INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD 1 NOVEMBER 2025 TO 31 OCTOBER 2026 ON THE DESCRIPTION OF THE .LEGAL COMPLIANCE PLATFORM AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS, RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

.LEGAL A/S

Penneo dokumentnøgle: TVZF8-778ZP-O2S3U-UKVLF-0XV8J-S3U0B

CONTENTS

1. INDEPENDENT AUDITOR'S REPORT 2

2. .LEGAL'S STATEMENT 5

3. .LEGAL A/S' DESCRIPTION OF THE .LEGAL COMPLIANCE PLATFORM 7

General description of .legal 7
Description of the.legal compliance platform and processing of personal data 7
General description of .legal's organisation 8
Management of personal data security 8
Risk management of THE .legal Compliance Platform 9
Control framework, control structure and criteria for control implementation 10
Changes during the period from 1 November 2025 to 31 October 2026. 18
Complementary controls for .legal's customers 18

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND THE RESULT OF TESTS 19

A.4: Risk assessment 21
A.5: Information security policies 22
A.6: Organisation of information security 23
A.7: Human resource security 24
A.8: Asset management 26
A.9: Access management 27
A.10: Cryptography 29
A.11: Physical and environmental security 30
A.12: Operations security 31
A.13: Communications security 33
A.14: System acquisition, development, and maintenance of systems 34
A.15: Supplier relationships 35
A.16: Information security incident management 38
A.17: Information security aspects of disaster recovery, contingency and restore 39
A.18: Compliance 40

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

1. INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT FOR THE PERIOD 1 NOVEMBER 2025 TO 31 OCTOBER 2026 ON THE DESCRIPTION OF THE .LEGAL COMPLIANCE PLATFORM AND .LEGAL A/S AND RELATED TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DANISH ACT ON SUPPLEMENTARY PROVISIONS

To: The Management of .legal A/S
.legal A/S' Customers

Scope

We have been engaged to report on .legal (the Data Processor) description in section 3 of the .legal Compliance Platform and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions to the Regulation (Danish Data Protection Act), and on the design and operating effectiveness of the technical and organisational measures and other controls related to the control objectives stated in the description for the period 1 November 2025 to 31 October 2026.

The Data Processor's Responsibilities

The Data Processor is responsible for preparing the statement in section 2 and the accompanying description including the completeness, accuracy, and method of presenting the statement and the description. Furthermore, the Data Processor is responsible for providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's Independence and Quality Control

We have complied with the requirements of independence and other ethical requirements of the International Code of Ethics for Professional Accountants (including International Independence Standards (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 to express an opinion on the Data Processor's description in section 3 and on the design and operating effectiveness of the controls related to the control objectives stated in the description, based on our procedures.

We conducted our engagement in accordance with the International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information ". That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed and operating effectively.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

An assurance engagement to report on the description, design and operating effectiveness of controls at a Data Processor involves performing procedures to obtain evidence about the disclosures in the Data Processor's description and about the design and operating effectiveness of the 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 suitability of the criteria specified by the Data Processor and described 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 Data Processor

The Data Processor's description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the use of the .legal Compliance Platform, that each individual data controller may consider important in their own environment. Also, because of their nature, controls at a Data Processor may not prevent or detect all breaches of the personal data security. Furthermore, the projection of any evaluation of the operating effectiveness of controls to future periods is subject to the risk that controls at a data processor 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 Data Processor's statement in section 2. In our opinion, in all material respects:

a. The description presents fairly the .legal Compliance Platform and the related technical and organisational measures and other controls, relating to processing and protection of personal data in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act, as designed and implemented for the period 1 November 2025 to 31 October 2026

b. The technical and organisational measures and other controls, relating to the control objectives stated in the description were appropriately designed for the period 1 November 2025 to 31 October 2026.

c. The technical and organisational measures and other 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 Test of Controls

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

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

Intended Users and Purpose

This report is intended solely for data controllers who have used the .legal Compliance Platform, and who have a sufficient understanding to consider it along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves when assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Copenhagen, 20 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: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

2. .LEGAL'S STATEMENT

.legal A/S processes personal data in relation to the .legal Compliance Platform to our customers, who are Data Controllers according to the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation) and the Danish Act on Supplementary Provisions (the Danish Data Protection Act).

The description has been prepared for Data Controllers who have used the .legal Compliance Platform, and who have a sufficient understanding to consider the description along with other information, including information about the technical and organisational measures and other controls operated by the data controllers themselves in assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

.legal A/S uses sub-processors. These sub-processors' 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 in section 3 fairly presents the .legal Compliance Platform and the related technical and organisational measures and other controls for the period 1 November 2025 to 31 October 2026. The criteria used in making this statement were that the accompanying description:

1. Presents the .legal Compliance Platform, and how the related technical and organisational measures and other controls were designed and implemented, including:
    - The types of services provided, including the type of personal data processed.
    - The processes in both IT systems and business procedures applied to process personal data and, if necessary, correct and delete personal data as well as limiting the processing of personal data.
    - The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the data controller.
    - 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 ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation.
    - 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.
    - The controls that we, with reference to the delimitation of the .legal Compliance Platform would have been designed and implemented by the data controllers, and which, if necessary to achieve the control objectives, are identified in the description.
    - The other aspects of the control environment, risk assessment process, information systems and communication, control activities and monitoring controls that are relevant to the processing of personal data.

2. Includes relevant information on changes in the .legal Compliance Platform and the related technical and organisational measures and other controls throughout the period.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

3. Does not omit or distort information relevant to the scope of the .legal Compliance Platform and the related technical and organisational measures and other controls described while acknowledging that this description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of the .legal Compliance Platform that the individual data controllers might consider important in their environment.

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

1. The risks threatening achievement of the described control objectives 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 applied consistently as designed, including manual controls were performed by persons with appropriate competencies and rights, in the entire period from 1 November 2025 to 31 October 2026

.legal A/S confirms that appropriate technical and organisational measures and other controls were implemented and maintained to comply with the agreements with data controllers, good practices for the data processing of data and relevant requirements for Data Processors in accordance with the EU General Data Protection Regulation and the Danish Data Protection Act.

Aarhus, 20 November 2026

.legal A/S

Brian Østberg
CEO

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

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

GENERAL DESCRIPTION OF .LEGAL

.legal A/S (hereinafter ".legal") is a Danish-founded company located in Aarhus. .legal develops and provides a Software-as-a-Service (SaaS) solution called .legal Compliance Platform (hereinafter "The Platform" or "the system"). to support legal and compliance work within both private and public organisations.

It is .legal's objectives, that The Platform are ensuring a solid and trustworthy foundation, both in terms of service and security. This report is part of our endeavour in making a set of policies, processes, and procedures, which helps .legal ensure the interaction with .legal's customers and their data, takes place in the most secure manner, and complies with applicable legislation.

This description is prepared for the purpose of reporting on the IT general controls that The Platform applies to support and safeguard provision of IT operations to its customers. The description focuses on business-related control objectives and processes implemented to safeguard The Platform provision of IT operations.

DESCRIPTION OF THE.LEGAL COMPLIANCE PLATFORM AND PROCESSING OF PERSONAL DATA

The .legal Compliance Platform 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.

Use of hosting centre:
.legal uses sub-processors for delivering the services. Microsoft Azure provides the overall IT platform for .legal Compliance Platform, where data is stored in Azure Storage and Azure SQL in European data centres.

Further, .legal uses Hetzner Online GmbH in Germany for the storage of offline Azure backups.

How data is used
.legal is processing personal data on behalf of .legal's costumers, when the costumers use The Platform according to their purpose. .legal has entered a data processing agreement which regulates the processing. The types of personal data processed by .legal is non-sensitive personal data which is information such as name, e-mail, phone number and identification.

.legal advises the data controller expressly that The Platform are not designed to process sensitive or other confidential data and the processor cannot take into account how the data controller uses The Platform to process personal data, including what types of personal data the data controller processes when using The Platform other than described in Data Processor Agreement.

.legal is processing, using and collecting personal data from the data controller/the costumer to operate effectively and provide The Platform. .legal will process personal data as necessary to perform and provide The Platform, in accordance with the agreement made with the data controller in the data processing agreement. The data processing instructions regarding purpose and subject matter are therefore to process data to provide and improve The Platform, which .legal offers and to perform essential business operations related to The Platform. This includes operation, maintaining and improving The Platform and providing customer service.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

GENERAL DESCRIPTION OF .LEGAL'S ORGANISATION

.legal is a legaltech company, which with its employees specialised in the design and development of digital solutions and cooperation with Bech-Bruun, combines technological possibilities with specific legal knowledge. .legal is organised with an administration department, a sales department, a development department, and an operations and support department.

MANAGEMENT OF PERSONAL DATA SECURITY

The Administration Department manages .legal's personal data security in relation to the processing that .legal handles on behalf of its customers, including the conclusion of data processing agreements, the response to requests from the data controller, notification of personal data breaches, and compliance with internal policies and procedures.

.legal has set up requirements for establishment, implementation, maintenance and current improvement of an ISMS, so that this is managing the processing of personal data. This is supported by agreements with the data controllers in which relevant requirements for data processors according to the General Data Protection Regulation and the Danish Data Protection Act are described.

The technical and organisational measures and other controls for protection of personal data are designed according to risk assessments and are implemented to ensure confidentiality, integrity, and accessibility as well as compliance with applicable data protection legislation. Security measures and controls are as far as possible automated and technically supported by IT systems.

The management of the personal data security and technical and organisational measures and other controls are organised in the following main areas for which control objectives and control activities have been defined:

ISO 27001	Control activities	GDPR article
Risk assessment	• 4.1.1 Risk assessment	• Art. 28(3)(c)
A.5: Information security policies	• 5.1.1 Policies for information security • 5.1.2 Review of policies for information security	• Art. 28(1)
A.6: Organisation of information security	• 6.1.1 Roles and responsibilities • 6.1.2 Remote workplaces and mobile equipment	• Art. 28(1) • Art. 28(3)(c)
A.7: Human resource security	• 7.1.1 Before employment • 7.1.2 During employment • 7.1.3 Non-disclosure and confidentiality agreements • 7.1.4 Resignation of employment	• Art. 28(1) • Art. 28(3)(b)
A.8: Asset management	• 8.1.1 Record of categories of processing activities • 8.1.2 Classification of information	• Art. 30(2), (3) & (4)
A.9: Access management	• 9.1.1 Policy for access management • 9.1.2 Allocation of user rights • 9.1.3 Management of privileged access rights • 9.1.4 Management and use of passwords	• Art. 28(3)(c)
A.10: Cryptography	• 10.1.1 Encryption	• Art. 28(3)(c)
A.11: Physical and environmental security	• 11.1.1 Physical perimeter safety guarding in office • 11.1.2 Clean desk and screen saver	• Art. 28(3)(c)
A.12: Operations security	• 12.1.1 Backup of information – customers' data • 12.1.2 Incident logging • 12.1.3 Administrator and operator logs • 12.1.4 Vulnerability management	• Art. 28(3)(c)
A.13: Communication security	• 13.1.1 Policies and procedures for transfer of information	• Art. 28(3)(c)

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

ISO 27001	Control activities	GDPR article
A.14: Acquisition, development, and maintenance of systems	• 14.1.1 Development and maintenance of systems	• Art. 25
A.15: Supplier relationships	• 15.1.1 Agreements with sub-processors • 15.1.2 Approval of sub-processors • 15.1.3 Changes to approved sub-processors. • 15.1.4 Control with sub-processor	• Art. 28(2) & (4)
A.16: Information security incident management	• 16.1.1 Handling of information security incidents • 16.1.2 Reporting of information privacy information incidents	• Art. 33(2)
A.17: Information security aspects of disaster recovery, contingency and restore management	• 17.1.1 Implementation of information security continuity • 17.1.2 Verify, review, and evaluate the information security continuity	• Art. 28(3)(c)
A.18: Compliance	• 18.1.1 Privacy and protection of personally identifiable information • 18.1.2 Instruction for processing of personal data • 18.1.3 Assistance to the data controller • 18.1.4 Deletion and return of customers data. • 18.1.5 Independent review of controls	• Art. 28(3)(a), (c), (e)-(h) • Art. 29 • Art. 32(4) • Art. 28(10)

RISK MANAGEMENT OF THE .LEGAL COMPLIANCE PLATFORM

Annual risk assessment

The Executive Board of .legal conducts a risk assessment at least once a year. The likelihood and consequence of the threats are reassessed based on the information existing at the present time. This reflects, in combination, the threat level. When the threat level has been determined, it is assessed to which extent the security environment considers the relevant threat level, and it can be deduced from here how high the current remaining risk is. The risk assessment exposes the likelihood and consequences of incidents which can threaten personal data security and thus, the interests or fundamental rights and freedoms of the data subject, including random, intentional, and unintentional incidents. The risks considering are related to the accidental or unlawful destruction, loss or alteration of personal data, or unauthorised disclosure or access to personal data transmitted, stored, or otherwise processed. The risk assessment takes the state of art and the cost of implementation into account.

Risk assessments are based on the implementation guidelines in the international standard ISO 27002.

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 ensures 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.

This report includes solely controls and control objectives for processes and controls that are managed by .legal and, thus, it does not include controls or control objectives that are managed by sub-organisations.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

CONTROL FRAMEWORK, CONTROL STRUCTURE AND CRITERIA FOR CONTROL IMPLEMENTATION

.legals information security is defined on the basis of the objective to provide dedicated IT outsourcing and high-quality infrastructure solutions, including stability and security.

The determination of criteria and scope of control implementation at .legal is based on the ISO 27002:2013 framework for management of information security. The following control areas in ISO 27002 were assessed:

- A.5. Information security policy
- A.6. Organisation of information security
- A.7. Human resource security
- A.8. Asset management
- A.9. Access management
- A.10. Cryptography
- A.11. Physical and environmental security
- A.12. Operations security
- A.13. Communications security
- A.14. Acquisition, development, and maintenance of systems
- A.15. Supplier relationships
- A.16. Information security incident management
- A.17. Information security aspects of contingency, disaster recovery, and restore
- A.18. Compliance

Implemented control environment
The implemented controls are based on the services provided by .legal's customers and include control areas and control activities within operation and hosting. All of the above areas are described in detail in the following in separate paragraphs, and the described control objectives and controls for those areas in the paragraph on control objectives, controls, tests and result of tests are an integral part of the description.

A.5 Information security policy

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

The IT security policy is reassessed annually by Management.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.6 Organisation of information security

IT security manager
.legal has dedicated an security officer with responsibility of organisational and system security, complying with personal data protection, internally and in relation to customer data.

Remote workplaces and mobile equipment
.legal staff manual sets out guidelines for use of mobile equipment outside the company. Only equipment that complies with the service's security policy regarding protection against malicious code is allowed.

A.7 Human resource security

.legal has implemented controls to ensure that employees are qualified and conscious of their tasks and responsibilities in relation to information security.

Management's responsibility
With respect to employees, they commit themselves, upon employment, to adhere to the company's policies, including the security policy.

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.

Awareness training
Employees at .legal are informed about how to handle personally identifiable data through the IT Security Policy and via yearly awareness campaigns.

Obligations relating to departure:
General employment conditions, including conditions in relation to end of employment, are described in the employee's employment contract. Moreover, there is a formal procedure for departure that must be followed by the immediate manager, the CEO has the ultimate responsibility in this respect. This procedure includes the return of all received material to .legal, when the contract ends and the closing of rights, ensuring that the employee does not have any physical or digital access when the employment ends. In addition to common employment law provisions, the employment contract specifies sanctions. The workplace is subject to .legal's security routines which must not be broken. If this happens, it is considered a breach of the employment contract.

Return of equipment
All employees are to return all received material when the employment contract ends. This is done through a workflow placed at the HR department.

Closing of access rights
.legal's formal offboarding procedures ensure that all rights and physical access are withdrawn when employment ends. Accesses are reviewed annually.

A.8 Asset management

.legal has implemented controls to ensure achievement and maintenance of suitable protection of the organisation's equipment.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

Record of categories of processing activities as a data processor
A record has been prepared of all data processing agreements and processing of personally identifiable data, which is administered in .legal. The record is stored electronically and only persons with a functional need to have access have rights and access hereto.

All processing of data follows the guidelines set out in the IT Security Policy.

The guidelines for processing of personally identifiable data comply with the guidelines set out in the IT Security Policy.

A.9 Access management
.legal has implemented controls to ensure that access to systems and data is granted through a documented process in accordance with a relevant work-related need and is closed down when the relevant access is no longer necessary.

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 procedure
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 Executive Board. Employees with privileged access must always use 2-factor authentication.

Reassessment of user access rights
All accesses and rights are reviewed periodically by the IT Security Manager.

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

A.10 Cryptography
Encryption
The system is a purely 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.

Data is encrypted when stored in the data centre and automatically decrypted when accessed.

A.11 Physical and environment security
.legal has implemented measures to ensure that office IT equipment and other relevant assets are properly protected against unauthorised physical access and damage caused by environmental incidents.

Physical security of premises and machines

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

.legal's premises are locked at all times. Additionally, all .legal employees have met the requirements for automatic screensaver and adhere to the clean desk policy.

.legal does not host solutions itself, which means that physical security also pertains to the hosting partner, Microsoft Azure. We refer to a separate SOC 2 report for the description of controls, their design, and operational effectiveness in relation to Microsoft Azure, as described in A.15 regarding supplier relationship.

Physical access control
.legal premises have access control in the form of a required personal code and a systems key to ensure that only authorised staff have access.

A.12 Operational reliability

Secure hosting
Microsoft Azure is the overall IT platform for the system.

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

The system is 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.

Data redundancy
Production databases are actively geo-replicated to secondary databases located in Northern 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 system.

The primary data location for the production environment for documents is Western Europe. At the location, data is stored in 3 different copies. In the event of a crash, the Azure platform setup automatically switches to one of the redundant copies. The system uses Geo Redundant Storage (GRS)

Management of capacity
Monitoring of capacity has been implemented in relation to internet, network, servers, disk space and log files. .legal receives reporting from Microsoft Azure and other tools which are used in the planning of purchase of additional capacity. Data from monitoring are registered and evaluated currently.

Data backup
The platform runs continuous backup that allows point-in-time restore. It is possible to restore a maximum of 30 days back in time.

For all services backup is replicated multiple times (within the EU) to ensure a reliable backup solution.

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

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

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.

Logging, Monitoring and Alerts
System events are logged to a central system log, so that 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. Incidents concerning breach in relation to the processing of personal data are always marked, so that they can rapidly be identified and dealt with by .legals management.

Vulnerability management
legal performs regular vulnerability scans to identify vulnerabilities in the system. Identified vulnerabilities are assessed, and appropriate security measures are implemented to mitigate the risks associated with such vulnerabilities.

A.13 Communications 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.

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

A.14 Acquisition, development, and maintenance of systems

.legal has implemented controls to ensure that servers and relevant infrastructure components are updated and maintained as necessary and that this is done in a structured process.

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 system we work with.

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

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

- Structured process
    - 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.
- Automated quality assurance
    - Version-controlled code

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

  - Continuous integration which continuously builds the code to ensure integrity
  - Automated tests that run continuously to minimise regression errors
  - Automated deployment pipelines which mean that we can safely and with high traceability deploy new code for tests and production environments.
- Development, test, and production environment
  - Dedicated development, testing, and production environments to be able to ensure quality on several levels before new code reaches the production environment.
- Monitoring and alerting
  - Our environments are monitored so that we can ensure high uptime and receive alarms about any errors or vulnerabilities as quickly as possible.

A.15 Supplier relationships

Supplier agreements

.legal uses sub-suppliers of operation of system infrastructure including backup and AI service provider and handling support tickets.

.legal has established an overview of sub-processors, indicating the sub-processor's name, CVR number, address, and description of the processing. Below is an overview of the sub-processors used:

Sub-processor	Address	Location for data processing	Description of processing
Microsoft Ireland Operations Ltd (Microsoft Azure)	Microsoft Plc. Leopardstown South County Business Park, Dublin 18, Ireland.	Data is stored in European data centres (Microsoft Azure).	Operation of system infrastructure including application servers, backup, databases and other data storage components.
HubSpot Ireland Ltd.	HubSpot House, 1 Sir John Rogerson's Quay, Dublin, Ireland.	Data is stored in European data centres.	Handling support tickets and inquiries in relation to the use of the Services.
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen, Germany	Data is stored in European data centres.	Hosting and backup services.
Mistral AI	15 Rue des Halles, 75001 Paris, France.	Data is stored in European data centres by default.	AI service provider. Zero Data Retention (ZDR) is enabled, ensuring that no input or output data is retained or used for model training.

Hetzner Online GmbH was engaged as a sub-processor during the assurance period. Hetzner Online GmbH is responsible for the storage of offline Azure backups.

Mistral AI was engaged as a sub-processor during the assurance period. Mistral AI provides AI support within the .legals Compliance platform to the extent that customers make use of AI-enabled functionality.

Supplier agreements are established with all customers who use the system. When engaging sub-processors, .legal compares its security requirements with the security measures described and implemented by the relevant sub-processor to assess whether an appropriate and equivalent level of security is maintained.

To the extent that .legal's sub-suppliers store or otherwise manage personal data on behalf of .legal customers in the course of the sub-supplier's provision of services to .legal, the sub-supplier acts as data processor

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

solely according to instructions from .legal and .legal's customer. Thus, .legal's sub-suppliers commit themselves to take the necessary technical and organisational security measures to ensure that personal data are not accidentally or illegally destroyed, lost or impaired, and that they are not disclosed to unauthorised parties, misused or otherwise processed in violation of data protection legislation.

Supplier control

.legal performs an annual security check of third-party service providers that are part of the overall Compliance platform.

EU-U.S. Data Privacy Framework

.legal primarily use EU based sub-processors. .legal does not use sub-processors in unsafe third countries; sub-processors from the US are only used if the company is registered as an active participant under the framework. Furthermore, .legal ensures to always stay updated on whether sub-processors for .legal are registered as active participants regarding the EU-U.S. Data Privacy Framework.

Any sub-processors that are not certified under the framework are subject to a transfer basis (e.g., the EU Commission's Standard Contractual Clauses) and a prior TIA (Transfer Impact Assessment).

A.16 Information security incident management

All safety and personal data incidents or observed weaknesses are reported to the security officer. As soon as a security incident or vulnerability is reported, the following activities are initiated to stop and contain the incident:

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 detailed as possible, including as a minimum:

2.1. When the incident took place
2.2. What the incident was actually about
2.3. Who reported the incident

3. The incident is then analysed with a view to the following:

3.1. Determine how extensive the incident is
3.2. Which customers are affected
3.3. 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 prioritised 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.

Procedures have been implemented based on the data processing agreements with our customers. This is done to ensure correct management of security incidents within the agreed frame. A template has also been implemented to be used for reporting of breach of the Regulation to the data controller which ensures that all necessary information is provided, for the purpose of further consideration on the part of the data controller.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

Specifically on the handling of personal data breaches when .legal A/S is the data processor

.legal A/S shall notify the data controller of personal data breaches in accordance with Article 33(2) of the GDPR and, where possible, within 24 hours of .legal A/S becoming aware of the personal data breach, to enable the data controller to comply with its obligation to notify the supervisory authorities in accordance with Article 33(1) of the GDPR.

A.17 Information security aspects of contingency, disaster recovery and restore

.legal has developed contingency plans to maintain or restore operations and ensure access to data at the required level and within acceptable time after failure or outage of critical business processes.

Roles and responsibilities are defined in the contingency plan. The operations manager and the contingency managers are responsible for different areas.

.legal assesses risks regularly, and the contingency plan is updated to the existing risk exposure at least once a year. Furthermore, the contingency plan is tested annually to ensure that it is applicable, sufficient, and effective.

A.18 Compliance with customer requirements and regulatory and public authority requirements

.legal has implemented controls to ensure that all relevant customer requirements and regulatory and public authority requirements are complied with.

Privacy and protection of personal data

.legal stores and processes personal data as instructed by the customer for the customers who have entered data processing agreements with us.

Signing of data processing agreements

.legal has implemented procedures for entering data processing agreements which ensures that the CEO of .legal in relation to the contract with the customers signs a data processing agreement which describes the terms for processing of personal data on behalf of the data controller. .legal uses a template for data processing agreements in accordance with the services delivered, including information on the use of sub-processors. The data processing agreements are signed digitally and stored electronically.

Instruction for processing of personal data

.legal has implemented procedures which ensure that .legal acts according to instructions by the data controller in the data processing agreement. The instructions are maintained in the company's classification system, which instructs the employees on how the processing of personal data is to be performed, including the persons at the data controller that can give binding instructions to .legal. The instructions ensure also that .legal informs the data controller when the data controller's instructions are contrary to the data protection legislation.

Assistance to the data controller

.legal has implemented instructions which ensure that .legal can assist the data controller in complying with his obligations to respond to requests for exercising of the data subjects' rights.

.legal has implemented instructions which ensure that .legal can assist the data controller in complying with the obligations in article 32 on security of processing, article 33 on reporting and notification of breach of the personal data security, and articles 34 to 36 on impact assessments.

.legal has implemented instructions which ensure that .legal can make all information required to prove compliance with the requirements for data processors to the data controller available. .legal also enables and contributes to audits, including inspections, made by the data controller or other parties authorised by the data controller.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

Deletion and return of customer's data
.legal has implemented instructions which ensure that personal data are deleted or returned according to the data controller's instruction when the processing of personal data ends on expiry of the contract with the data controller. The customer's personal data remains in the company's classification system in 30 days or until the customer finally approves the frames for off-boarding, including deletion of data and the relevant circumstances.

Independent review of controls
Compliance with the EU General Data Protection Regulation is confirmed by annually obtaining an independent auditor's report which supports the company's compliance with the Regulation.

Once a year, the .legal A/S Executive Board asks the law firm Bech-Bruun to assess whether there have been changes to the legislation in a way that changes the security policy and/or the system. The result of the request is noted at the board meeting and any resulting changes are implemented.

CHANGES DURING THE PERIOD FROM 1 NOVEMBER 2025 TO 31 OCTOBER 2026.

.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.
- .legal has implemented AI functionality to support the preparation and generation of documents within the platform.

COMPLEMENTARY CONTROLS FOR .LEGAL'S CUSTOMERS

The data controller is under an obligation to implement the following technical and organisational measures and other controls to achieve the control objectives and to comply with the data protection legislation:

- It is the responsibility of the data controller to ensure that the administrators' use of the platforms and the processing of personal data carried out in the system comply with the data protection legislation.
- The data controller manages the user rights in the platforms, including to whom administrator access is allocated and which rights are allocated to the individual administrators.
- The platforms are not designed to process sensitive personal data in documents and free-text fields, and it is the data controller's responsibility to ensure that such personal data are not entered into or uploaded to the platform.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND THE RESULT OF TESTS

Objective and scope

We conducted our engagement in accordance with ISAE 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information.

BDO has inspected procedures to obtain evidence of the information in the .legal's description of .legal Compliance Platform, the design and operating effectiveness of the relating technical and organisational measures and other controls. The procedures selected depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not appropriately designed or operating effectively.

BDO's test of the design and the operating effectiveness of the relating technical and organisational measures and other controls and their implementation has included the control objectives and related the control objectives and related control activities selected by .legal A/S, and which are described in the check form below.

In the test form, BDO has described the tests carried out which were assessed necessary to obtain reasonable assurance that the stated control objectives were achieved, and that related controls were appropriately designed and operated effectively for the period 1 November 2025 to 31 October 2026.

Test procedures

Test of the design of the relating technical and organisational measures and other controls and their implementation was performed by inquiries, inspection, observation, and re-performance.

Type	Description
Inquiry	Inquiries of relevant personnel at .legal have been performed for all significant control activities. The purpose of the inquiries 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, i.e., 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 has been 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 support administration services provided by HubSpot Ireland Ltd, 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 May 2025 to 30 April 2026, as well as a Bridge Letter dated 30 June 2026.

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

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

For the service provided by Mistral AI as AI service provider we have received an ISO 27001:2022 certificate valid from 12. September 2024 to 11. September 2027.

These sub-processor's and service organisation's relevant control objectives and related controls are not included in .legal A/S description of the .legal Compliance Platform and relevant controls related to operation of the .legal Compliance Platform. Thus, we have solely assessed the reports and tested the controls at .legal A/S, which ensures appropriate supervision of the sub-processor's compliance with the data processing agreement made between the sub processor and the data processor and compliance with the General Data Protection Regulation and the Danish Data Protection Act.

Result of test

The results of our tests, including any exceptions noted, are set out in the tables below

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective, or
- Technical and organisational measures and other controls related to a control objective are not suitably designed and implemented or did not operate effectively throughout the period.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.4: Risk assessment

4.1 Control Objective

- *To ensure that the data processor carries out an annual risk assessment in relation to the consequences for the data subjects which forms basis for the technical and organisational measures GDPR art. 28, paragraph 3,*

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 carried out that provides the basis for data protection reasoned implementations.	We made inquiries of relevant personnel at .legal A/S. We have inspected that the data processor has prepared a procedure for annual review of risk assessments. We have inspected documentation for that the management have approved the risk assessments. We have inspected that prepared risk assessments form the basis for data protection reasoned implementations. We have inspected that the risk assessment has been updated within the assurance period.	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.5: Information security policies

5.1 Control Objective

- *To provide guidelines for and support information security and data protection in accordance with business requirements and relevant laws and regulations. GDPR art. 28, paragraph 1, art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
5.1.1 Policies for information security and Privacy ▶ 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 that the data processor has a management-approved IT security policy containing a policy for information security and personal data protection. On a sample basis, we inspected evidence that employees have signed to confirm that they had read and understood the data processor's IT security and data protection policies.	No exceptions noted.
5.1.2 Review of policies for information security and data privacy ▶ The data processor has implemented an annual plan of controls which ensures periodical review of the information security policy and privacy policy. ▶ A written policy's has been drawn up which is reassessed annually. ▶ The information policy's is updated and approved by Management.	We made inquiries of relevant personnel at .legal A/S. We have inspected that the data processor has set up a procedure for annual review and approval of the IT security policy and privacy policy. We have inspected that policies are reviewed annually. We have inspected that the policy's has been reviewed, updated and approved by the management team within the assurance period.	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.6: Organisation of information security

6.1 Control Objective

- *To establish a management basis for initiating and managing the implementation and operation of information security and data protection in the organisation. GDPR art. 28, paragraph 1*
- *To secure remote workplaces and the use of mobile equipment. GDPR art. 28, paragraph 3.*

Control Activity	Test performed by BDO	Result of test
6.1.1 Roles and responsibilities ▶ The responsibility for the information security lies with Management. ▶ The data processor has designated a contact point for the data controller regarding the processing of personal data.	We made inquiries of relevant personnel at .legal A/S. We have inspected that the data processor in their IT security policy has placed the responsibility for information security. On a sample basis we have inspected the data processor agreements are accepted doing the signing the specified contact information.	No exceptions noted.
6.1.2 Remote workplaces and mobile equipment ▶ The data processor has implemented a policy and supported security measures to manage the risks of personal data arising from the use of mobile devices.	We made inquiries of relevant personnel at .legal A/S. We have inspected that the data processors IT security policy and observed that they have guidelines for mobile equipment. We have by sampling inspected that security measures are in place on mobile workstations.	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.7: Human resource security

7.1 Control Objective

- *To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles they are intended. GDPR art. 28, paragraph 1, art. 28, paragraph 3.*
- *To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR art. 28, paragraph 1, art. 28, paragraph 3.*
- *To protect the organisation's interests as part of the change or termination of the employment relationship. GDPR art. 28, paragraph 3.*

Control Activity	Test performed by BDO	Result of test
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 data processor'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.
7.1.2 During employment ▶ Employees at the data processor are currently informed of information security matters and potential threats in relation to their tasks. ▶ Employees at the data processor declare upon employment that they have read and accept the information security policy. ▶ Awareness campaigns towards the data processor employees are performed yearly to ensure continuous focus on data protection and security.	We made inquiries of relevant personnel at .legal A/S. We have inspected documentation for that all employees have signed that they have read and understood the data processor's IT security policy. We have inspected that the data processor has a procedure to ensure that there is awareness in data protection and security. On a sample basis we have inspected internal GDPR awareness training has been held within the assurance period.	No exceptions noted.
7.1.3 Non-disclosure and confidentiality agreements ▶ All employees working with confidential data – including personal data – have signed a non-disclosure agreement. ▶ The employees are bound by a confidentiality agreement both internally and towards the customers.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's employment contract template and observed that it contains requirements for confidentiality during and after employment applicable to everything concerning their work. On a sample basis we have for employees inspected documentation for that requirement for confidentiality during and	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.7: Human resource security

7.1 Control Objective

- *To ensure that employees and contracting parties understand their responsibilities and are suitable for the roles they are intended. GDPR art. 28, paragraph 1, art. 28, paragraph 3.*
- *To ensure that employees and contracting parties are aware of and meet their information security responsibilities. GDPR art. 28, paragraph 1, art. 28, paragraph 3.*
- *To protect the organisation's interests as part of the change or termination of the employment relationship. GDPR art. 28, paragraph 3.*

Control Activity	Test performed by BDO	Result of test
	after employment applicable to everything related to their work have been signed.	
7.1.4 Resignation of employment ▶ Upon resignation or change of the employment, accesses and rights are withdrawn or changed in accordance with the functional need in this respect. ▶ Upon resignation of the employment, equipment received by the leaving employee is returned. ▶ The data processor has defined rules in their employment contracts concerning off boarding.	We made inquiries of relevant personnel at .legal A/S. We have inspected that the data processor has a procedure for off boarding, which ensures that all accesses are closed, and material is handed over. 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.	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.8: Asset management

8.1 Control Objective

- *To identify the organisation's assets and define appropriate responsibilities for its protection. GDPR art. 30, paragraph 2, art. 30, paragraph 3.*
- *To ensure adequate protection of information and personal data that is in relation to the importance of the information and personal data for the organisation. GDPR art. 30, paragraph 3, art. 30, paragraph 4.*
- *To prevent unauthorised disclosure, modification, removal or destruction of information and personal data stored on media. GDPR art. 28, paragraph 3.*

Control Activity	Test performed by BDO	Result of test
8.1.1 Record of categories of processing activities ▶ The data processor has prepared a record of processing activities, which is kept updated occasionally – at least once a year. ▶ The record is kept electronically. ▶ The data processor makes the record available to the supervisory authority upon request.	We made inquiries of relevant personnel at .legal A/S. We have inspected that the data processor has prepared a record of processing activities as processor. We observed that the data processor has prepared a record of categories of processing activities on behalf of the customers. Furthermore, we have observed that the record is stored electronically and includes the elements required according to General Data Protection Regulation article 30(2). We have been informed that General Data Protection Regulation article 30(2) records is made available to the supervisory authority upon request. Upon request, we have been informed that there have not been any requests regarding the data processor's records of processing activities from the supervisory authorities within the assurance period.	Upon request, we have been informed that there have not been any requests regarding the data processor's records of processing activities from the supervisory authorities within the assurance period. Therefore, we cannot test control implementation and operational effectiveness. No exceptions noted.
8.1.2 Classification of information ▶ The different information handled and managed by the data processor has been identified and separated into categories reflecting the consequences if the information and data privacy was compromised.	We made inquiries of relevant personnel at .legal A/S. We have inspected that the various information handled and managed by the organisation have been identified and divided into categories that reflect the consequences if the information and data protection were compromised.	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.9: Access management

9.1 Control Objective

- *To restrict access to information and personal data, including information and personal data processing facilities. GDPR art. 28, paragraph 3.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR art. 28, paragraph 3.*
- *To make users responsible for securing their authentication information. GDPR art. 28, paragraph 3.*
- *To prevent unauthorised access to systems and applications. GDPR art. 28, paragraph 3.*

Control Activity	Test performed by BDO	Result of test
9.1.1 Policy for access management ▶ Processes and procedures have been adopted to manage access and restrictions to systems and data based on business and functional requirements. ▶ All access and changes to access to systems and data follow the adopted processes and procedures.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's procedure for access control and observed that rights must be granted according to a work-related need. We inspected the rights granted to employee with access to data and confirmed that the appropriate rights were granted according to the procedure and their work-related need. We have inspected that leaving employees during the assurance period have been removed as a user.	No exceptions noted.
9.1.2 Allocation of user rights ▶ The data processor has a matrix of users with access to systems with personal data and their job function. ▶ User rights are granted based on a work-related need. ▶ All accesses and rights are reviewed periodically by the management.	We made inquiries of relevant personnel at .legal A/S. We have inspected that the data processor has a matrix of user rights for the systems and observed that it is only employees with the right "global administrators" which can access personal data. We have reviewed the overview with the data processor and found that only employees with a work-related need can access personal data in the systems. We have inspected documentation on periodic review of users and associated rights and observed it were conducted within the assurance period.	No exceptions noted.
9.1.3 Management of privileged access rights ▶ The data processor has implemented granting of administrative access to entities according to the functional need which is authorised.	We made inquiries of relevant personnel at .legal A/S. We have inspected the procedure for allocating administrative rights in the system and observed that this must be done after approval by a member of management.	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: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.9: Access management

9.1 Control Objective

- *To restrict access to information and personal data, including information and personal data processing facilities. GDPR art. 28, paragraph 3.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services. GDPR art. 28, paragraph 3.*
- *To make users responsible for securing their authentication information. GDPR art. 28, paragraph 3.*
- *To prevent unauthorised access to systems and applications. GDPR art. 28, paragraph 3.*

Control Activity	Test performed by BDO	Result of test
▶ The data processor has implemented logging of accesses with privileged accounts (administrative rights).	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 have inspected that the data processor has implemented logging of accesses with privileged accounts.	No exceptions noted. .
9.1.4 Management and use of passwords ▶ The data processor has implemented a process and rules for granting and management of passwords. ▶ The data processor has implemented rules for establishment of passwords which must be followed by all employees. ▶ 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. ▶ 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 IT security policy and observed that all employees are required to use the company-approved password manager. We inspected the data processer'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. 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. We have inspected the configuration for automatic antivirus scanning of documents in document storage.	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.10: Cryptography		
10.1 Control Objective ▶ *To ensure the correct and effective use of cryptography to protect the confidentiality, authenticity and / or integrity of information and personal data. GDPR art. 28, paragraph 3.*		
Control Activity	**Test performed by BDO**	**Result of test**
10.1.1 Encryption ▶ The data processor uses an up-to-date encryption policy to protect data.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's encryption policy and observed that requirements of encryption are defined. We have inspected system configuration an observed that SHA-2 SSL certificate with a minimum of 2048bit encryption is used. Further, we have inspected that Azure also uses data encryption. On a sample basis, we inspected the encryption settings on employees' workstations and observed that encryption was enabled.	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.11: Physical and environmental security

11.1 Control Objective

- *To prevent unauthorised physical access to, and damage/disruption of the organisation's information and personal data, including information- and personal data processing facilities. GDPR art. 28, paragraph 3.*
- *To avoid loss, damage, theft or compromise of assets and disruptions in the organisation. GDPR art. 28, paragraph 3.*

Control Activity	Test performed by BDO	Result of test
11.1.1 Physical perimeter safety guarding in office ▶ The established physical perimeter safety guarding agrees with the adopted security requirements.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processer's procedure for physical security and observed that physical security of the control must be established. We have inspected the office in Aarhus and observed that a lock and alarm have been set up for both the office and the building. We have also inspected an overview of physical access via key to the location. On a sample basis we have inspected leaving employees returning of keys to office locations.	No exceptions noted.
11.1.2 Clean desk and screen saver ▶ Workstations have automatic screen saver, and employees are instructed to activate screen saver when leaving the workstation. ▶ Employees are instructed to keep a clean desk.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's policy for clean desk and automatic screen saver. On a sample basis we have inspected workstation configuration and observed that screen saver on the employees' workstations is in place. During our visit we have inspected office location and observed that clean desk is in place.	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.12: Operations security

12.1 Control Objective

- *To ensure proper and safe operation of information and data processing facilities. GDPR Art. 25, Art. 28, paragraph 3.*
- *To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR Art. 28, paragraph 3.*
- *To protect against data loss. GDPR Art. 28, paragraph 3.*
- *To record events and provide evidence. GDPR Art. 33, paragraph 2.*
- *To prevent technical vulnerabilities being exploited. GDPR Art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
12.1.1 Backup of information – customers' data ▶ Backup of data is taken for all customers with backup agreements, some via sub-processors and others internally in the data processor. ▶ 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 have inspected the data processor's backup procedure in Azure. We have observed that backup is performed in according with the procedure. We have inspected the configuration of automated monitoring of backup execution. We have inspected documentation for restore test of services has been performed within the assurance period.	No exceptions noted.
12.1.2 Incident logging ▶ Recording and managing of all relevant incidents has been established. ▶ Monitoring of customers' servers has been established for the purpose of accessibility and systems errors. ▶ All incidents are logged in the Service Management System. ▶ Any incidents concerning personal data leaks or suspicion of leaks are marked separately to sort these cases from other incidents.	We made inquiries of relevant personnel at .legal A/S. We have inspected that logging has been established in Azure and that relevant events are logged. We have inspected that the data processor receives alerts and that relevant employees review and act upon these alerts. We have inspected that the data processor identifies and classifies personal data breaches and that a separate process has been established for handling personal data breaches.	No exceptions noted.
12.1.3 Administrator and operator logs ▶ Procedures are implemented to ensure that all activities performed by systems administrator or employees with administrative rights are recorded.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's formal guidelines for log management.	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.12: Operations security

12.1 Control Objective

- *To ensure proper and safe operation of information and data processing facilities. GDPR Art. 25, Art. 28, paragraph 3.*
- *To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR Art. 28, paragraph 3.*
- *To protect against data loss. GDPR Art. 28, paragraph 3.*
- *To record events and provide evidence. GDPR Art. 33, paragraph 2.*
- *To prevent technical vulnerabilities being exploited. GDPR Art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
	We have been informed upon request that all activity performed by administrators is logged. We have inspected that activity performed by administrators is logged.	
12.1.4 Vulnerability Management ▶ Vulnerability scans are conducted monthly. The result is documented. ▶ The Data Processor reviews the results and follows up on identified vulnerabilities. ▶ The Data Processor has documented their mitigation efforts of identified vulnerabilities	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's policy for vulnerability scanning and observed that vulnerability scans are performed monthly. We have inspected vulnerability scanning reports and observed that identified vulnerabilities are 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.	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.13: Communications security

13.1 Control Objective

- *To ensure protection of network information and personal data and supportive information and personal data processing facilities. GDPR art. 28, paragraph 3, point c.*
- *To maintain information security and data protection when transferring internally in an organisation and to an external entity. GDPR art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
13.1.1 Policies and procedures for transfer of information ▶ Communication between the browser and the rest of the system takes place via HTTPS (SHA-2 SSL certificate with a minimum of 2048bit encryption). ▶ 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 have inspected the data processor's encryption policy and observed that systems processing personal information as a minimum must be encrypted with a SHA-2 SSL certificate with a minimum 2048-bit encryption. We have inspected system configuration that the communication between the browser and the rest of the system takes place using a SHA-2, 2048-bit encryption. We have inspected documentation for private networks (Vnet).	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

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

14.1 Control Objective

- *To ensure that information security and data protection is an integral part of information systems throughout the life cycle. This also includes the requirements for information systems that provide public network services. GDPR art. 25.*
- *To ensure that information security and data protection is organised and implemented within the information systems development life cycle. GDPR art. 25.*
- *To ensure the protection of data used for testing. GDPR art. 25.*

Control Activity	Test performed by BDO	Result of test
14.1.1 Development and maintenance of systems ▶ Formal processes and procedures have been implemented for all changes made in .legal Compliance Platform. ▶ Development of .legal Compliance Platform is based on principle of privacy-by-design and privacy-by-default based on risk assessment. ▶ Development of .legal Compliance Platform is based on principles to reduce risk and vulnerabilities in the application. ▶ The data processor has separated IT environments into development, test and operating environments for the customers who require this. ▶ Generated test data is used in the development and test environment.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's development procedure and observed that changes to systems within the development life cycle must be managed using a formal change management procedure covering principle of privacy-by-design and privacy-by-default, vulnerabilities in application and all based on a risk assessment. On sample basis of changes within the assurance period, we have inspected that change management procedure is followed, so that all changes are tested and approved before they are deployed in production environments. Furthermore, we have inspected the branching configuration and observed that it is not possible for the developing programmer to push code into production without a code review from another developer. We have inspected that data processor has separated production-, development- and test environments. Furthermore, we have inspected that access to developing environments is compliant with the data processor's development procedure. We have inspected data used in the development and test environment and observed that data is constructed fake data. Real personal data is only stored in the production environment.	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.15: Supplier relationships

15.1 Control Objective

- *To ensure protection of the organisation's assets and personal data that suppliers have access to. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.*
- *To maintain an agreed level of information security, data protection and delivery of services under the supplier agreements. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.*

Control Activity	Test performed by BDO	Result of test
15.1.1 Supplier agreements ▶ Supplier agreements are established with all customers who use the systems. ▶ Any subcontractors must live up to the same level of security and as minimum comply with the same security policies as the data processor.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's supplier overview and observed that sub-processors are used for support services, hosting and operations, backup storage and the provision of AI services. We have inspected the data processor's data processing agreements with its sub-processors and observed that the agreements require the sub-processors to maintain at least the same level of security as that required by the data controllers of the data processor. We have inspected the data processing agreements and observed that only data centres located within the EU may be used. We have inspected documentation supporting compliance with this requirement. We have inspected that, in addition to the technical measures already implemented by .legal, the data processor has enabled Customer Lockbox for Microsoft Azure, requiring the data processor's approval before the sub-processor may access data. We have inspected that the two sub-processors, Microsoft and HubSpot, have self-certified under the EU-U.S. Data Privacy Framework.	No exceptions noted.
15.1.2 Approval of sub-processors ▶ The data processor uses only approved sub-processors.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's standard data processor agreement, and observed that the following sub-processors are specified: ▶ Microsoft Azure ▶ HubSpot	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.15: Supplier relationships

15.1 Control Objective

- *To ensure protection of the organisation's assets and personal data that suppliers have access to. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.*
- *To maintain an agreed level of information security, data protection and delivery of services under the supplier agreements. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.*

Control Activity	Test performed by BDO	Result of test
	▶ Hetzner Online ▶ Mistral AI We have inspected the data processor's supplier overview and observed that information regarding its sub-processors is included in the Terms of Service applicable to customers.	
15.1.3 Changes to approved sub-processors ▶ The data processor notifies the data controller when the sub-data processor is replaced in connection with general approval of the sub-data processor. ▶ The data controller can object to the replacement of a sub-processor.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's standard data processor agreement and observed that the data processor does not use other sub-processors without the approval of the data controllers. We have observed that agreements with two new sub-processors, Hetzner Online GmbH and Mistral AI, respectively, were entered into during the assurance period. We have inspected that the data controllers have been notified of the appointment of new sub-processors during the assurance period. Notifications of such changes are published on .legal's website. We have inspected that the data controller has the right to object to the replacement of a sub-processor.	No exceptions noted.
15.1.4 Control with sub-processor ▶ The data processor performs an annual security check of third-party service providers that are part of the overall system.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's procedure for supervising sub-processors and observed that the data processor annually checks that sub-processors' auditor's statements and certifications are satisfactory, based on the data processor's risk assessment. We have inspected the monitoring performed in respect of sub-processors and observed that relevant SOC 2 reports	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.15: Supplier relationships

15.1 Control Objective

- *To ensure protection of the organisation's assets and personal data that suppliers have access to. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.*
- *To maintain an agreed level of information security, data protection and delivery of services under the supplier agreements. GDPR Art. 28, paragraph 2, Art. 28, paragraph 3, point d, Art. 28, paragraph 4.*

Control Activity	Test performed by BDO	Result of test
	and other supporting documentation have been re-viewed.We have inspected that identified deviations have been assessed based on their associated risks, and that sup-plementary activities at the data-processer have been per-formed where deemed necessary.	

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.16: Information security incident management

16.1 Control Objective

- *To ensure a uniform and effective method of managing information security breaches and personal data breaches, including communication on security incidents and weaknesses. GDPR Art. 33, paragraph 2.*

Control Activity	Test performed by BDO	Result of test
16.1.1 Handling of privacy information incidents ▶ All privacy and it-security incidents are managed in Service Management System and in accordance with established procedures. ▶ The data processor has implemented procedures for documentation of all personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. ▶ Guidelines to reporting information security incidents have been implemented and communicated to the employees responsible for data protection in the data processor.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's procedure for breaches of personal data security and observed that the data processors security officer is responsible for the process in case of a breach of personal data security. Furthermore, we have observed that formal requirements for documentation and reporting in case of a breach of personal data security are described in their procedure and are stored in Service Management System. Upon request, we have been informed that there are no registered privacy or it-security breaches as data processor within the assurance period. Consequently, we have not been able to test the implementation and effectiveness of the procedure.	Upon request, we have been informed that there are no examples of breaches of personal data security within the assurance period. Therefore, we cannot test control implementation and operational effectiveness No exceptions noted.
16.1.2 Reporting of privacy information incidents ▶ Processes and procedures have been established for handling of security incidents to ensure a uniform and effective method of managing information security incidents, including communication of security incidents and weaknesses which are documented in Service Management System. ▶ Processes and procedures have been established to ensure recording and handling of security incidents by the right employee. ▶ Procedures have been implemented based on the data processing agreements with our customers to ensure handling of personal data and responding to security incidents within the agreed time frames.	We made inquiries of relevant personnel at .legal A/S. We have inspected that the data processor has a procedure for how personal data breaches are to be treated and documented, so that it is ensured that all affected data controllers and possibly supervisors are aware of the breach. We have inspected the data processors procedure for breaches of personal data security and observed that it is specified who is the leader of the Incident Response Team. Upon request, we have been informed that there are no examples of breaches of personal data security in the assurance period. Consequently, we have not been able to test the implementation and effectiveness of the procedure.	Upon request, we have been informed that there are no examples of breaches of personal data security within the assurance period. Therefore, we cannot test control implementation and operational effectiveness No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.17: Information security aspects of disaster recovery, contingency and restore		
17.1 Control Objective ▶ *To ensure that information security- and data protection continuity is rooted in the organisation's management systems for emergency and re-establishment. GDPR Art. 28, paragraph 3, point c.* ▶ *To ensure accessibility of information- and personal data processing facilities. GDPR Art. 28, paragraph 3, point c.*		
Control Activity	**Test performed by BDO**	**Result of test**
17.1.1 Implementation of information security continuity ▶ Contingency plans are prepared for relevant functions to ensure business continuance in connection with security incidents.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's contingency plan and observed that this ensures the continuation of the business in connection in connection with security incidents.	No exceptions noted.
17.1.2 Verify, review, and evaluate the information security continuity ▶ The data processor has established periodical testing of contingency plans for the purpose of ensuring that the contingency plans are up-to-date and effective in critical situations. ▶ Contingency tests are documented by reports from testing.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's procedure for testing of the information security continuity on annually basis. Vi have inspected documentation for controls of contingency plan test and observed that test was performed in the assurance period.	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.18: Compliance

18.1 Control Objective

- *To prevent violations of statutory, regulatory, or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.*
- *To ensure that information security and data protection is implemented and run, in accordance with the organisation's policies and procedures. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
18.1.1 Privacy and protection of personally identifiable information ▶ The data processor has procedures for making written, electronic data processing agreements, including template for data processing agreement in accordance with the services provided. ▶ Data processing agreements have been entered with the relevant customers and stored electronically. ▶ Data processing agreements include information on the use of sub-processors.	We made inquiries of relevant personnel at .legal A/S. We have inspected that when concluding contracts, the data controllers in the online approval flow must also approve and accept the data processor agreement. We have on new agreements in the assurance period inspected that data processer agreement is signed and stores electronically. On a sample basis we have inspected that Data processing agreements include information on the use of sub-processors.	No exceptions noted.
18.1.2 Instruction for processing of personal data ▶ The data processor stores and processes personal data according to the customer's instruction for the customers who have made a data processing agreement. ▶ Data processing agreements provide terms to the effect that the data controller must be informed of instructions which are not compliant with legislation.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's procedures and template for entering into data processing agreements with customers. We have observed that the template for the data processing agreement complies with the requirements relating to the content of a data processing agreement in accordance with General Data Protection Regulation article 28(3), and that it includes information on the use of sub-processors. We have inspected the data processor agreement template and observed that it contains instruction for a valid data processing. We have inspected that the data processor must notify the data controller in the event of illegal instructions. Upon request, we have been informed that there have been no incidents regarding illegal instructions in the assurance	Upon request, we have been informed that there have been no incidents regarding illegal instructions within the assurance period. Therefore, we cannot test control implementation and operational effectiveness No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.18: Compliance

18.1 Control Objective

- *To prevent violations of statutory, regulatory, or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.*
- *To ensure that information security and data protection is implemented and run, in accordance with the organisation's policies and procedures. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
	period. Consequently, we have not been able to test the implementation and effectiveness of the procedure.	
18.1.3 Assistance to the data controller ▶ The data processor has an obligation according to the data processing agreements to assist the customers in relation to requests for exercising of the data subjects' rights. ▶ The data processor has an obligation according to the data processing agreements to assist the customers with their obligations according to articles 32 to 36. ▶ The data processor has an obligation according to the data processing agreements to obtain an ISAE 3000 report annually for the purpose of the customer's inspection of .legal.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor's data processor template and observed that the data processor must aid a request for the rights of the registers and Articles 32 and 36. We have upon request, been informed that the data processor has not received inquiries regarding the rights of data subjects and the specific requirements of the regulation in the assurance period. Consequently, we have not been able to test the implementation and effectiveness of the procedure.	We have upon request, been informed that the data processor has not received inquiries regarding the rights of data subjects and the specific requirements of the regulation in the assurance period. Therefore, we cannot test control implementation and operational effectiveness. No exceptions noted.
18.1.4 Deletion and return of customers data. ▶ Procedures have been implemented to ensure protection of customer's confidential and sensitive information when offboarding a customer.	We made inquiries of relevant personnel at .legal A/S. We have inspected the procedure for off-boarding of customers and observed that the data processor has a procedure for deleting or returning data upon customer termination. Upon request, we have been informed that upon termination of agreements, the data controllers can withdraw data themselves. On a sample basis we have observed that the data processor has followed their procedure for off boarding a customer, including deleting data.	No exceptions noted.

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

A.18: Compliance

18.1 Control Objective

- *To prevent violations of statutory, regulatory, or contractual requirements in relation to information security and other security requirements. GDPR Art. 25, Art. 28, paragraph 2, Art. 28, paragraph 3, point a, Art. 28, paragraph 3, point e, Art. 28, paragraph 3, point g, Art. 28, paragraph 3, point h, Art. 28, paragraph 3, point f, Art. 28, paragraph 10, Art. 29, Art. 32, paragraph 4, Art. 33, paragraph 2.*
- *To ensure that information security and data protection is implemented and run, in accordance with the organisation's policies and procedures. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
18.1.5 Independent review of controls ▶ The data processor conducts an annual compliance check with legislation and other standards to ensure compliance legislation and other standards.	We made inquiries of relevant personnel at .legal A/S. We have inspected the data processor'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: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

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: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

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: 80.196.xxx.xxx
2026-11-20 12:24:27 UTC

Nicolai Tobias Visti Pedersen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Statsautoriseret revisor
Serienummer: c42f66e9-59bb-478a-9d92-2a2b8602724e
IP: 77.243.xxx.xxx
2026-11-20 13:11:11 UTC

Mikkel Jon Larssen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Partner
Serienummer: cd9a38dd-e75c-40f7-80d6-ec5b5d0841d6
IP: 37.96.xxx.xxx
2026-11-20 14:06:46 UTC

Penneo dokumentnøgle: TVZF8-778ZP-O3S3U-UKWYF-0XV8J-S3MPB

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.