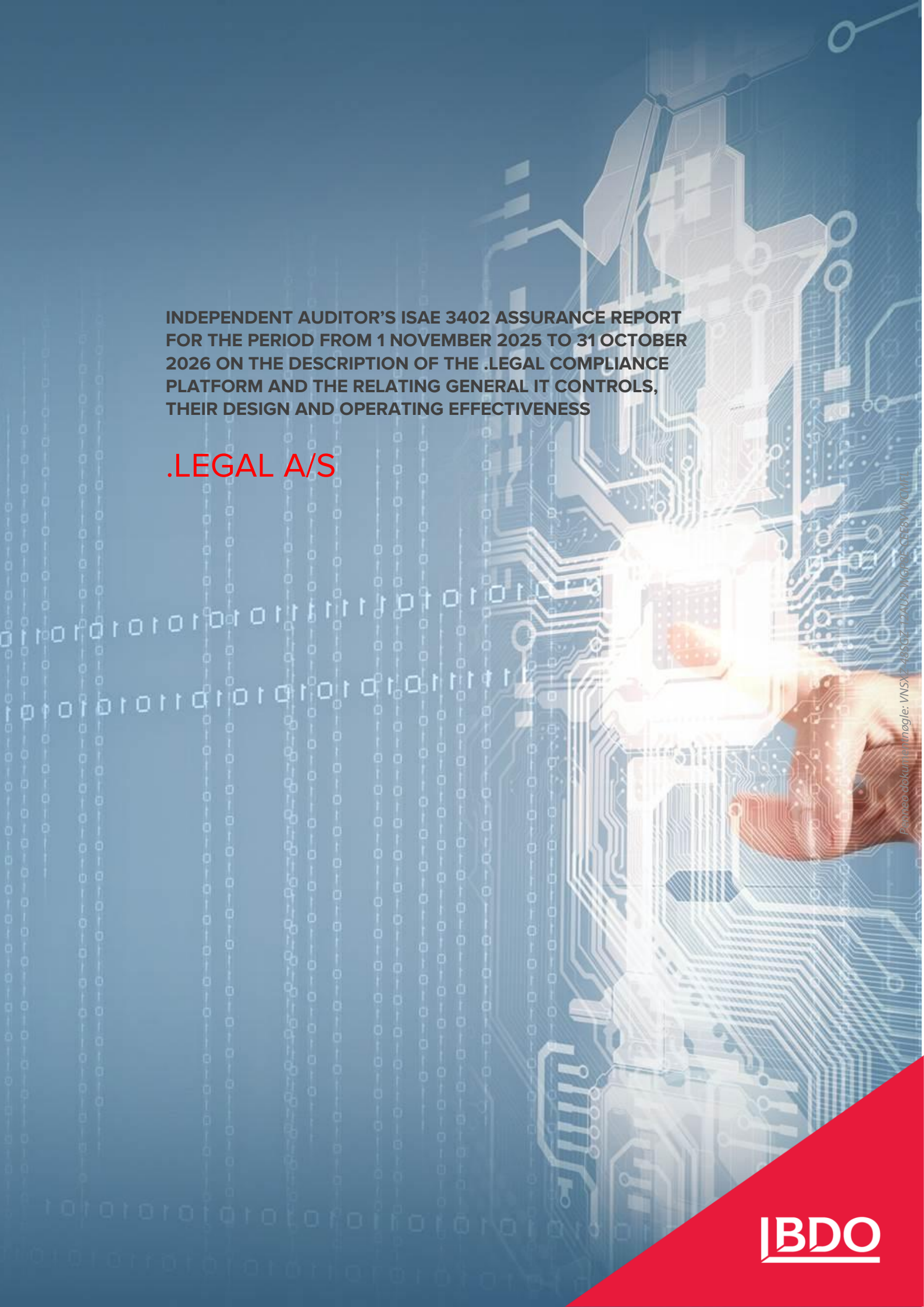
INDEPENDENT AUDITOR'S ISAE 3402 ASSURANCE REPORT FOR THE PERIOD FROM 1 NOVEMBER 2025 TO 31 OCTOBER 2026 ON THE DESCRIPTION OF THE .LEGAL COMPLIANCE PLATFORM AND THE RELATING GENERAL IT CONTROLS, THEIR DESIGN AND OPERATING EFFECTIVENESS

.LEGAL A/S



Penneo dokumentnøgle: VNSX2-48SGZ-1PA02-WGP2E-CEE8V-WCMT

BDO

CONTENTS

1. AUDITOR'S REPORT 2

2. .LEGAL A/S' STATEMENT 4

3. .LEGAL A/S' DESCRIPTON OF THE .LEGAL COMPLIANCE PLATFORM 6

.legal A/S' description of control environment 6

4. CONTROL OBJECTIVES, CONTROLS, TEST AND RESULTS OF TESTS 14

A.4: Risk assessment 16

A.5 Information security policies 17

A.6 Organisation of information security 18

A.7 Human resource security 19

A.8 Asset management 21

A.9 Access management 22

A.10 Cryptography 26

A.11 Physical and environmental security 27

A.12 Operations security 28

A.13 Communications security 32

A.14 System acquisition, development, and maintenance of systems 34

A.15 Supplier relationship 37

A.16 Information security incident management 39

A.18 Compliance 41

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

1. AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT FOR THE PERIOD FROM 1 NOVEMBER 2025 TO 31 OCTOBER 2026 ON THE DESCRIPTION OF THE .LEGAL COMPLIANCE PLATFORM AND THE RELATING GENERAL IT CONTROLS, THEIR DESIGN AND OPERATING EFFECTIVENESS

To: The Management in .legal A/S
.legal A/S customers and their auditors

Scope

We have been engaged to report on .legal A/S's (the service provider) description in Section 3 of the .legal Compliance Platform and the related general IT controls, and on the design and operating effectiveness of the controls related to the control objectives stated in the description throughout the period from 1 November 2025 to 31 October 2026.

.

The service provider's Responsibilities

The service provider is responsible for preparing the description and accompanying statement in section 2, including the completeness, accuracy, and method of presentation of the description and the statement.

The service provider is responsible for providing the services covered by the description; stating the control objectives; and identifying the risks threatening achievement of the control objectives; designing and implementing effectively operating controls to achieve the stated control objectives.

Auditor's Independence and Quality Assurance

We have complied with the requirements of independence and other ethical requirements of the International Ethics Standards Board of Auditors' International Guidelines on the Conduct of Auditors (IESBA Code), which are based on the fundamental principles of integrity, objectivity, professional competence, and due diligence, confidentiality, and professional conduct, as well as ethical requirements applicable in Denmark.

BDO Statsautoriseret Revisionspartnerselskab applies International Standard on Quality Management, ISQM 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's Responsibilities

Our responsibility is, on the basis of our actions, to express a conclusion about the service provider's description as well as about the design and operational efficiency of controls related to the control objectives set out in this description.

We have performed our work in accordance with the International Standard on Assurance Engagements 3402 on assurance engagements with security checks at a service organisation. This standard requires that we plan and carry out our actions in order to obtain a high degree of certainty as to whether the description is correct in all material respects and whether the controls in all essential respects are appropriately designed and have operated effectively.

A declaration task with certainty to provide a statement about the description, design, and operational effectiveness of controls at a service provider includes performing actions to obtain evidence of the information in the service provider's description as well as of the controls' design and operational effectiveness. The actions

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

chosen depends on the assessment of the service provider's auditor, including the assessment of the risks that the description is not accurate and that the controls are not appropriately designed or do not operate effectively. Our actions have included tests of the operational effectiveness of such controls, which we consider necessary to provide a high degree of assurance that the control objectives set out in the description were achieved. A statement of assurance with certainty of this type further includes an assessment of the overall presentation of the description, the appropriateness of the control objectives set out therein and the appropriateness of the criteria specified and described by the service provider in section 2.

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

Limitations of Controls at a Service Organisation

The service organiations' description is prepared to meet the common needs of a wide range of customers and their auditors and may not, therefore, include every aspect of the .legal Compliance Platform that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in service providers statement in section 2. In our opinion, in all material respects:

a. The description of the .legal Compliance Platform and related controls, as designed and implemented throughout the period from 1 November 2025 to 31 October 2026 is in all material aspects, accurate and

b. The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 November 2025 to 31 October 2026; 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 November 2025 to 31 October 2026.

Description of Tests of Controls

The specific controls tested, and results of those tests are listed in section 4.

Intended Users and Purpose

This report is intended only for customers, which have used the service providers .legal Compliance Platform services, and their auditors who have a sufficient understanding to consider it, along with other information about controls operated by the customer themselves when obtaining an understanding of customers' information systems relevant to financial reporting.

Copenhagen, 27 November 2026

BDO Statsautoriseret Revisionspartnerselskab

Nicolai T. Visti
Partner, State Authorised Public Accountant

Mikkel Jon Larssen
Partner, head of Risk Assurance, CISA, CRISC

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

2. .LEGAL A/S' STATEMENT

.legal A/S has prepared the following descriptions of controls relating to the .legal Compliance Platform to the company's customers.

The accompanying description has been prepared for customers who have used the .legal Compliance Platform, and their auditors who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

.legal A/S uses sub-service providers. These sub-service providers' relevant control objectives and related technical and organisational measures, as well as other controls, are not included in the accompanying description.

.legal A/S confirms that the accompanying description fairly presents controls in relation to the .legal Compliance Platform throughout the period from 1 November 2025 to 31 October 2026. The criteria used in making this statement were that the accompanying description:

1. Presents how the controls in relation to the .legal Compliance Platform were designed and implemented, including:
    - The services provided.
    - The procedures within both information technology and manual systems used to manage the controls.
    - Relevant control objectives and controls designed to achieve those objectives.
    - Other relevant aspects of control environment, risk assessment process, information systems, communication, control activities and monitoring controls of relevance for the services provided.
2. Includes relevant details of changes to the controls relating to the .legal Compliance Platform during the period from 1 November 2025 to 31 October 2026.
3. Does not omit or distort information relevant to the scope of the controls described relating to the .legal Compliance Platform considering that the description is prepared to meet the general needs of a wide range of customers and their auditors and therefore cannot include every aspect of the .legal Compliance Platform and controls that the individual customer may consider of importance to their special environment.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

.legal A/S confirms that controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 November 2025 to 31 October 2026. The criteria we used in making this statement were that:

1. The risks that threatened achievement of that control objectives stated in the description were identified.

2. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

3. The controls were consistently applied as designed, including those manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 November 2025 to 31 October 2026.

Aarhus, 27 November 2026

.legal A/S

Brian Østberg
CEO

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

3. .LEGAL A/S' DESCRIPTON OF THE .LEGAL COMPLIANCE PLATFORM

GENERAL DESCRIPTION OF .LEGAL

.legal Compliance Platform (hereinafter "The Platform" or "the system") is a comprehensive governance, risk & compliance (GRC) software solution that helps organisations with their compliance work. It provides four main modules: Data Protection for GDPR compliance, Information Security for cybersecurity compliance (including NIS2), Contract Management for operational contract oversight, and Vendor Management for controlling vendor relationships. The platform includes features like compliance task management, risk assessments, data mapping of processes and assets, vendor audits and assessments, and various add-ons such as framework management and advanced user management.

.LEGAL A/S' DESCRIPTION OF CONTROL ENVIRONMENT

A.4 Risk management

Annual risk assessment
The Executive Board of .legal A/S conducts a risk assessment at least once a year, which includes the IT installations and their use. It is based on the current threat picture and new knowledge in the field, which forms the basis for new security initiatives.

Guidelines and control objectives
Internally, we have documented several control objectives to ensure that we comply with our own security policy.

The control objectives include:

- Purpose: Describes why the control objective is established and ensure that it reflects the overall guideline for the ISO section.
- Measurement point: Describes how the control objective is to be assessed, so that a satisfactory data basis is established, and so that the measurement can be carried out within the time interval described, which ensures that the objective is specific and measurable.
- Threshold: Shows what is required to meet the control objective.

The .legal Compliance is used for follow-up and documentation of the internal control objectives.

A.5 Information security policies

IT security policy
.legal works according to an IT security policy that covers the Services. The IT security policy is organised according to ISO 27001: 2013 and forms the basis for those involved in the development or operation of the Services. The IT security policy is organised according to the standardised ISO areas.

The follow-up on whether the requirements are complied with is in accordance with several guidelines and control objectives, which are described in the policy for each ISO area.

The IT security policy has been approved by Management and published in the Company, including communication to relevant employees and partners. To ensure that the IT security policy is appropriate, adequate, and effective, the IT security policy is reassessed at least once a year or in the event of extensive changes in the organisation that have an impact on the information security.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.6 Organisation of information security

IT security manager
.legal A/S has dedicated an employee with responsibility for organisational and system security.

Segregation of duties
.legal A/S works with segregation of duties to ensure that employees only have access to information required to perform their duties and functions. We work with the functions “Bookkeeping, HR, Legal & Compliance, Marketing, Project Management, Sales, Support, Development and UX & Design”.

We review the employees’ access regularly to ensure that the accesses continue to match their duties.

A.7 Human resource security

Confidentiality
As part of the employment, all employees/consultants have entered a duty of confidentiality which ensures that confidential information is not passed on. The duty of confidentiality applies both during and after employment. In addition, the relevant employees sign a declaration of compliance with the IT Security Policy, which further ensures that information about the system and its security conditions, employees, trade secrets, and information about business relationships remain confidential.

A.8 Asset management

Inventory of assets
All the assets of the systems have been identified, and a list of the assets has been prepared. The list of assets is documented and contains relevant descriptions of sub-components, physical and logical location as well as ownership.

A.9 Access control

Principles of access control
Access to the systems is always allocated based on the "need-to-know" / "need-to-have" and "least privilege" principles, so that it is ensured that access is allocated to users with work-related needs.

Secure login with two-factor authentication
There are several options for system access, depending on the system. The options range from a single sign-on solution via integration with the customer's Microsoft Azure Active Directory to standard email/password authentication or via .legal ID.

.legal ID is a proprietary login provider based on the OpenID Connect / OAuth2.0 security protocols and allows the user to use their .legal ID across .legal products. In addition, .legal ID also supports 2-factor authentication.

Brute force protection
Our login provider is protected against brute force attacks by blocking the user after three login attempts.

The password requirements are:

- Must contain at least 12 characters
- Must contain at least 5 different characters
- Must combine uppercase and lowercase letters, numbers, and symbols
- Must not contain the username
- May not be too common (We check against OWASP's SecLists Project of 10,000 most used passwords)

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

Roles and rights management
Access to functionality in the systems is controlled via a role-based model, where a user is assigned several roles that provide access to specific parts or functions in the system. In systems where there is a need, the rights can be further granulated in relation to reading and writing access.

Privileged access management
An employee with a need for access to production data or production infrastructure (privileged access) must, in addition to a work-related need, have separate approval from the management. Employees with privileged access must always use 2-factor authentication. Employees with privileged access is minimized to an absolute minimum.

Customer Lockbox for Microsoft Azure
Most operations, support, and troubleshooting performed by Microsoft personnel and sub-service providers do not require access to customer data. In those rare circumstances where such access is required, Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data, whether in response to a customer-initiated support ticket or a problem identified by Microsoft.

Customer Lockbox is enabled for all .legal Microsoft Azure Tenants.

A.10 Cryptography

Encryption
The system is a pure browser-based solution. The system encrypts all communication between the client (browser) and the server.

The system uses a SHA-2 SSL certificate with a minimum of 2048bit encryption from a trusted provider.
A minimum of TLS 1.2 is required for all requests to the system.

Data is encrypted "at rest" when stored in the data center and automatically decrypted when accessed. This is done using AES-256 encryption. Encryption keys are managed automatically with regular rotation.

A.11 Physical- and environmental security

Physical security of premises and machines
.legal A/S' premises are locked at all times. .legal A/S does not host solutions itself, which means that the physical security primarily concerns the employees' machines. All employees' machines are encrypted.

Physical access management
Physical access to the office premises is restricted to employees with a work-related need. Access rights are revoked immediately when an employee leaves .legal A/S as part of the offboarding process. On a yearly basis, .legal A/S reviews the list of users with physical access to the office premises to ensure that access rights remain appropriate and that any unauthorised access is identified in a timely manner.

A.12 Operational reliability

Secure hosting
Microsoft Azure is the overall IT platform for the systems in .legal A/S.

A. The code is stored and managed in Azure DevOps.
B. Data is stored in Azure Storage and Azure SQL European data centres.
C. Test and operating environments for the applications are also established in Azure.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

The systems are hosted in Microsoft Azure - i.a. for security reasons, as the underlying platform, is always up-to-date, and the possibilities for data encryption, redundancy, backup and access control are generally good.

Concerning the use of third-party services outside Azure, these are selected based on requirements for a high-security standard (eg ISO27001 certification) as well as compliance with the GDPR. In general, we try to reduce the need of third-party services outside of Microsoft Azure.

Data redundancy
Production databases are actively geo-replicated to secondary databases located in Nothern Europe. If a primary database is down, this allows for fast failover to the corresponding secondary database which help to ensure high availability of the systems.

Customer documents are stored in read-access geo-redundant storage: three synchronous copies in West Europe and three further copies replicated to North Europe.

Database backup within Azure
Continuous backup allows the database to be restored to any point in time within the last 30 days.

Weekly full backups are retained for a further two months in immutable storage that cannot be altered or deleted, including by .legal's own personnel.

Database backups are stored in geo-redundant storage: three copies within West Europe and three further copies in North Europe. This applies both to the continuous point-in-time backup and to the weekly full backups.

Database backups are held in storage managed by Microsoft and are not reachable from .legal's environment or with .legal's credentials.

All database backups are written with checksum verification, and integrity is verified during both backup and restore.

Document backup within Azure
Documents are versioned, so earlier versions remain available after a document is changed or overwritten.

A deleted document can be restored for 30 days after deletion, and permanent deletion within that period is blocked at platform level.

Each customers document storage can be restored as a whole to any point in time within the last 30 days.

Document storage is geo-redundant, as described under Data redundancy above.

Backup outside Azure
In addition to the backup within Azure, a copy of production databases and document files is transferred every night to object storage at an independent provider, Hetzner, so that the data is also held outside Microsoft Azure and protected against provider-level incidents. The provider is listed in .legal's overview of service providers.

Hetzner is a European company, wholly owned and operated within the EU, and the data is stored in Germany. The backup is therefore held both outside Microsoft Azure and outside the ownership of any non-EU group.

Both the database backup files and the file contents are encrypted with AES-256 before they leave Azure. The encryption keys are held by .legal outside Microsoft Azure environment and are not available to the storage provider, which therefore holds only encrypted data.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

The nightly backup is retained for 30 days on immutable storage that cannot be altered or deleted during that period, which protects it against ransomware and against accidental or malicious deletion.

Network Security
Documents and database records never traverse the public internet within our infrastructure. All connections between our application and storage systems occur through isolated private networks (VNet) with strict firewall rules.

Passwordless Storage and Database Access
Database and document storage use managed identity authentication instead of passwords or keys. This means:
No database passwords or secrets are stored in configuration files
Automatic credential rotation without downtime

Automated Threat Detection
All uploaded documents undergo automatic malware scanning before storage. Files are checked against continuously updated threat databases, with infected documents automatically quarantined.

Vulnerability management
An authorised external provider performs scheduled and documented vulnerability scans and penetration tests monthly to effectively identify potential vulnerabilities. If risks classified as 'high' or 'medium' are identified, mitigating measures are implemented as soon as possible. 'Low' severity findings are documented and prioritised alongside other development activities.

Logging, Monitoring, and Alerts
System events are logged to a central system log, so it is possible to track any errors across components in the overall system. The overall system is monitored via Dashboards, where we can follow resource consumption, usage, and errors in an overall overview. Based on the centralised log, several alarms have been defined that are handled by the development team.

Changes to data and configuration in the Services are recorded in an audit log, which is available to the customer's administrators within the Services.

Access to logs is restricted to personnel with privileged access, as described under A.9. Logs contain only the information necessary for security monitoring and incident investigation, such as user identity, timestamp and action performed.

High availability
We strive to keep all our services available 24 hours a day, 365 days a year. We continually release new features and enhancements, but all services are released automatically and most without downtime. If a service cannot be released without downtime, we schedule the change according to usage so that as few users as possible are affected. If we know the change will affect users, the customer is notified in advance.

All our services are hosted on Azure with the following service level agreement (SLA):

- Web Apps SLA: 99,95%
- Azure SQL Server SLA: 99,99%
- SLA for Document Storage: 99,99%

More details: https://azure.microsoft.com/en-us/support/legal/sla/summary/

The availability of our systems is continually monitored and logged. And the current status as well as the uptime history can be accessed at https://status.dotlegal.com.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.13 Communication security

Secure communication via SSL
Communication between the browser and the rest of the system takes place via HTTPS (SHA-2 SSL certificate with a minimum of 2048bit encryption).

Exchange of data between the customers and the system takes place either via SFTP or built-in functionality for import and export of data, which in turn is protected with HTTPS.

Confidentiality agreements
All employees and any subcontractors are subject to confidentiality agreements, which apply both during and after working with the systems.

A.14 Procurement, development, and maintenance of systems

Development process
The focal point of our daily work is our joint development process, which is based on modern but well-proven methods such as SCRUM and Kanban. Each product has its own product owner with responsibility for planning and prioritising as well as a permanent development team with responsibility for development and quality assurance. In addition, support speaks directly with the product owner, development team and customers.

The development process ensures that we have daily back-and-forth discussion that address any challenges and help each other to effective solutions. We have more eyes on the changes we make and actively try to constantly improve our skills and improve the systems we work with.

All development teams have experienced people onboard to ensure a high level - also when it comes to safety.

Quality assurance
Quality assurance elements from the common .legal development process:

A. Structured process
    i. All work, regardless of character, is visualised as tasks in our task management. All tasks must go through the same overall process with several phases, including code review, internal testing, and acceptance testing.
B. Automated quality assurance
    i. Version-controlled code
    ii. Continuous integration which continuously builds the code to ensure integrity
    iii. Automated tests that run continuously to minimise regression errors
    iv. Automated deployment pipelines which mean that we can safely and with high traceability deploy new code for tests and production environments.
C. Development, test, and production environment
    i. Dedicated development, testing and production environments to be able to ensure quality on several levels before new code reaches the production environment.
D. Monitoring and alerting
    I. Our environments are monitored so that we can ensure high uptime and receive alarms about any errors or vulnerabilities as quickly as possible.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.15 Supplier conditions

Supplier agreements
Agreements are established with all suppliers that have access to the systems. Subservice organisations are, where possible, subject to security requirements that are consistent with the security standards and policies applied by .legal A/S.

For SaaS subservice organisations where .legal A/S is unable to impose its own security requirements, reliance is placed on the contractual terms and security measures established and maintained by the respective subservice organisations.

Supplier control
.legal performs an annual security supervising of 3rd party sub-service providers that are part of the overall system.

A.16 Management of information security and personal data breaches

Procedure for handling information security incidents
All safety incidents or observed weaknesses are reported to the Executive Board or the safety officer. As soon as a security incident or vulnerability is reported, the following activities are initiated:

1. The security incident is registered in the company's task management.
2. In the description of the task, the security incident/weakness is noted in as many details as possible, including as a minimum:
    a) When the incident took place
    b) What the incident was actually about
    c) Who reported the incident
3. The incident is then analysed with a view to the following:
    a) Determine how extensive the incident is
    b) Which customers are affected
    c) What needs to be done to either stop the incident or accommodate the incident in the future e.g. for code corrections
4. Customers identified in point 3 are then informed about the incident and the consequences of the incident, as well as what measures have been taken in the future.
5. The measures that have been decided are prioritized and implemented.
6. Once the measures have been implemented, the task is closed.
7. After the problem is solved, the process is described as an incident in the project's incident log. The purpose is to investigate whether there is an underlying problem that may give rise to further improvements or help remedy similar future problems.

Procedure for handling personal data breaches
All security incidents or observed vulnerabilities involving personal data are reported to the Executive Board or the safety officer. As soon as a security incident or vulnerability is reported, an internal process is initiated to stop and contain the incident.

Specifically on the handling of personal data breaches when .legal A/S is the service provider
.legal A/S shall notify the data controller without undue delay after becoming aware of a personal data breach, in accordance with Article 33(2) of the GDPR, to enable the data controller to comply with its obligation to notify the supervisory authority in accordance with Article 33(1) of the GDPR.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.18: Compliance

Procedure for compliance with applicable legislation
It is the responsibility of the Executive Board of .legal A/S that regulatory safety requirements are complied with, including:

- Act no. 502 of 23 May 2018 on supplementary provisions to the Regulation on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data (Data Protection Act)
- Personal Data Regulation (Regulation No 2016/679)
- Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act)

Once a year, the .legal A/S Executive Board asks the company's legal function to assess whether changes in legislation require changes to the security policy and/or the system. The assessment is documented and presented to the Executive Board, which reviews and approves it. The result is noted at the board meeting, and any resulting changes are implemented.

Changes during the period 1. November 2025 to 31. October 2026 relating to the .legal platform

.legal has made the following significant changes to the service and the associated technical and organisational security measures and other controls during the period 1 November 2025 to 31 October 2026

- .legal has implemented off-Azure backup to a 100% EU based and EU owned provider.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

4. CONTROL OBJECTIVES, CONTROLS, TEST AND RESULTS OF TESTS

Objective and scope

BDO has carried out the work in accordance with ISAE 3402 on assurance engagements relating to controls at a service organisation.

BDO has performed procedures to obtain evidence of the information in .legal A/S' description of the .legal Compliance Platform and of the design and the operating effectiveness of the related general IT controls. The procedures performed depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed or operating effectively.

BDO's test of the design and operating effectiveness of general IT controls has included the control objectives and related control activities selected by .legal A/S, and which are described in the following.

In the check form, BDO has described the tests performed which were considered necessary to obtain a reasonable degree of assurance that the stated control objectives were achieved and that the related controls were suitably designed and operated effectively throughout the period from 1 November 2025 to 31 October 2026.

Tests performed

Tests of the design of technical and organisational security measures and other controls and implementation hereof were performed on inquiry, inspection, observation, and re-performance.

Type	Description
Inquiry	Interviews of relevant personnel at .legal A/S have been performed for all significant control activities. The purpose of the interviews was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures, and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, and whether the design of the controls is such that they are expected to be effective if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals. Tests have been performed of significant system structures of technical platforms, databases, and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations and access controls, data transmission and inspection of equipment and locations.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the control is implemented.
Re-performance	Controls have been re-performed to obtain additional evidence that the controls operate as assumed.

For the hosting services provided by Microsoft Azure, we received an independent auditor's SOC 2 report on the sub-service provider's technical and organisational security measures and other controls for the period from 1 April 2025 to 31 March 2026, as well as Bridge Letters from 1 July 2026.

For the service provided by Hetzner Online GmbH within storage backup, we have received an ISO 27001:2022 certificate valid from 27. September 2026 to 26. September 2028

These subcontractors relevant control objectives and related controls are not include in .legal A/S' description of the .legal Compliance Platform and the related controls. We have therefore only inspected the received

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

documentation and tested the controls with .legal A/S, who secures the supervision on the agreement between the service subcontractor and .legal A/S.

Result of test

The results of the tests performed of controls show whether the test has given rise to note deviations.

A deviation exists when:

- Controls have not been designed and implemented to achieve a control objective
- Controls relating to a control objective are not suitably designed and implemented or did not operate effectively throughout the period.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.4: Risk assessment

4.1 Control Objective

- *To ensure that the service provider carries out an annual risk assessment in relation to the consequences for the company which forms basis for the information security.*

Control Activity	Test performed by BDO	Result of test
4.1.1 Risk assessment ▶ A risk assessment is performed annually which is presented to and assessed by management. ▶ An annual risk assessment is performed, providing the basis for the selection and implementation of appropriate information security measures	We made inquiries of relevant personnel at .legal A/S. We have inspected the service provider's procedure for the annual review of risk assessments and observed that such reviews are required to be performed annually. We have inspected documentation for that the management have approved the risk assessments. We have inspected that the risk assessment has been updated within the assurance period.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.5 Information security policies

A.5.1 Guidelines for managing information security

- *To provide guidelines for and supporting information security and data protection in accordance with business requirements and relevant laws and regulations.*

Control Activity	Test performed by BDO	Result of test
5.1.1 Policies for information security ▶ Management sets out and approves policies for information security which after approval are published and communicated to staff and relevant external parties.	We made inquiries of relevant personnel at .legal A/S. We have inspected the information security policies and observed that they have been established and approved by Management. On a sample basis, we inspected evidence that employees had signed to confirm that they had read and understood the security policies.	No exceptions noted.
5.1.2 Review of policies for information security ▶ The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	We made inquiries of relevant personnel at .legal A/S. We have inspected the information security policy and observed that it was updated and approved by management during the assurance period.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.6 Organisation of information security		
Control Objective ▶ *To establish a management basis for initiating and managing the implementation and operation of information security and data protection in the organisation.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.6.1.1 Roles and responsibilities for information security ▶ All information security responsibilities are defined and allocated.	We made inquiries of relevant personnel at .legal A/S. We have inspected the service provider's information security policy and observed that all responsibilities for information security are clearly defined and allocated.	No exceptions noted.
A.6.1.2 Segregation of duties ▶ Contradictory functions and responsibilities are separated to reduce the possibility of unauthorized or accidental use, alteration or misuse of organizational assets.	We made inquiries of relevant personnel at .legal A/S. We have inspected the service provider's procedure for segregation of duties and observed that roles and responsibilities have been defined and segregated to ensure appropriate segregation of duties. We further observed that the creation of administrator accounts requires management approval. We inspected the service provider's employee list and observed that employees' roles and responsibilities are documented. We inspected user access listings for the relevant systems and observed that appropriate segregation of duties has been implemented. We were informed that no new administrator accounts were created during the reporting period. Consequently, there was no population available for testing, and we were therefore unable to test the operating effectiveness of the control relating to management's approval of the creation of new administrator accounts.	Upon request, we have been informed that no new administrators have been created during the assurance period. Therefore, we cannot test control implementation and operational effectiveness. No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.7 Human resource security

Control Objective

- *To ensure that employees and contracting parties are aware of and meet their information security responsibilities.*
- *To protect the organisation's interests as part of the change or termination of the employment relationship.*

Control Activity	Test performed by BDO	Result of test
A.7.1.1 Before employment ▶ A background check is made of all job candidates in accordance with business requirements regarding the function to be held by the employee.	We made inquiries of relevant personnel at .legal A/S. We have inspected the service provider's procedure for background check for new employees with access to personal data and observed that they must present a criminal record. Upon request, we have been informed that there have not been any new joiners within the assurance period relevant for background check in accordance with business requirements.	Upon request, we have been informed that there have not been any new joiners within the assurance period. Therefore, we cannot test control implementation and operational effectiveness. No exceptions noted.
A.7.2.1. Management responsibilities ▶ Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	We made inquiries of relevant personnel at .legal A/S. We have inspected the service provider's procedures for employee and supplier security and observed that all employees and contractors are required to sign a declaration confirming that they have read, understood and agreed to comply with the organisation's established information security policies and procedures. On a sample basis, we have inspected signed declarations from the service provider's employees and observed that the declarations had been duly signed.	No exceptions noted.
A.7.3.1 Termination or change of employment responsibilities ▶ Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor, and enforced.	We made inquiries of relevant personnel at .legal A/S. We have inspected the service provider's employment contract template and observed that it sets out employees' obligations and responsibilities that continue to apply following termination or changes in employment.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.7 Human resource security

Control Objective

- *To ensure that employees and contracting parties are aware of and meet their information security responsibilities.*
- *To protect the organisation's interests as part of the change or termination of the employment relationship.*

Control Activity	Test performed by BDO	Result of test
	On a sample basis, we inspected documentation and observed that former employees had returned their equipment and that their access rights had been removed from all relevant systems.	

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.8 Asset management		
Control Objective ▶ *To identify the organisation's assets and define appropriate responsibilities for its protection.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.8.1.1 Inventory of assets ▶ Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	We made inquiries of relevant personnel at .legal A/S. We have inspected the service provider's inventory of information assets and information processing facilities. We have inspected the asset inventory and observed that it was updated during the assurance period.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.9 Access management

Control Objective

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control Activity	Test performed by BDO	Result of test
A.9.1.2 Access to networks and network services ▶ Users shall only be provided with access to the network and net- work services that they have been specifically authorized to use. ▶ Documents and database records never traverse the public internet within our infrastructure. All connections between our application and storage systems occur through isolated private networks (Vnet) with strict firewall rules.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's access control procedure and observed that it includes restrictions governing access to the network and network services. We inspected access to the service provider's network and network services and observed that access is restricted to a limited number of employees with a business need for such access. We inspected the configuration of the private networks (VNets) and observed that the private networks are isolated.	No exceptions noted.
A.9.2.2 User Access provision ▶ A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's access control procedure and observed that access rights are required to be granted based on business need. We were informed that the service provider has established a formal process for evaluating and approving access rights for new employees. Upon request, we have been informed that there have not been any new joiners within the assurance period.	Upon request, we have been informed that there have not been any new joiners within the assurance period. Therefore, we cannot test control implementation and operational effectiveness. No exceptions noted.
A.9.2.3 Management of privileged access rights ▶ The service provider has implemented granting of administrative access to entities according to the functional need which is authorized by management. ▶ Access with privileged rights requires two-factor login.	We made inquiries of relevant personnel at .legal A/S.	Upon request, we were informed that no new employees were granted privileged access during the assurance period. Therefore, we cannot test control implementation and operational effectiveness.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.9 Access management		
Control Objective ▶ *To restrict access to information and information processing facilities.* ▶ *To ensure access for authorised users and prevent unauthorised access to systems and services.* ▶ *To prevent unauthorised access to systems and applications.*		
Control Activity	**Test performed by BDO**	**Result of test**
▶ The service provider has implemented logging of accesses with privileged accounts (administrative rights). .	We have inspected the procedure for allocating administrative rights in the system and observed that this must be done after approval by management. We inspected the user access overview and observed that no new employees were granted privileged access during the assurance period. Consequently, there were no instances available for testing, and we were therefore unable to test this control. We inspected that access with privileged access rights requires the use of passwords and two-factor login We have inspected that the service provider has implemented logging of accesses with privileged accounts.	No exceptions noted.
A.9.2.5 Review or adjustment of access rights ▶ User rights are reviewed periodically.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's periodic review of assigned access rights and confirmed that the review was performed during the assurance period.	No exceptions noted.
A.9.4.1 Information access restriction ▶ Access to information and application system functions shall be restricted in accordance with the access control policy.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's access control procedure and observed that access and user rights are granted based on a business need. We inspected the access and user rights granted to employees and observed that access is restricted to systems and services required for the performance of their work.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.9 Access management

Control Objective

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control Activity	Test performed by BDO	Result of test
A.9.4.2 Secure log-on procedures ▶ Where required by the access control policy, access to systems and application shall be controlled by a secure log-on procedure as password and two-factor login ▶ The login functionality is configured with security measures designed to mitigate the risk of brute-force attacks ▶ Access to the Azure environments is controlled and monitored through Microsoft Lockbox functionality	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's access control procedure and observed that it requires the use of passwords and two-factor authentication where possible. We inspected the configuration of the .legal Compliance Platform and observed that two-factor authentication has been implemented. We inspected security measures to mitigate the risk of brute-force attacks. We inspected the configuration relating to the use of Microsoft Lockbox functionality.	No exceptions noted.
A.9.4.3 Password management system ▶ Password management systems shall be interactive and shall ensure quality passwords. ▶ Database and document storage use managed identity authentication instead of password or keys. No database passwords og secrets are stored in configuration files. Credentials are automatically rotated without downtime.	We made inquiries of relevant personnel at .legal A/S. We inspected the IT security policy and observed that all employees are required to use the company-approved password manager. We inspected the service provider's password manager and observed that all employees had active user accounts. We inspected the configuration of the password manager and observed that multi-factor authentication is mandatory for all active users. We have inspected identify authentication to Azure environment and observed that access only is granted from .legals network using password and multi-factor authentication.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.9 Access management		
Control Objective ▶ *To restrict access to information and information processing facilities.* ▶ *To ensure access for authorised users and prevent unauthorised access to systems and services.* ▶ *To prevent unauthorised access to systems and applications.*		
Control Activity	**Test performed by BDO**	**Result of test**
	We inspected the configuration of managed identity authentication for databases and document storage and observed that managed identity authentication had been implemented. We have on a sample basis inspected that workstations have password requirements.	
A.9.4.5 Access control to program source code ▶ Access to program code shall be restricted.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's access control procedure for development environments, including access to source code, and observed that source code is securely stored in a dedicated project. We inspected the access controls for the source code of the .legal Compliance Platform and observed that access is restricted to authorised developers.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.10 Cryptography		
Control Objective ▶ *To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.10.1.1 Policy on the use of cryptographic controls ▶ A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's encryption policy and observed that systems are required to use, as a minimum, a SHA-2 SSL certificate with a key length of at least 2,048 bits. We inspected the configuration of the .legal Compliance Platform and observed that it uses a SHA-2 SSL certificate with a key length of at least 2,048 bits. On a sample basis, we inspected the encryption settings on employees' workstations and observed that encryption was enabled.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.11 Physical and environmental security

Control Objective

- *To prevent unauthorised physical access to and damage and interruption of the organisation's information and information processing facilities.*

Control Activity	Test performed by BDO	Result of test
A.11.1.3 Securing offices, rooms, and facilities ▶ Physical security for offices, rooms and facilities shall be designed and applied ▶ A review of access rights to the office facilities performed quarterly	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's physical security procedure and observed that physical security controls are required to be implemented at locations under the service provider's physical control. We inspected the service provider's premises in Aarhus and observed that physical access to both the office and the building is secured by locks and alarm systems. We also inspected the list of employees with physical access to the premises and observed that access is restricted to internal employees. On a sample basis we inspected review of access rights to the office facilities.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.12 Operations security

Control Objective

- *To ensure correct and reliable operation of information processing facilities.*
- *To protect against data loss.*
- *To record incidents and obtain evidence.*

Control Activity	Test performed by BDO	Result of test
A.12.1.1 Documented operating procedures ▶ Operating procedures shall be documented and made available to all users who need them.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's operating procedure and observed that it had been established and made available to employees on the service provider's internal platform.	No exceptions noted.
A.12.1.2 Change management ▶ Changes to the organisation, business processes, information processing facilities and systems that affect information security shall be controlled.	We made inquiries of relevant personnel at .legal A/S. We have inspected the service provider has a development procedure and observed that change management are included in the procedure. Furthermore, we have observed that the procedure states that development projects in the .legal Compliance Platform are controlled with version historic and traceability. By inquiry we have been informed that newly developed code is quality assured and tested by another developer prior to implementation in the production environment. On a sample basis we inspected, that all changes followed the procedure for change management.	No exceptions noted.
A.12.1.4 Separation of development, test, and operation environments ▶ Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's procedure for segregation of duties and segregation of environments.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.12 Operations security

Control Objective

- *To ensure correct and reliable operation of information processing facilities.*
- *To protect against data loss.*
- *To record incidents and obtain evidence.*

Control Activity	Test performed by BDO	Result of test
	We inspected the configuration of the .legal Compliance Platform and observed that the development, testing and production environments are segregated. .	
A.12.3.1 Backup of information ▶ Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy. ▶ Backup copies outside the Azure environment are securely stored at a separate location. ▶ Restore tests are carried out for customers with restore agreements according to the agreements	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's backup procedure for the .legal Compliance Platform and observed that backups are required to be performed in accordance with the procedure. We have inspected the configuration of automated monitoring of backup execution. We have inspected security measures for backups storing in separate location outside the Azure environment. We have inspected documentation for restore test of services has been performed from Azure and offline location within the assurance period.	No exceptions noted.
A.12.4.1 Event logging ▶ Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's procedure for logging, monitoring and alerting and observed that it requires event-based logging of user activities, signatures, errors and information security incidents. We also observed that logs are notified in communications channels to the operations. We inspected the logging configuration of the .legal Compliance Platform and observed that event logging had been implemented.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.12 Operations security

Control Objective

- *To ensure correct and reliable operation of information processing facilities.*
- *To protect against data loss.*
- *To record incidents and obtain evidence.*

Control Activity	Test performed by BDO	Result of test
	We inspected the service provider's alerting configuration for event logging and observed that key personnel are notified when an alert is triggered. We inspected the service provider's event monitoring dashboard and observed that events are reviewed daily by the operations team.	
12.6.1 Vulnerability Scanning - Vulnerability scans are conducted monthly. The result is documented. - The service provider reviews the results and follows up on identified vulnerabilities. - The service provider has documented their mitigation efforts of identified vulnerabilities - All uploaded documents undergo automatic malware scanning before storage. Files are checked against continuously updated threats databases, with infected document automatically quarantined.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's procedure for logging, monitoring and alerting By inquiry we have been informed that the service provider performs vulnerability scanning each month. We inspected the service provider's vulnerability scanning history and observed that vulnerability scans had been performed multiple times during the assurance period. We inspected the vulnerability scanning reports and observed that identified vulnerabilities were reported. On a sample basis, we have inspected that identified vulnerabilities have been remediate or that the associated risks have been reduced to an accepted level. We inspected the configuration for automatic antivirus scanning of documents and observed that automatic scanning had been implemented.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.12 Operations security

Control Objective

- *To ensure correct and reliable operation of information processing facilities.*
- *To protect against data loss.*
- *To record incidents and obtain evidence.*

Control Activity	Test performed by BDO	Result of test
12.7-1 High availability ▶ System availability is monitored and complies with the requirements specified in customer agreements.	We made inquiries of relevant personnel at .legal A/S. We inspected the monitoring of high availability om system and services. We inspected whether the actual system's availability was in accordance with the levels specified in the customer agreements.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.13 Communications security		
Control Objective ▶ *To maintain information security when transferring internally in an organisation and to an external entity.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.13.2.2 Agreements on information transfer ▶ Agreements shall address the secure transfer of business information between the organisation and external parties.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's supplier security procedure and observed that, when entering into an agreement with a supplier, a declaration is required to be signed in accordance with the service provider's security policy. Furthermore, we inspected the service provider's encryption policy and observed that data transmitted over the internet is required, as a minimum, to be protected using an SSL certificate based on SHA-2 with a key length of at least 2,048 bits. We inspected the service provider's supplier agreement template. We inspected the system configuration and observed that communication between the browser and the system is secured using HTTPS with an SSL certificate based on SHA-2 with a key length of 2,048 bits. We inspected the system configuration and observed that data exchanged between customers and the system is transferred using SFTP with RSA-SHA256 and a key length of 3,072 bits. By inquiry, we were informed that no supplier had been given access during the assurance period. Consequently, we were unable to test the operating effectiveness of the procedure during the assurance period.	Upon request, we were informed that no suppliers were granted access during the assurance period. Therefore, we cannot test control implementation and operational effectiveness No exceptions noted.
A.13.2.4 Confidentiality or non-disclosure agreements ▶ Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed, and documented.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's personnel security procedure and observed that new employees are required to sign a declaration confirming compliance with the service provider's information security policy upon commencement of employment.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.13 Communications security		
Control Objective ▶ *To maintain information security when transferring internally in an organisation and to an external entity.*		
Control Activity	**Test performed by BDO**	**Result of test**
	We also inspected the service provider's employment contract template and observed that it includes confidentiality requirements applicable both during and after employment. On a sample basis, we inspected confidentiality agreements for employees and confirmed that they had been signed.	

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.14 System acquisition, development, and maintenance of systems		
Control Objective ▶ *To ensure that information security is organised and implemented within the information systems development life cycle.* ▶ *To ensure the protection of data used for testing.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.14.2.2 System change control procedures ▶ Changes to systems within the development lifecycle shall be controlled using formal Change Management procedures.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's development procedure and observed that changes to systems throughout the development life cycle are required to be managed in accordance with formal change management procedures. We inspected the implementation of the change management procedure and observed that system changes are subject to a formal approval process. On a sample basis, we inspected changes made during the assurance period and confirmed that they had been performed in accordance with the service provider's change management procedure.	No exceptions noted.
A.14.2.3 Technical review of applications after changes to operating platforms ▶ Formal processes and procedures have been implemented for all changes made in the company's own IT environment.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's development procedure and observed that all changes are required to be approved first by another developer and subsequently by the task manager. On a sample basis, we inspected changes made during the assurance period and confirmed that they had been approved in accordance with the service provider's development procedure.	No exceptions noted.
A.14.2.6 Secure development environment	We made inquiries of relevant personnel at .legal A/S.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.14 System acquisition, development, and maintenance of systems		
Control Objective ▶ *To ensure that information security is organised and implemented within the information systems development life cycle.* ▶ *To ensure the protection of data used for testing.*		
Control Activity	**Test performed by BDO**	**Result of test**
▶ Organisations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	We inspected the service provider's development procedure and observed that it includes formal requirements governing development activities throughout the entire development life cycle. We inspected the service provider's development tool, including version history and code reviews, and observed that development activities were performed in accordance with the service provider's development procedure. We inspected the service provider's test environment and observed that only non-production data were used for testing purposes.	
A.14.2.8 System security testing ▶ Testing of security functionality shall be carried out during development.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's development procedure and observed that regression testing is required to be performed to ensure that changes do not adversely affect the organisation's operations or information security. On a sample basis, we inspected changes made during the assurance period and confirmed that testing had been performed in accordance with the service provider's development procedure.	No exceptions noted.
A.14.3.1 Securing test data ▶ A fixed procedure has been implemented for the protection of test data.	We made inquiries of relevant personnel at .legal A/S. We have inspected the service provider's procedure for development and observed that the test environment must be segregated and only contain fake data.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.14 System acquisition, development, and maintenance of systems		
Control Objective ▶ *To ensure that information security is organised and implemented within the information systems development life cycle.* ▶ *To ensure the protection of data used for testing.*		
Control Activity	**Test performed by BDO**	**Result of test**
	We have inspected the service providers test environment and observed that data are non-production data.	

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.15 Supplier relationship

Control Objective

- *To ensure protection of the organisation's assets that suppliers have access to.*

Control Activity	Test performed by BDO	Result of test
A.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 shall be agreed with the supplier and documented.	We made inquiries of relevant personnel at .legal A/S. We have inspected the service provider's supplier overview and observed that sub-service providers are used for hosting, operations and backup storage. We observed that .legal is unable to impose its own security requirements on the service providers used in connection with the provision of SaaS solutions. .legal therefore relies on the contractual terms and security measures established by the respective service providers. We have inspected the service provider's procedure for supervising sub-service providers and observed that the service provider annually checks that sub-service providers' auditor's statements and certifications are satisfactory, based on the service provider's risk assessment and actual security requirements. We have observed that agreements with a new sub-service provider, Hetzner Online GmbH, were entered into during the assurance period. We have inspected that the service provider has agreed to the Teams of Measures. We have inspected the monitoring performed with respect to sub-service providers and observed that relevant SOC 2 reports or other supporting documentation e.g. ISO certificates have been reviewed. We have inspected that identified deviations have been assessed based on their associated risks, and that supplementary activities at the service provider have been performed where deemed necessary.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.15 Supplier relationship

Control Objective

- *To ensure protection of the organisation's assets that suppliers have access to.*

Control Activity	Test performed by BDO	Result of test
A.15.1.2 Addressing security within supplier agreements ▶ All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's supplier security procedure and observed that, when entering into an agreement with a supplier, a declaration is required to be signed in accordance with the service provider's information security policy. We also inspected the template for the declaration. By inquiry, we were informed that no suppliers were granted access to the service provider's systems or infrastructure during the assurance period. Consequently, we were unable to test the operating effectiveness of the control during the assurance period.	By inquiry, we were informed that no suppliers were granted access to the service provider's systems or infrastructure during the assurance period. Therefore, we cannot test control implementation and operational effectiveness. No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.16 Information security incident management		
Control Objective ▶ *To ensure a uniform and effective method of managing information security incidents, including communication on security incidents and weaknesses.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.16.1.1 Responsibilities and procedures ▶ Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's procedure for security breaches and observed that roles and responsibilities for incident handling in the event of a security breach have been defined by management.	No exceptions noted.
A.16.1.2 Reporting of information security incidents ▶ Information security events shall be reported through appropriate management channels as quickly as possible.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's procedure for security breaches and observed that a report is required to be prepared whenever a security breach occurs. By inquiry, we were informed that no security breaches had occurred during the assurance period. Consequently, we were unable to test the operating effectiveness of the control during the assurance period.	Upon request, we have been informed that the service provider has not had any security breaches during the assurance period. Therefore, we cannot test control implementation and operational effectiveness. No exceptions noted.
A.16.1.6 Learning from information security incidents ▶ Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's procedure for security breaches and observed that, as part of the reporting of an information security breach, an evaluation of the handling of the incident is required to be included in the incident report. By inquiry, we were informed that no security breaches had occurred during the assurance period. Consequently, we were unable to test the operating effectiveness of the control during the assurance period.	Upon request, we have been informed that the service provider has not had any security breaches during the assurance period. Therefore, we cannot test control implementation and operational effectiveness. No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.16 Information security incident management		
Control Objective ▶ *To ensure a uniform and effective method of managing information security incidents, including communication on security incidents and weaknesses.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.16.1.7 Collection of evidence ▶ Evidence of information security breaches is collected.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's procedure for security breaches and observed that, in the event of an information security breach, relevant evidence is required to be collected where possible. By inquiry, we were informed that no security breaches had occurred during the assurance period. Consequently, we were unable to test the operating effectiveness of the control during the assurance period.	Upon request, we have been informed that the service provider has not had any security breaches during the assurance period. Therefore, we cannot test control implementation and operational effectiveness. No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

A.18 Compliance

Control Objective

- *To ensure that information security and data protection is implemented and run in accordance with the organisation's policies and procedures.*

Control Activity	Test performed by BDO	Result of test
A.18.1.1 Identification of applicable legislation and contractual requirements ▶ All relevant legislative, statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented, and kept up to date for each information system and the organisation.	We made inquiries of relevant personnel at .legal A/S. We inspected the service provider's procedure for compliance with legal and contractual requirements and observed that management performs an annual review of relevant legislation and standards to ensure continued compliance with applicable legal, regulatory and contractual requirements. We have inspected that the annual review was performed during the assurance period.	No exceptions noted.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

BDO STATSAUTORISERET REVISIONSPARTNERSELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

BDO Statsautoriseret Revisionspartnerselskab, a Danish-owned advisory and auditing firm, is a member of BDO International Limited - a UK-based company with limited liability - and part of the international BDO network consisting of independent member firms. BDO is the trademark of both the BDO network and of all BDO member firms. BDO in Denmark employs more than 1,800 people, while the worldwide BDO network has approx. 95,000 employees in 169 countries.

Copyright - BDO Statsautoriseret Revisionspartnerselskab, cvr.nr. 45719375.

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8F-CEE8V-WCMFL

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Brian Østberg
CEO
Serienummer: dab750c2-1b99-4493-8e2f-4e0c44e45883
IP: 93.165.xxx.xxx
2026-11-27 08:12:08 UTC

MitID

Mikkel Jon Larssen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Partner
Serienummer: cd9a38dd-e75c-40f7-80d6-ec5b5d0841d6
IP: 77.243.xxx.xxx
2026-11-27 08:47:23 UTC

MitID

Nicolai Tobias Visti Pedersen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Statsautoriseret revisor
Serienummer: c42f66e9-59bb-478a-9d92-2a2b8602724e
IP: 77.243.xxx.xxx
2026-11-27 08:56:22 UTC

MitID

Penneo dokumentnøgle: VNSXZ-48SGZ-12AU2-WGP8E-CEE8V-WCMFL

Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se **https://eutl.penneo.com**.

Sådan kan du verificere, at dokumentet er originalt
Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskriveres digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, **https://penneo.com/validator**, eller andre valideringstjenester for digitale underskrifter.