Assurance report

emagine Consulting A/S

Independent auditor's ISAE 3000 type 2 assurance report on information security and measures pursuant to emagine Consulting A/S' services supported by ProManagement in the role of data controller throughout the period from 1 March 2024 to 28 February 2025

May 2025

Grant Thornton | www.grantthornton.dk
Lautrupsgade 11, 2100 København Ø
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Table of contents

Section 1: emagine Consulting A/S' statement

The accompanying description has been prepared for data controllers, who has signed a data processing agreement with emagine Consulting A/S, and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with.

emagine Consulting A/S uses the following processors: Microsoft, DocuSign and Hubspot. This statement does not include control objectives and related controls at emagine Consulting A/S' processors. Certain control objectives in the description can only be achieved, if the processor's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by processors.

a) The accompanying description, Section 3, fairly presents how emagine Consulting A/S' services supported by ProManagement has processed personal data subject to the Regulation throughout the period from 1 March 2024 to 28 February 2025. The criteria used in making this statement were that the accompanying description:

   (i) Presents how emagine Consulting A/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 Consulting A/S' services supported by ProManagement have 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 emagine Consulting A/S' services supported by ProManagement during the period from 1 March 2024 to 28 February 2025;

   (iii) Does not omit or distort information relevant to the scope of emagine Consulting A/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 services supported by ProManagement that the individual customers 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 2024 to 28 February 2025 and if relevant controls with processors were operationally effective, assumed in the design of emagine Consulting A/S' controls during the period from 1 March 2024 to 28 February 2025. 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 individuals who have the appropriate competence and authority, throughout the period from 1 March 2024 to 28 February 2025.

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, 14 May 2025
emagine Consulting A/S

Anders Gratte
CEO

Section 2: Independent auditor's ISAE 3000 assurance report with reasonable assurance on information security and measures pursuant to emagine Consulting A/S' services supported by ProManagement in the role of data controller throughout the period from 1 March 2024 to 28 February 2025

To: emagine Consulting A/S and their customers

Scope

We were engaged to provide assurance about a) emagine Consulting A/S' description, Section 3 of emagine Consulting A/S' services supported by ProManagement in the role of data controller throughout the period from 1 March 2024 to 28 February 2025 and about b+c) the design and operational effectiveness of controls related to the control objectives stated in the Description.

emagine Consulting A/S uses the following processors, Microsoft, DocuSign and Hubspot. This statement does not include control objectives and related controls at emagine Consulting A/S' processors. Certain control objectives in the description can only be achieved if the processor's controls, assumed in the design of our controls, are appropriately designed, and operating effectively. The description does not include control activities performed by processor.

Our opinion is based on reasonable assurance.

emagine Consulting A/S' responsibilities

emagine Consulting A/S is responsible for: preparing the Description and the accompanying statement, Section 1, 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 for the design and implementation of operationally effective 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 applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain 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 Consulting A/S' Description and on the design and operational effectiveness of controls related to the control objectives stated in that Description, based on our procedures.

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

An assurance engagement to report on the Description, design, and operating effectiveness of controls at a data controller involves performing procedures to obtain evidence about the disclosures in the data controller's description of its emagine Consulting A/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 processor and described in Section 1.

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

Limitations of controls at a data controller

emagine Consulting A/S' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of emagine Consulting A/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 1. In our opinion, in all material respects:

(a) the description fairly presents how the IT general controls in relation to emagine Consulting A/S' services supported by ProManagement were designed and implemented throughout the period 1 March 2024 to 28 February 2025.

(b) the controls related to the control objectives stated in the description were suitably designed and implemented throughout the period 1 March 2024 to 28 February 2025 in all material respects, and

(c) the controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, operated effectively throughout the period from 1 March 2024 to 28 February 2025.

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 Consulting A/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, 14 May 2025

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Martin Brogaard Nielsen
Partner, CISA, CIPP/E, CRISC

Section 3: emagine Consulting A/S' description of processing activity for the services supported by ProManagement

Introduction

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

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

The description pertains emagine Consulting A/S' and subsidiaries' (collectively mentioned as 'emagine Group') in role of data controller and services supported by ProManagement (PM), throughout the period of from 1 March 2024 to 28 February 2025.

The following data controllers are within the scope of the description:

1. emagine Consulting A/S ('emagine DK'),
2. emagine Sp. z o.o ('emagine PL'),
3. emagine Consulting AB ('emagine SE'),
4. emagine AS ('emagine NO'),
5. emagine Consulting B.V. ('emagine NL'),
6. emagine Group SAS, emagine Consulting SARL and otherwise Portage SARL (collectively as 'emagine FR'),
7. emagine GmbH and emagine Flexwork GmbH (collectively as 'emagine DE'),
8. emagine Consulting Ltd. ('emagine UK'),
9. emagine Expertise Ltd. ('emagine IE')

Our Services

emagine Group's services are all related to helping clients acquire IT and business consultants according to the clients' specific requirements. Sectors with a strong presence include finance/banking, IT/telecom, energy, telecom, media, transport, and the public sector. Services are delivered directly in all the countries where emagine Group operates, as well as delivered through our Bestshore services which are supplied out of our locations in Poland, UAE, and India. Depending on the location of emagine's clients and supplied consultants, such Bestshore services can be further categorised as "Nearshore", "Offshore" or "Remote" consulting.

Clients place a request with emagine Group to supply a number of consultant profiles eligible for the specific request, and after interviewing the relevant candidates, contracts between the client and emagine Group, as well as between emagine Group and the consultant, are agreed and executed.

In direct support of the consultant deliveries, emagine registers the delivered hours, does a follow-up on quality, and invoices the services rendered.

In addition to these services focusing on offering individual consultants' expertise, emagine Group delivers Managed Services to several clients in various custom-made service offerings.

All 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 functionalities.

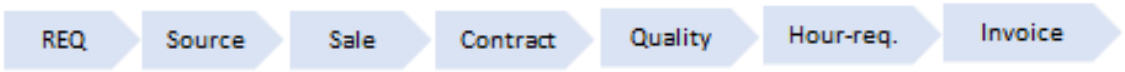
General compliance with legislative requirements is reported and controlled by appointed internal employees in emagine Group and audited by external professionals on a yearly basis.

GDPR – conditions for collection and processing of personal data

Purpose of processing
emagine Group stores and processes information related to freelance contractors and their professional career.

As defined and communicated in our privacy policy, emagine Group stores and processes personal data with the sole purpose of providing the consultant with a new contract with one of our clients. The purpose of processing has been recorded in the record of processing (ROPA).

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



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

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

The record of processing 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 Group.

Legal basis for processing of personal data

Each of the processing steps in the emagine Group's 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, the consultant is informed that registering involves a mandate for emagine to find clients' requests that match consultant's profile (which constitutes the contractual necessity). Upon registration, the consultants have all been referred to and confirmed the acknowledgement of emagine's privacy policy that outlines the rules for data processing in emagine Group. The acceptance of terms and conditions of our service happens also through the sign-up process and is stored for all registered consultants.

Processing of the different categories of personal information

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

For a very limited number of individual consultants, emagine Group's clients require emagine to verify personal data relating to criminal convictions and offences, such us criminal records. If needed, this data is verified 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.

Data Subjects' rights

The registered individuals' rights are preserved in the first place by the on-going possibility to access, change and control the processing of the data registered with emagine Group through our self-service portal: https://cv.it-consultant.com/ .

Sourcing Team's main objective is to keep consultant data accurate and up to date. Automatic and manual deletion schemes are in place. Consultants may always contact Sourcing Team with any question regarding his or 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 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 Group aims for all vendors interacting with emagine Group and may be processing personal data have entered into a data processing agreement with emagine, and that they guarantee an appropriate level of data security, preferably by holding external audit certifications to document their compliance.

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

- Microsoft Inc.
- DocuSign Inc.
- HubSpot 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 has 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 risks to the data subjects (candidates in our database and already enrolled consultants), such as, for example, risks stemming from unauthorised access, disclosure, or data breach, risks stemming from inaccurate or incomplete personal data, or risk of insufficient transparency.

Similarly, the main risk factors have been assessed and addressed accordingly.

On a risk scale 0-14 and taking into account the technical and organisational 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.

Transfer of personal data

Internal employees', clients', consultants', and candidates' personal data are made available within the companies constituting emagine Group. Each Group entity is a joint data controller.

emagine's main operations have so far concentrated in the EEA, therefore there have not been transfers of personal data outside the EEA. However, emagine Group has consistently grown, and new establishments in India (emagine Infotech Software Private Ltd. ['emagine IN']), and in the United Arab Emirates (Skillspark IT Consultancy L.L.C ['emagine UAE']), have been added and introduced to emagine's ERP system (PM).

emagine ensures the following security measures in this context:

- All Group companies are to co-sign standard contractual clauses (SCCs) – newly acquired legal entities are subsequently added to the SCC setup.
- Review procedures for third countries that become part of the SCC to determine whether the law or practice of the third country impairs the GDPR safeguards.
- Definition of the whole process of personal data inflow with descriptions of the categories of data, the purposes of their processing, as well as the information about technical and organisational security measures.
- Regularly updated privacy policy, informing individuals about the international transfer of their data and the safeguards in place.
- Safeguards to ensure an adequate level of safety while transferring personal data.
- Ensuring that rights of data subjects are observed, when data is being transferred outside the EEA, and provision of mechanisms for data subjects to exercise their rights.
- Group data protection responsible available to respond to any questions and requests.
- Platform where any irregularities can be anonymously reported (whistleblower).
- Regular monitoring of data transfers to ensure ongoing compliance with data protection requirements.
- Mechanisms to detect and respond to any breaches promptly (for example, security incidents reporting process).

When it comes to emagine's critical vendor, all servers and infrastructure are hosted with European Microsoft Azure datacentres – there is no data transfer outside the EEA in this regard.

Information security policies and operations

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

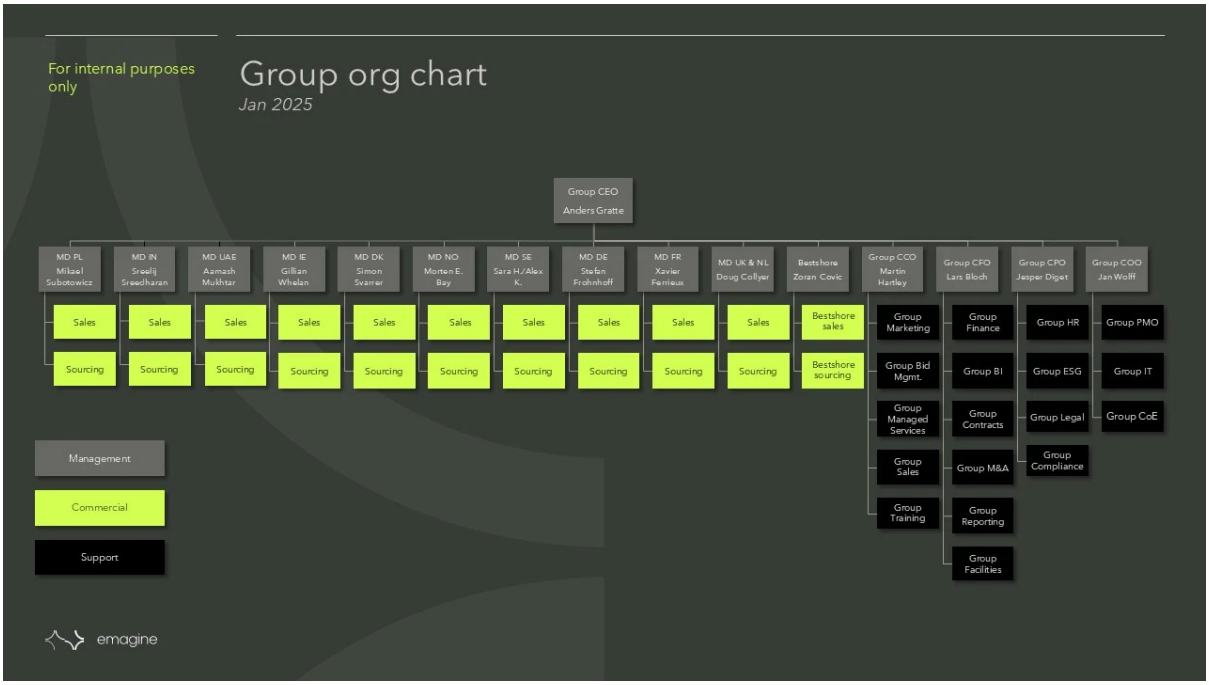
Most important policies & procedures in the ISMS framework:

- Information security policy
- Access control policy
- Backup policy
- Change management policy
- Control of documented information
- Development and acquisition policy
- Encryption policy
- Group business continuity plan
- Group data protection policy
- HR disciplinary policy
- Information classification policy
- Information security & data protection awareness policy
- Information security compliance policy
- Information security governance policy
- Internal controls and audit policy
- ISMS policy
- IT asset management security policy
- IT charter for emagine employees
- IT devices and operation procedures
- Logging policy

- Operations security policy
- Personal data breach policy
- Physical security policy
- Security incident and event management policy
- Social media policy
- Supplier management policy
- Teleworking policy
- Threat intelligence policy

Organisation of information security

Internal organisation
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 Group implemented an organisational 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 Group.

The COO role is responsible for management of Information Security in the Group. 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 Head of IT Security and Operations are accountable for the IT Operations, IT Security level, Change Advisory Board and the IT Support Team.

Security events are logged on an ongoing basis and reported on the CxO group meetings.

All activities including daily work in emagine Group are based on written security policies based on the ISO 27001:2022 standard. Additionally, the Employee Handbook governs and provides guidelines in information security aspects.

The Compliance Team in cooperation with Head of Security and Operations and COO will, based on risk assessment done by COO 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 Group if policies and procedures are not followed. Employees at all levels of the organisation must as part of the onboarding procedure be trained in information security. Additionally, all the IS policies, contacts, and educational materials are available to emagine's internal employees on the Intranet on a rolling basis.

Information security roles and responsibilities
We have a clearly defined organisation 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 unauthorised or unintentional modification or misuse of the organisations' assets.

Teleworking
emagine 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 external professionals applying for the internal roles, ensuring that we recruit the right candidate based on background and skills needed. We have descriptions of main roles and responsibilities for employees and employee categories to ensure that all employees are aware of their duties. When joining the company, all employees are interviewed in a HR-owned process, and a registration form is followed.

Terms and conditions of employment
General terms of employment, including confidentiality regarding internal and customer matters, are governed by each employee's employment contract. Terms of employment, such as termination and sanctions in case of potential security breaches are laid down either in the contract, or in the Work Regulations that constitute the part of the employment relationship by the virtue of the law. In all instances employees are regularly reminded of their confidentiality and data security obligations by compulsory trainings and internal communication.

During employment

Management responsibilities
In connection with employment, the new employee signs a contract. The contract or accompanying work regulations directly state 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
The disciplinary process within our organisation is outlined in the Group HR Disciplinary Policy with the possible necessary modifications stipulated in the local legislation, that are then reflected in employment agreements or local work regulations. All Employees are expected to comply with the organisation's information security policy and supporting policies. Information security policy details scenarios of possible data security infringements and associated disciplinary consequences.

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, 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 and CPO.

Asset management

Inventory of assets
Managing the assets of emagine Group's 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 Group'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 Group's access control policy which outlines the requirements for granting, modifying, and revoking access rights to our systems and data. The policy is 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 authorised 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 authorised personnel only.

Management of secret authentication information of users
Initial password allocation and further requirements are controlled through Group'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 the procedure for external party users to our information assets ("Just-in-time").

Use of secret authentication information
All users must follow emagine practices and password requirements as described in Group's Access Control Policy. Users are required to keep their authentication information secret and are instructed never to share their passwords with anyone.

Cryptography

Policy on the use of cryptographic controls
The use of cryptography in emagine is governed by the encryption policy. It is the accountability of the COO to oversee and approve the cryptographical standard implemented. Information assets must be encrypted both in transit and at rest. Connectivity communication to emagine Group is 256 Bit encrypted on a randomised 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 Azure Platform-managed keys (PMKs), and laptops are protected by BitLocker

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 outlines physical security measures on our premises.

Securing offices, rooms, and facilities
Physical security of our offices has been designed and applied accordingly. PL Warsaw office 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 Group offices.

Equipment sitting and protection
Physical infrastructure is protected in locked rooms inside the premises to limit the risks of environmental hazards such as heat, fire, smoke, water, dust and vibrations, and unauthorised access.

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.

Capacity management
We monitor and adjust the utilisation 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.

Event logging
We maintain logs recording user activities exceptions, faults, and information security events.

Protection of log information
We take measures to protect logging facilities and log information from tampering an unauthorised 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 unauthorised access..

Clock synchronisation
Logs are synchronised through the use of single reliable time source.

Installation of software on operational systems
We have procedures for patching software on operational systems.

Management of technical vulnerabilities
We have a procedure for identifying and addressing vulnerabilities in our systems and applications. This includes internal assessments and testing to identify potential weaknesses, prioritising vulnerabilities and implementing plans to remediate those vulnerabilities.

Communications security

Segregation of networks
Groups of information service 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 relocation 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 promptly and minimising potential data loss effectively. 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.

Compliance obligations

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

- ISAE3000 GDPR (DK – SE – NO – PL – FRA – UK – DE – NL – IE emagine entities)
- ISAE3402 Operations (emagine PL)
- ISO 27001 (DK – SE – NO – PL – FRA – UK – DE – NL – IE emagine entities)
- TISAX (emagine DE)
- ISO14001 (DK – SE – NO – PL – FRA – UK – DE – NL – IE emagine entities)
- ISO9001 (DK – SE – NO – PL – FRA – UK – DE – NL – IE emagine entities)
- ISO 45001 (DK – SE – NO – PL – FRA – UK – DE – NL – IE emagine entities)
- EcoVadis Platinum Medal

Changes during the audit period

Throughout the period from 1 March 2024 to 28 February 2025, we have undergone the following significant infrastructure changes:

- Digitalising advanced threat protection and vulnerability reporting in Azure
- Closing unsecure MFA Authentication methods (Mobile text/call)
- Moving all files from Fileshares into SharePoint
- Upgrading all devices to Windows 11

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 A-I below. Our test has included the controls; we find necessary to establish reasonable assurance for compliance with the articles stated throughout the period from 1 March 2024 to 28 February 2025.

Our statement, does not apply to controls, performed at emagine Consulting A/S' processors.

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

We performed our test of controls at emagine Consulting A/S by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at emagine Consulting A/S. The interviews have included questions about, how controls are performed.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals. The effectiveness of the controls during the audit period, is assessed by sample testing.
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 27001/2:2013
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 Consulting A/S' control	Grant Thornton's test	Test results
5.1.1	*Policies for information security* 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 contains relevant information. We have inspected that the risk assessment has identified risks relevant for the service. We have inspected that the information security policy is available for employees.	No deviations noted.
5.1.2	*Review of policies for information security* 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. We have inspected documentation that management has approved the risk assessment.	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 Consulting A/S' control	Grant Thornton's test	Test results
6.1.1	*Information security roles and responsibilities* All information security responsibilities are defined and allocated.	We have inspected that roles and responsibility for managing information security has been identified and that employees are required to follow them.	No deviations noted.
6.1.2	*Segregation of duties* Confliction duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisations' *assets*.	We have inspected documentation for that employees are segregated internally in accordance with their function.	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 Consulting A/S' control	Grant Thornton's test	Test results
6.2.2	*Teleworking* Policy and supporting security measures are implemented to protect information accessed, processed, and stored at teleworking sites.	We have inspected the teleworking policy and the procedure for IT devices and operation. We have inspected documentation that VPN is required to access the network. We have inspected use of MFA to access personal data.	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 Consulting A/S' control	Grant Thornton's test	Test results
7.1.1	*Screening* 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 inspected the procedure for employment of new employees and the security measures needed in the process. We have, by sample test, inspected documentation for of screening new employees during the period.	We have been informed that four (4) out of fourteen (14) samples of new employees, have not been tested with MPA and ACE in accordance with the Group Policy. We have been informed that three (3) out of fourteen (14) samples of new employees, have not been tested with ACE in accordance with the Group Policy. No further deviations noted.
7.1.2	*Terms and conditions of employment* 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 to determine whether these are signed by the employees. We have by sample test inspected that the onboarding process has been followed during the period	We have inspected that two (2) out of thirteen (13) samples of new employees, have not been informed about the organisation's requirements for information security in the contracts. No further deviations noted.

A.7.2 During employment Control objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities			
No.	**emagine Consulting A/S' control**	**Grant Thornton's test**	**Test results**
7.2.1	*Management responsibility* Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	We have inspected policies concerning establishing requirements for employees and partners.	No deviations noted
7.2.2	*Information security awareness education and training* 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 inspected documentation for activities developing and maintaining security awareness with relevant employees and consultants during the period.	No deviations noted
7.2.3	*Disciplinary process* 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 are communicated to the employees. We have, by sample test, inspected a selection of contracts with employees and consultants to determine whether these contain a provision of sanctions, in case employees fail to keep the organisation's policies and procedures.	We have inspected that one (1) out of thirteen (13) new employees, have not been informed about the organisation's requirements for sanctions in the contracts. No further deviations noted.

A.7.3 Termination and change of employment Control objective: To protect the organisation's interests as part of the process of changing or terminating employment			
No.	**emagine Consulting A/S' control**	**Grant Thornton's test**	**Test results**
7.3.1	*Termination or change of employment responsibility* 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. We have, by sample test, ensured that confidentiality agreements are enforced.	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 Consulting A/S' control**	**Grant Thornton's test**	**Test results**
8.1.1	*Inventory of assets* 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 that records of assets contain relevant assets in accordance with internal policy.	No deviations noted.
8.1.2	*Ownership of assets* Assets maintained in the inventory are being owned.	We have inspected that the record of asset ownership has an identified owner.	No deviations noted
8.1.3	*Acceptable use of assets* 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 inspected that there are guidelines for acceptable use of assets and that the guidelines are available to employees.	No deviations noted

No.	emagine Consulting A/S' control	Grant Thornton's test	Test results
8.1.4	*Return of assets* 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 inspected the procedure for securing the return of assets delivered. We have by sample inspected the return of assets during the period.	No deviations noted.

A.8.3 Media handling Control objective: To prevent unauthorised disclosure, modification, removal, or destruction of information stored on media			
No.	**emagine Consulting A/S' control**	**Grant Thornton's test**	**Test results**
8.3.1	*Management of removable media* 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 transportable media.	No deviations noted
8.3.2	*Disposal of media* Media are being disposed of securely when no longer required using formal procedures.	We have inspected the media disposal guidelines. We have inspected reports of disposed media in the audit period.	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 Consulting A/S' control	Grant Thornton's test	Test results
9.1.1	*Access control policy* An access control policy has been established, documented, and reviewed based on business and information security requirements.	We have inspected that the policy of managing access control is updated and approved	No deviations noted
9.1.2	*Access to network and network services* Users are only being provided with access to the network and network services that they have been specifically authorised to use.	We have inspected that the procedure for access management describes how to gain access to the network. We have, by sample test, inspected documentation for how users gain access to the network. We have, by sample test, inspected that users are identifiable in accordance with the procedure for accesses management.	No deviations noted

A.9.2 User access management Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services.			
No.	**emagine Consulting A/S' control**	**Grant Thornton's test**	**Test results**
9.2.1	*User Registration and de-registration* A formal user registration and de-registration process has been implemented to enable assignment of access rights.	We have inspected the procedure for user registration and de-registration. We have by sample inspected that granting and removal of access right has followed the procedure.	We have inspected that the policy for de-registration of user access have not been followed for 2 out of 19 samples of terminated employees during the period as access was withdrawn after the last working day. No further deviations noted.
9.2.2	*User access provisioning* 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 inquired about changes in user registrations during the period. We have, by sample test, inspected that granting of access right has followed the procedure. We have inquired about changes in user access rights during the period.	We have been informed that there have been no changes in access rights for employees during the period. No deviations noted.
9.2.3	*Management of privileged access rights* The allocation and use of privileged access rights have been restricted and controlled.	We have inspected procedures for allocation of user rights, use and limitation of privileged access rights. We have inspected list of administrators for selected servers that process personal data. We have inspected documentation for yearly control of privileged users with access to personal data.	Results of the annual control of privileged users with access to personal data, have not been logged. No further deviations noted.
9.2.4	*Management of secret-authentication information of users* The allocation of secret authentication information is controlled through a formal management process.	We have inspected the password policy. We have, by sample test, inspected the process for handing out passwords to users.	No deviations noted.
9.2.5	*Review of user access rights* Asset owners are reviewing user's access rights at regular intervals	We have inspected the control for access review. We have inspected documentation that review of access has followed the procedure.	Results of the annual control of users with access to personal data, have not been logged. No further deviations noted.

No.	emagine Consulting A/S' control	Grant Thornton's test	Test results
9.2.6	*Removal or adjustment of access rights* 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 inspected procedures about discontinuation and adjustment of access rights. We have, by sample test, inspected that terminated employees have had their access rights removed	For two (2) out of nineteen (19) samples of terminated employees, we have inspected that access was withdrawn after the last working day. No further deviations noted

A.9.3 User responsibilities Control objective: To make users accountable for safeguarding their authentication information			
No.	**emagine Consulting A/S' control**	**Grant Thornton's test**	**Test results**
9.3.1	*Use of secret authentication information* Users are required to follow the organisations' s practices in the use of secret authentication information.	We have inspected the policy for passwords. We have inspected that the password policy 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 Consulting A/S' control**	**Grant Thornton's test**	**Test results**
10.1.1	*Policy on the use of cryptographic controls* A policy for the use of cryptographic controls for protection of information has been developed and implemented.	We have inspected that the policy for encryption has been updated during the period. We have, by sample test, inspected that transmission via the internet follows the internal policy.	Two (2) out of eleven (11) samples have an incomplete certificate chain. We have observed that this has been corrected. 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 Consulting A/S' control	Grant Thornton's test	Test results
11.1.1	*Physical security perimeter* Security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information.	We have inspected that physical requirements have been identified in the policy for physical security.	No deviations noted.
11.1.2	*Physical entry control* Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	We have inspected that the physical security in office buildings follows the internal policy for physical security.	No deviations noted.
11.1.3	*Securing offices, rooms, and facilities* Physical security for offices rooms and facilities has been designed and applied.	We have inspected that the physical security in office buildings follows the internal policy for physical security.	No deviations noted.

A.11.2 Equipment
Control objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations

No.	emagine Consulting A/S' control	Grant Thornton's test	Test results
11.2.1	*Equipment sitting and protection* Equipment is sited and protected to reduce the risks from environmental threats and hazards and opportunities for unauthorised access.	We have, by sample test, inspected that unattended equipment in office location follows the internal policy.	No deviations noted.
11.2.9	*Clear desk and clear screen policy* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities has been adopted.	We have inspected the policy of tidy desk and clear screen. We have inspected documentation for mandatory 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 Consulting A/S' control	Grant Thornton's test	Test results
12.1.2	*Change management* Changes to the organisation business processes information processing facilities and systems that affect information security have been controlled.	We have inspected the procedure for changes. We have, by sample test, inspected changes during the period.	The procedure has not been followed in eight (8) out of thirty-six (36) samples of changes during the period. No further deviations noted.
12.1.3	*Capacity management* 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 inspected that capacity alarms have been established.	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 Consulting A/S' control	Grant Thornton's test	Test results
12.2.1	*Control against malware* 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 on servers and endpoints.	No deviations noted

A.12.4 Logging and monitoring Control objective: To record events and generate evidence			
No.	**emagine Consulting A/S' control**	**Grant Thornton's test**	**Test results**
12.4.1	*Event logging* Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed.	We have, by sample test, inspected that servers and databases have event logging of users and events in accordance with internal policy.	No deviations noted.
12.4.2	*Protection of log information* Logging facilities and log information are being protected against tampering and unauthorised access.	We have, by sample test, inspected that logs are protected in accordance with internal policy.	No deviations noted.
12.4.3	*Administrator and operator logs* System administrator and system operator activities have been logged, and the logs are protected and regularly reviewed.	We have, by sample test, inspected documentation for that administrators are logged.	No deviations noted
12.4.4	*Clock synchronisation* 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 Control objective: To ensure the integrity of operational systems			
No.	**emagine Consulting A/S' control**	**Grant Thornton's test**	**Test results**
12.5.1	*Installation of software on operational systems* Procedures are implemented to control the installation of software on operational systems.	We have inspected documentation that patching follows the procedure for patching during the period. We have, by sample test, inspected that patching has followed the procedure.	The procedure has not been followed for eight (8) out of thirty-six (36) samples of changes during the period. No further deviations noted.

A.12.6 Technical vulnerability management Control objective: To prevent exploitation of technical vulnerabilities			
No.	**emagine Consulting A/S' control**	**Grant Thornton's test**	**Test results**
12.6.1	*Management of technical vulnerabilities* 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 that vulnerability scanners have been implemented for the period. We have inspected remediation actions have been carried out 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 Consulting A/S' control	Grant Thornton's test	Test results
13.1.3	*Segregation of networks* Groups of information services users and information systems are segregated on networks.	We have inspected that servers and databases are segregated.	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 Consulting A/S' control	Grant Thornton's test	Test results
15.1.1	*Information security policy for supplier relationships* 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 that policies for supplier relations contain requirements for information security. We have inspected a list of suppliers.	No deviations noted
15.1.2	*Addressing security within supplier agreements* 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 that relevant vendors have been risk assessed. We have inspected that supplier agreements contain relevant requirements for information security.	No deviations noted

15.2 Supplier service delivery management
Control objective: To maintain an agreed level of information security and service delivery in line with supplier agreements

No.	emagine Consulting A/S' control	Grant Thornton's test	Test results
15.2.1	*Monitoring and review of third-party services* 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
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 Consulting A/S' control	Grant Thornton's test	Test results
16.1.1	*Responsibilities and procedures* Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents.	We have inspected that the procedure for handling incidents has distribution of responsibilities. We have inspected that the procedure has been maintained.	No deviations noted.
16.1.2	*Reporting information security events* Information security events are being reported through appropriate management channels as quickly as possible.	We have inspected that the procedure for handling incidents describes reporting of security events. We have, by sample test, inspected that the log of incidents have the required information about incidents.	No deviations noted.
16.1.3	*Reporting security weaknesses* 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 that the procedure for handling incidents describes reporting of vulnerabilities. We have inspected the log of incidents. We have inquired about information security weaknesses during the period.	We have been informed that there have been no information security weaknesses. No deviations noted.
16.1.4	*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.	We have inspected the log of incidents. We have inquired about information security breaches for ProManagement.	We have inspected that seven (7) out of thirteen (13) relevant incidents do not have Severity Level indicated. We have been informed that there have been no information security breaches related to ProManagement. No further deviations noted.

No.	emagine Consulting A/S' control	Grant Thornton's test	Test results
16.1.5	*Response to information security incidents* Information security incidents are responded to in accordance with the documented procedures.	We have inquired about information security breaches for ProManagement.	We have been informed that there have been no information security breaches related to ProManagement. No deviations noted.
16.1.6	*Learning from information security incidents* Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents.	We have inspected that the procedure for handling information security breaches describes remedies for preventing information security breaches.	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 Consulting A/S' control**	**Grant Thornton's test**	**Test results**
17.1.1	*Planning information security continuity* 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 inspected that the contingency plan to ensure the continuation of operations, contains relevant systems and plans.	No deviations noted.
17.1.2	*Implementing information security continuity* 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 inspected that all relevant systems are included in the contingency plan. We have inspected that the contingency plan is properly maintained.	No deviations noted.

No.	emagine Consulting A/S' control	Grant Thornton's test	Test results
17.1.3	*Verify review and evaluate information security continuity* 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 inspected that the contingency plan to ensure the continuation of operations contains relevant systems and plans. We have inspected documentation that the plan has been tested during the period.	No 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 Consulting A/S' control	Grant Thornton's test	Test results
18.2.1	*Independent review of information security* 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 inspected, that independent evaluation of information security has been established.	No deviations noted.
18.2.2	*Compliance with security policies and standards* 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 inspected that internal compliance has been tested during the period.	No deviations noted.

ISO 27701 controls

A.7.2 Conditions for collection and processing 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 Consulting A/S' control**	**Grant Thornton's test**	**Test results**
7.2.1	*Identify and document purpose* Specific purpose of processing personal information is identified and documented.	We have inspected that the record of processing has relevant processes identified. We have inspected that the record of processing has been updated and approved.	No deviations noted.
7.2.2	*Identify lawful basis* Lawful basis for processing personal data is identified, documented, and complies with relevant law.	We have inspected that the record of processing has relevant legal basis for processing identified.	No deviations noted.
7.2.6	*Contract with data processors* The organisation has signed written agreements with data processors and appropriate requirements for processing of personal data are included.	We have inspected that the controller has signed data processing agreements with relevant processors.	No deviations noted.
7.2.8	*Record related to processing personal data* Records of processing are kept and maintained on an ongoing basis.	We have inspected that the record of processing has identified relevant purposes for processing.	No deviations noted.

A.7.3: Obligations to data subject 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 Consulting A/S' control**	**Grant Thornton's test**	**Test results**
7.3.1	*Determining and fulfilling obligations to data subjects* Legal, regulatory, and business obligations related to obligations to data subjects are determined and documented, to meet obligations in question.	We have inspected that the record of processing and privacy policies has identified relevant data subjects.	No deviations noted.
7.3.2	*Determining information for data subjects* Information regarding the processing of data subjects' personal data is determined and documented.	We have inspected that privacy policies are available to data subjects.	No deviations noted.
7.3.3	*Providing information for data subjects* 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 ensured that they are available to data subjects.	We have inspected that not all relevant retention periods are stated in the privacy policy. No further deviations noted.
7.3.5	*Providing procedure on how to object to the processing of personal data* There is a procedure for data subjects, on how to object to the processing of personal data.	We have inspected that there are procedure for handling objection requests from data subjects. We have inquired about objection requests during the period.	We have been informed that there has been no objection request during the period. No deviations noted.
7.3.6	*Access, correction and/or erasure* Data subjects' rights regarding access, correction and/or erasure of their personal data, follows documented policies, procedures and/or mechanisms	We have inspected that there are procedures for insight, correction and deletion of personal data requests. We have, by sample test, inspected that requests have followed the procedure.	No deviations noted.

No.	emagine Consulting A/S' control	Grant Thornton's test	Test results
7.3.8	*Providing copy of personal data processed* When requested a copy of personal data is provided to the data subject.	We have inspected procedures for handling data portability requests. We have inquired about data portability requests during the period.	We have been informed that there has been no request for data portability during the period. No deviations noted.
7.3.9	*Handling requests* Policies and procedures for handling and responding to legitimate requests from data subjects are defined and documented.	We have inspected the procedure for handling requests from data subjects. We have, by sample test, inspected that requests have been handled during the period.	No deviations noted.

A.7.4: Privacy by design and privacy by default 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 Consulting A/S' control**	**Grant Thornton's test**	**Test results**
7.4.1	*Limited collection* Collection of personal data is limited to what is relevant, proportional, and necessary for the identified purposes.	We have inspected that processed data are in accordance with the record of processing and is limited and proportional to what is needed.	No deviations noted
7.4,2	*Limited processing* Processing of personal data is limited to what is adequate, relevant, and necessary for the identified purposes.	We have inspected that processed data are in accordance with the record of processing and is limited and proportional to what is needed.	No deviations noted
7.4.3	*Accuracy and quality* 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 inspected that processed data are in accordance with the record of processing and is limited and proportional to what is needed.	No deviations noted

No.	emagine Consulting A/S' control	Grant Thornton's test	Test results
7.4.4	*Minimisation objectives* Data minimisation objectives and mechanisms is defined and documented	We have inspected that the internal policy for data protection and privacy policy contains requirements about the categories of personal data that is relevant for the processing. We have, by sample test, inspected that production data are not used in development/tests.	No deviations noted
7.4.5	*Personal de-identification and deletion at the end of processing* 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 that the record of processing contains relevant retention schemes. We have inspected documentation for implementation of the retention periods.	No deviations noted
7.4.7	*Retention* *Personal data is not retained longer than what is necessary for the purposes for which it is processed.*	We have inspected that the record of processing contains relevant retention schemes. We have, by sample test, inspected documentation for implementation of the retention periods.	No deviations noted
7.4.8	*Disposal* Disposal of personal data follows a documented policy, procedure and/or mechanism for disposal of personal data.	We have inspected that the data protection policy contains instructions about removal of personal data when it is no longer needed. We have inspected the process for automatic deletion of personal data.	No deviations noted
7.4.9	*Transmissions controls* Controls are designed and implemented ensuring that Personal data transmitted over a data-transmission network reaches its intended destination.	We have inspected that the policy for encryption has been updated during the period. We have inspected that transmission over the internet follow the internal policy.	Two (2) out of eleven (11) samples have an incomplete certificate chain. No further deviations noted.

A.7.5: Personal data sharing, transfer, and disclosure 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 Consulting A/S' control**	**Grant Thornton's test**	**Test results**
7.5.1	*Identify basis for personal data transfer between jurisdictions* Relevant basis for transfer of personal data between jurisdictions is identified and documented.	We have inspected that the record of processing contains relevant transfer of personal data to third countries.	No deviations noted
7.5.2	*Countries and international organisations to which personal data is transferred* Countries and international organisations to which personal data can be transferred to, are identified, and documented.	We have inspected that the record of processing and privacy policies references legal basis for transfer.	The legal basis for transfer of personal data that is described in the record of processing and privacy policy does not match. Transfers to India and UAE do not appear in the record of processing. No further deviations noted.
7.5.3	*Records of transfer of personal data* 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 addressed. 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* 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 we have ensured that personal data transferred to third countries are identified.	No deviations noted

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 Fredrik Gratte
Underskriver 1
Serial number: f37555ae-8ab8-4fb9-bfb4-4a1612b5332c
IP: 87.49.xxx.xxx
2025-05-14 14:21:53 UTC

Mit ID

Martin Brogaard Borup Nielsen
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serial number: 658bcd61-1988-4367-b3eb-215cfbbb49b0
IP: 62.243.xxx.xxx
2025-05-14 14:24:27 UTC

Mit ID

Kristian Randløv Lydolph
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 3
On behalf of: Kristian Randløv Lydolph
Serial number: 84758c07-82ce-4650-a48d-5224b246b5c4
IP: 62.243.xxx.xxx
2025-05-14 15:53:50 UTC

Mit ID