are valid and effective during adverse situations. | We have inquired about test of the BCP during the period. | We have observed that the BCP has not been tested during the period.<br><br>No further deviations noted. |

# A.18 Compliance

## A.18.2 Information security reviews
Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 18.2.1 | *Independent review of information security*<br><br>Processes and procedures for information security) (control objectives, controls, policies, processes, and procedures for information security) are reviewed independently at planned intervals or when significant changes occur. | We have observed that independent evaluation of information security has been established. | No deviations noted. |
| 18.2.2 | *Compliance with security policies and standards*<br><br>Managers are regularly reviewing the compliance of information processing and procedures within their area of responsibility with the appropriate security policies standards and any other security requirements. | We have inquired for internal controls to ensure compliance with security policies and procedures, and we have inspected selected controls.<br><br>We have, by sample test, inspected compliance meetings during the period. | No deviations noted. |

# ISO 27701 controls

| A.7.2 Conditions for collection and processing<br>Control objective: To determine and document that processing is lawful with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes. | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 7.2.1 | *Identify and document purpose*<br>Specific purpose of processing personal information is identified and documented. | We have inspected the record of processing and ensured that relevant processes and purposes has been identified. | No deviations noted. |
| 7.2.2 | *Identify lawful basis*<br>Lawful basis for processing personal data is identified, documented, and complies with relevant law. | We have inspected the record of processing and ensured that relevant legal basis for processing has been identified. | No deviations noted. |
| 7.2.6 | *Contract with data processors*<br>The organization has signed written agreements with data processors and appropriate requirements for processing of personal data are included. | We have, by sample test, inspected list of processors and by sample test inspected data processor agreements. | No deviations noted. |
| 7.2.8 | *Record related to processing personal data*<br>Records of processing are kept and maintained on an ongoing basis. | We have inspected the record of processing | No deviations noted. |

| A.7.3: Obligations to data subject<br>Control objective: To ensure that data subjects are provided with appropriate information about the processing of their personal data and to meet any other applicable obligations to data subjects related to the processing of their personal data. | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 7.3.1 | *Determining and fulfilling obligations to data subjects*<br>Legal, regulatory, and business obligations related to obligations to data subjects are determined and documented, to meet obligations in question. | We have inspected documentation that the controller has identified relevant obligations in regard to their data protection responsibilities. | No deviations noted. |
| 7.3.2 | *Determining information for data subjects*<br>Information regarding the processing of data subjects' personal data is determined and documented. | We have inspected privacy policies and ensured that they are available to data subjects. | No deviations noted. |
| 7.3.3 | *Providing information for data subjects*<br>Information regarding the processing of personal data is provided to the data subject in an intelligible and easily accessible way. | We have inspected privacy policies and verified that they contain relevant information. | We have observed that there is a difference between the stated retentions in regard to the processing of data in the privacy policies.<br>No further deviations noted. |
| 7.3.5 | *Providing procedure on how to object to the processing of personal data*<br>There is a procedure for data subjects, on how to object to the processing of personal data. | We have inquired about objection to processing requests during the period.<br>We have inquired about objections to processing during the period. | We have been informed that the controller has not received any insight requests during the period, and we have therefore not been able to test the effectiveness of the controllers' processes.<br>No deviations noted. |
| 7.3.6 | *Access, correction and/or erasure*<br>Data subjects' rights regarding access, correction and/or erasure of their personal data, follows documented policies, procedures and/or mechanisms | We have inspected the process for handling requests from data subject.<br>We have, by sample test, inspected requests from data subjects during the period, and by sample test ensured that requests have been handled according to the process. | No deviations noted. |

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 7.3.8 | *Providing copy of personal data processed*<br><br>When requested a copy of personal data is provided to the data subject. | We have inquired about data portability requests during the period. | We have been informed that the controller has not received any data portability requests during the period, and we have therefore not been able to test the effectiveness of the controllers' processes.<br><br>No deviations noted. |
| 7.3.9 | *Handling requests*<br><br>Policies and procedures for handling and responding to legitimate requests from data subjects are defined and documented. | We have inspected the process for handling requests from data subjects.<br><br>We have, by sample test, inspected the list of requests during the period, and by sample test ensured that the process has been followed. | No deviations noted. |

| A.7.4: Privacy by design and privacy by default<br>Control objective: To ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission, and disposal) are limited to what is necessary for the identified purpose. | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 7.4.1 | *Limited collection*<br><br>Collection of personal data is limited to what is relevant, proportional, and necessary for the identified purposes. | We have, by sample test, inspected collection of personal data and by sample test ensured that the collected personal data is proportional and necessary. | No deviations noted. |
| 7.4,2 | *Limited processing*<br><br>Processing of personal data is limited to what is adequate, relevant, and necessary for the identified purposes. | We have, by sample test, inspected processing of personal data and by sample test ensured that processed personal data is proportional and necessary. | No deviations noted. |
| 7.4.3 | *Accuracy and quality*<br><br>It is documented that personal data is accurate, complete, and up to date as necessary for the purposes for which it is processed. | We have, by sample test, inspected the record of processing and by sample test ensured that the personal data is accurate and up to date. | No deviations noted. |

| No. | emagine's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 7.4.4 | *Minimization objectives*<br><br>Data minimization objectives and mechanisms is defined and documented | We have inspected the record of processing and ensured that the controller only processes relevant personal data. | No deviations noted. |
| 7.4.5 | *Personal de-identification and deletion at the end of processing*<br><br>Personal data is either deleted or rendered in a form which does not permit identification or re-identification of data subject as soon as the original personal data is no longer necessary. | We have inspected the anonymization process once the processing of personal data has stopped | No deviations noted. |
| 7.4.7 | *Retention*<br><br>Personal data is not retained longer than what is necessary for the purposes for which it is processed. | We have inspected the record of processing and by sample test inspected that retention of personal data is in accordance with the record of processing. | No deviations noted. |
| 7.4.8 | *Disposal*<br><br>Disposal of personal data follows a documented policy, procedure and/or mechanism for disposal of personal data. | We have inspected the process for automatic deletion of personal data. | No deviations noted. |
| 7.4.9 | *Transmissions controls*<br><br>Controls are designed and implemented ensuring that Personal data transmitted over a data-transmission network reaches its intended destination. | We have, by sample test, inspected transmission over the internet. | We have observed that one out of three samples of transmissions over the internet use an expired certificate.<br><br>We have observed that two out of three samples of transmissions over the internet support a deprecated cryptographic protocol.<br><br>No further deviations noted. |

| A.7.5: Personal data sharing, transfer, and disclosure<br>Control objective: To ensure that personal data is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with relevant obligations | | | |
|---|---|---|---|
| **No.** | **emagine's control** | **Grant Thornton's test** | **Test results** |
| 7.5.1 | *Identify basis for personal data transfer between jurisdictions*<br>Relevant basis for transfer of personal data between jurisdictions is identified and documented. | We have inspected the record of processing and ensured that relevant legal basis for transfer between jurisdictions has been identified, | No deviations noted. |
| 7.5.2 | *Countries and international organizations to which personal data is transferred*<br>Countries and international organizations to which personal data can be transferred to, are identified, and documented. | We have inspected the record of processing and ensured that relevant legal basis for transfer to third countries has been identified, | No deviations noted. |
| 7.5.3 | *Records of transfer of personal data*<br>Transfer of personal data is recorded and cooperation with third parties regarding rights of data subject is ensured. | We have inspected the record of processing and ensured that transfer to relevant third countries are being addressed.<br>We have inspected documentation that the controller has signed relevant standard contractual clauses. | No deviations noted. |
| 7.5.4 | *Record of personal data disclosure to third parties*<br>Disclosure of personal data to third parties is recorded, including what personal data has been disclosed, to whom and at what time. | We have inspected the record of processing and ensured that personal data transferred to third countries are identified. | No deviations noted. |

# Section 5: Comments from the data controller

## emagine's comments to the deviation noted in 5.1.1:

Our assessment of the data subjects' risks has been included in the Statement of Applicability document, explaining our approach and roadmap planned in this regard. The Main risks to the data subjects and main risks factors are addressed in this assessment.

emagine have considered the risks to the data subjects' rights and freedom when designing and constructing the PM system. Accordingly, adequate controls and measures have been established as part of the technical design. It must be emphasised, that the PM system as a bespoke platform respects the principle of privacy by design/default in support of emagine overall compliance efforts.

In the current regulatory context, we are convinced that our implementation of privacy by design in addition to the ever-ongoing system control exercised by Compliance and IT Teams, has been adequate to ensure the risks identified for data subjects and uphold emagine data protection compliance.

To strengthen evidence of the continuous monitoring of data subjects' risks, we will register assessments of each detailed processing flow in our data protection management tool. These assessments will be reviewed on a yearly basis by the Compliance Team and confirmed on management level.

Additionally, emagine will conduct and register assessments of any major changes and new functionalities in the PM system as they may be decided.

PENNEO

*The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.*

*"By my signature I confirm all dates and content in this document."*

**ANDERS GRATTE**
**Underskriver 1**
*Serial number: 19740606xxxx*
*IP: 80.198.xxx.xxx*
*2023-05-09 12:17:23 UTC*

**Basel Rimon Obari**
**Underskriver 2**
*Serial number: 7a620960-cd2a-41f1-82f4-f2021d544570*
*IP: 188.179.xxx.xxx*
*2023-05-09 13:20:15 UTC*

**Kristian Lydolph**
**Underskriver 3**
*Serial number: CVR:34209936-RID:43340328*
*IP: 62.243.xxx.xxx*
*2023-05-09 13:44:08 UTC*