INDEPENDENT AUDITOR'S ISAE 3402 ASSURANCE REPORT FOR THE PERIOD FROM 1 NOVEMBER 2023 TO 31 OCTOBER 2024 ON THE DESCRIPTION OF PACTIUS & PRIVACY AND THE RELATING CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS

.LEGAL A/S

CONTENTS

1. AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT FOR THE PERIOD FROM 1 NOVEMBER 2023 TO 31 OCTOBER 2024 ON THE DESCRIPTION OF PACTIUS & PRIVACY AND THE RELATING CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS

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

Scope

We have been engaged to report on .legal A/S (the service provider) description in section 3 of Pactius and Privacy and related controls, and on the design and operating effectiveness of controls related to the control objectives stated in the description, throughout the period from 1 November 2023 to 31 October 2024.

The Service Provider's Responsibilities

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

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

Auditor's Independence and Quality Assurance

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

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

Auditor's Responsibilities

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

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

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

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

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

Limitations of Controls at a Service Organisation

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

Opinion

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

a. The description of PACTIUS & PRIVACY and related controls, as designed and implemented throughout the period from 1 November 2023 to 31 October 2024 is in all material aspects, accurate and

b. The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 November 2023 to 31 October 2024; and

c. The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 November 2023 to 31 October 2024.

Description of Tests of Controls

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

Intended Users and Purpose

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

Copenhagen, 13 November 2024

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, State Authorised Public Accountant

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

2. .LEGAL A/S' STATEMENT

.legal A/S has prepared the following descriptions of controls relating to PACTIUS and PRIVACY Services to the company's customers.

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

.legal A/S is using sub service organisations. This sub service organisations relevant control objectives and related controls is not included in the description.

.legal A/S confirms that the accompanying description fairly presents controls in relation to PACTIUS and PRIVACY Service throughout the period from 1 November 2023 to 31 October 2024. The criteria used in making this statement were that the accompanying description:

1. Presents how the controls in relation to PACTIUS and PRIVACY Service were designed and implemented, including:
    - The services provided.
    - The procedures within both information technology and manual systems used to manage the controls.
    - Relevant control objectives and controls designed to achieve those objectives.
    - The controls that we, referring to the design of our services, have assumed were implemented by the customer and, if necessary to achieve the control objectives stated in the description, were identified in the description along with the specific control objectives that we cannot achieve.
    - Other relevant aspects of control environment, risk assessment process, information systems, communication, control activities and monitoring controls of relevance for the services provided.
2. Includes relevant details of changes to the controls relating to PACTIUS and PRIVACY Service during the period from 1 November 2023 to 31 October 2024.
3. Does not omit or distort information relevant to the scope of the controls described relating to PACTIUS and Privacy Service considering that the description is prepared to meet the general needs of a wide range of customers and their auditors and therefore cannot include every aspect of PACTIUS and Privacy Service and controls that the individual customer may consider of importance to their special environment.

.legal A/S confirms that controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 November 2023 to 31 October 2024. The criteria we used in making this statement were that:

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

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

3. The controls were consistently applied as designed, including those manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 November 2023 to 31 October 2024.

Aarhus, 13 November 2024

.legal A/S

Brian Østberg
CEO

3. .LEGAL A/S' DESCRIPTON ON PACTIUS AND PRIVACY SERVICE

THE .LEGAL PRODUCT FAMILY

PACTIUS and PRIVACY Service are independent services but are still part of the same .legal product family. Therefore, we have chosen to let them assess according to the same standard, as we want all services from .legal A/S to live up to live up to a uniformly high standard in relation to IT operations and security.

PACTIUS

PACTIUS is a contract management system developed and operated by .legal A/S. PACTIUS can be used for multiple purposes including everything from simple storage of contracts to follow-up on rights, obligations and complex deliveries on large IT, enterprise, and outsourcing contracts.

PRIVACY

Privacy streamlines compliance, helping develop, manage, and improve programs to foster trust, ensure compliance, and simplify operations. Privacy supports compliance work within the areas of data protection (GDPR), information security and vendor management.

.LEGAL A/S' DESCRIPTION OF CONTROL ENVIRONMENT

A.4 Risk management

Annual risk assessment

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

Guidelines and control objectives

Internally, we have documented a number of 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.

PRIVACY is used for follow-up and documentation of the internal control objectives.

A.5 Information Security Policies

IT Security Policy
.legal works according to an IT security policy which covers PACTIUS and Privacy Service. The IT security policy is organised according to ISO 27001: 2013 and forms the basis for those involved in development or operation of PACTIUS and PRIVACY Service. 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 a number of guidelines and control objectives, which are described in the policy for each ISO area.

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

A.6 Organisation of information security

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

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

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

A.7 Human resource security

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

A.8 Asset management

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

A.9 Access control

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

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

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

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.

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

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

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

A.10 Cryptography

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

The system uses a SHA-2 SSL certificate with a minimum of 2048bit encryption from a trusted provider. Data is encrypted when stored in the data center and automatically decrypted when accessed.

A minimum of TLS 1.2 is required for all requests to the system.

Data is encrypted "at rest" when stored in the data centre and automatically decrypted when accessed. This is done using AES 256 and Microsoft-managed keys.

A.11 Physical- and environmental protection

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

A.12 Operational reliability

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

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

The systems are hosted in Microsoft Azure - i.a. for security reasons, as the underlying platform is always up-to-date, and the possibilities for data encryption, redundancy, backup and access control are generally good. Concerning the use of third-party services outside Azure, these are selected based on requirements for a high-security standard (eg ISO27001 certification) as well as compliance with the GDPR. In general, we try to reduce the need of third-party services outside of Microsoft Azure

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

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)

Data Backup
PACTIUS performs a nightly backup of data in the production environment which is stored for 7 days. Privacy runs continuous backup that allows data to be restored at a specific time. It is possible to restore a maximum of 30 days back in time.

Additionally, Privacy and PACTIUS has a monthly backup that is stored for 3 months.

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

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

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

All our services are hosted on Azure with the following service level agreement (SLA):
Webapps SLA: 99,95 %
Cosmos DB SLA: 99,99 %
Azure SQL Server SLA: 99,99 %
SLA for Data Storage Accounts: 99,99 %

More details: https://azure.microsoft.com/en-us/support/legal/sla/summary/
The availability of our systems is continually monitored and logged. And the current status as well as the up-time history can be accessed at https://status.dotlegal.com.

Brute force protection
Our login provider (id.dotlegal.dk) is protected against brute force attacks by blocking the user after three login attempts.

The password requirements are:
- Must contain at least 10 characters
- Must contain at least 5 different characters
- Must not contain the username
- May not be too common. (We check against OWASP's SecLists project of 10,000 most used passwords)

System and security testing
An authorised external company conducts planned and documented vulnerability scans on a regular basis, at least quarterly, to efficiently identify potential vulnerabilities. The CTO of .legal then thoroughly evaluates these findings and takes appropriate action (if discrepancies or issues are identified).

A.13 Communication security

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

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

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

A.14 Procurement, development, and maintenance of systems

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

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

All development teams have experienced people 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
    - 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 conditions

Supplier agreements
- Supplier agreements are established with all customers who use the systems.
- Any subcontractors must live up to the same security standard and comply with the same security policies as .legal A/S.

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

A.16 Management of information security and personal data breaches

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

1. The security incident is registered in the company's task management.
2. In the description of the task, the security incident/weakness is noted in as many details as possible, including as a minimum:
    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 prioritized and implemented
6. Once the measures have been implemented, the task is closed.
7. After the problem is solved, the process is described as an incident in the project's incident log. The purpose is to investigate whether there is an underlying problem that may give rise to further improvements or help remedy similar future problems.

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

Specifically on the handling of personal data breaches when .legal A/S is the 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.18: Compliance

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

- Act no. 502 of 23 May 2018 on supplementary provisions to the Regulation on the protection of natural persons in connection with the processing of personal data and on the free exchange of such data (Data Protection Act)
- Personal Data Regulation (Regulation No 2016/679)

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

Changes during the period 1. November 2024 to 31. October 2024 relating to PACTIUS and Privacy Service

Following changes have been made during the audit period:

- Active geo replication added to the production databases of Privacy
- Regular and systematic vulnerability scans tests are performed against Privacy
- A public status page showing historic up time for the systems has been added

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

Objective and scope

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

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

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

In the check form, BDO has described the tests performed which were considered necessary to obtain a reasonable degree of assurance that the stated control objectives were achieved and that the related controls were suitably designed and operated effectively throughout the period from 1 November 2023 to 31 October 2024.

Tests performed

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

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

For the services provided by Microsoft Azure in the field of infrastructure hosting, we have received the Service Organisation Control (SOC 2) type 2 Report for the period from April 1, 2023, to March 31, 2024 and Bridge Letters to July 8 2024.

This service subcontractors relevant control objectives and related controls does not include in .legal A/S' description of PACTIUS and Privacy Service and the related controls. We have therefore only inspected the received documentation and tested the controls with .legal A/S, who secures the supervision on the agreement between the service subcontractor and .legal A/S.

Result of test

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

A deviation exists when:

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

A.5 Information security policies

A.5.1 Guidelines for managing information security

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

Control Activity	Test performed by BDO	Result of test
5.1.1 Policies for information security ▶ Management sets out and approves policies for information security which after approval are published and communicated to staff and relevant external parties.	We have interviewed relevant personnel at .legal A/S. We have inspected that management has settled and approved a set of information security policies. We have inspected, that the latest versions of the policies have been published and communicated to the employees and relevant external partners.	No deviations identified.
5.1.2 Review of policies for information security ▶ The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	We have interviewed relevant personnel at .legal A/S. We have observed that the information security policy was updated and approved by management in the declaration period.	No deviations identified.

A.6 Organisation of information security		
Control Objective ▶ *To establish a management basis for initiating and managing the implementation and operation of information security and data protection in the organisation.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.6.1.1 Roles and responsibilities for information security ▶ All information security responsibilities are defined and allocated.	We have interviewed relevant personnel at .legal A/S. We have inspected, the service provider's information security policy and observed that all areas of responsibility for information security are clearly defined and allocated.	No deviations identified.
A.6.1.2 Segregation of duties ▶ Contradictory functions and responsibilities are separated to reduce the possibility of unauthorized or accidental use, alteration or misuse of organizational assets.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for segregation of duties and observed that the service provider has defined roles so that areas of responsibility are separated. We have observed that all administrator creations must be approved by the service provider's management. We have inspected the service provider's employee list and observed what job functions the employees have. We have inspected user extracts for relevant systems and observed that there is segregation of duties. We have been informed that no new administrators have been created during the declaration period. It is therefore not possible to test management approval of these.	We have been informed that no new administrators have been created during the declaration period. It is therefore not possible to test the control activity. No deviations identified.

A.7 Human resource security

Control Objective

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

Control Activity	Test performed by BDO	Result of test
A.7.2.1. Management responsibilities ▶ Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's employment procedure and supplier security. We have observed that the management of the service provider requires all employees and contractors to sign a declaration that the organisation's established policies and procedures within information security are read, understood and complied with. On a sample basis we have inspected signed declarations from the service provider's employees.	No deviations identified.
A.7.3.1 Termination or change of employment responsibilities ▶ Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor, and enforced.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's employment contract template and observed that this describes the employees' obligations and responsibilities after the termination of employment or changes. We have on a sample basis inspected that employees have signed of and accepted the mandatory obligations for information security.	No deviations identified.

A.8 Asset management		
Control Objective ▶ *To identify the organisation's assets and define appropriate responsibilities for its protection.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.8.1.1 Inventory of assets ▶ Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's inventory of assets in relation to information and information processing facilities. We have observed that the Inventory of assets have been updated within the declaration period.	No deviations identified.

A.9 Access management

Control Objective

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

Control Activity	Test performed by BDO	Result of test
A.9.1.2 Access to networks and network services ▶ Users shall only be provided with access to the network and net- work services that they have been specifically authorized to use.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for access control and observed that the procedure includes access restrictions to the network and network services. We have inspected that only a limited number of employees with a work-related purpose have access to the service provider's network and network services.	No deviations identified.
A.9.2.2 User Access provision ▶ A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for access control and observed that rights must be granted based on a work-related purpose. We have been informed that the service provider has a formal evaluation process for access permission to new employees We have inspected the employee's access and user rights granted to systems and confirmed that the appropriate access and user rights were granted according to the procedure and based on a work-related basis.	No deviations identified.
A.9.2.3 Management of privileged access rights ▶ The allocation of secret authentication information shall be controlled through a formal management process.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for access control and observed that the service provider has described how the management of privileged access rights takes place.	No deviations identified.

A.9 Access management		
Control Objective ▶ *To restrict access to information and information processing facilities.* ▶ *To ensure access for authorised users and prevent unauthorised access to systems and services.* ▶ *To prevent unauthorised access to systems and applications.*		
Control Activity	**Test performed by BDO**	**Result of test**
	We have been informed that there has been one new admin allocation during the audit period. We have on a sample basis inspected that the new admin allocation within the declaration period followed the service provider's access control procedure and were based on a work-related basis.	
A.9.2.5 Review or adjustment of access rights ▶ User rights are reviewed periodically.	We have interviewed relevant personnel at .legal A/S. We have inspected that the service provider has conducted a periodic review of all assigned access rights within the declaration period.	No deviations identified.
A.9.4.1 Information access restriction ▶ Access to information and application system functions shall be restricted in accordance with the access control policy.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for access control and observed that access and user rights are granted based on a work-related basis. We have inspected the service provider's systems and observed that employees are only granted access and user rights to systems and services related to their work.	No deviations identified.
A.9.4.2 Secure log-on procedures ▶ Where required by the access control policy, access to systems and application shall be controlled by a secure log-on procedure as two-factor login	We have interviewed relevant personnel at .legal A/S.	No deviations identified.

A.9 Access management		
Control Objective ▶ *To restrict access to information and information processing facilities.* ▶ *To ensure access for authorised users and prevent unauthorised access to systems and services.* ▶ *To prevent unauthorised access to systems and applications.*		
Control Activity	**Test performed by BDO**	**Result of test**
	We have inspected the service provider's procedure for access control and observed that there are requirements for using two factor authentication, when possible. We have inspected that two-factor authentication has been implemented in PACTIUS and Privacy Service systems.	
A.9.4.3 Password management system ▶ Password management systems shall be interactive and shall ensure quality passwords.	We have interviewed relevant personnel at .legal A/S. We have inspected the IT security policy and observed that all employees must use the company approved password manager. We have inspected the service providers password manager and observed that all employees were active. We have inspected the password managers configuration and observed that it is mandatory for all active users to have their multi factor authentication enabled. On a sample basis we inspected that the users with access to systems containing personal data use the password manager and with a requirement for two factor authentication. We have on a sample basis inspected that workstations have password requirements.	No deviations identified.
A.9.4.5 Access control to program source code ▶ Access to program code shall be restricted.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for access control to development environments, including source codes and	No deviations identified.

A.9 Access management		
Control Objective ▶ *To restrict access to information and information processing facilities.* ▶ *To ensure access for authorised users and prevent unauthorised access to systems and services.* ▶ *To prevent unauthorised access to systems and applications.*		
Control Activity	**Test performed by BDO**	**Result of test**
	observed that source codes are securely stored in a dedicated project. We have inspected that the service provider stores source codes for the PACTIUS and Privacy Service systems securely where only allowed developers have access.	

A.10 Cryptography		
Control Objective ▶ *To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.10.1.1 Policy on the use of cryptographic controls ▶ A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's encryption policy and observed that the systems as a minimum must use a SHA-2 SSL certificate with a minimum of 2048 bit encryption. We have inspected that PACTIUS and Privacy Service systems use a SHA-2 SSL certificate with a minimum of 2048 bit encryption. On a sample basis we inspected that encryption were activated on employees' workstations.	No deviations identified.

A.11 Physical and environmental security

Control Objective

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

Control Activity	Test performed by BDO	Result of test
A.11.1.3 Securing offices, rooms, and facilities ▶ Physical security for offices, rooms and facilities shall be designed and applied	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for physical security and observed that physical security must be established at the service providers physical controlled locations. We have inspected the building 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 employees with access to the location and observed that only internal employees have access. We have inspected the latest SOC 2 report and related bridge letters from Microsoft Azure and observed that no deviations have been found in relation to physical security.	No deviations identified.

A.12 Operations security

Control Objective

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

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

A.12 Operations security

Control Objective

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

Control Activity	Test performed by BDO	Result of test
	We have inspected that there is a segregation between the development, testing and the production environment for PACTIUS and Privacy Service.	
A.12.3.1 Backup of information ▶ Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy. ▶ Restore tests are carried out for customers with restore agreements according to the agreements	We have interviewed relevant personnel at .legal A/S. We have inspected the data processor's backup procedure for PACTIUS and Privacy Service. We have observed that backup is performed in accordance with the procedure. On a sample basis we inspected that routine backup was performed according to the backup procedure. We have inspected the service providers latest restore test and observed that it was conducted within the declaration period.	No deviations identified.
A.12.4.1 Event logging ▶ Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for logging, monitoring, and alerting and observed that there must be event-based logging of user activity, signatures, errors, and information security incidents. The log must be kept and reviewed regularly. We have inspected that event logs have been set up for PACTIUS and Privacy Service systems. We have inspected the service providers alarming of event logging and observed that key personal are informed and notified whenever an alarm is set of.	No deviations identified.

A.12 Operations security		
Control Objective ▶ *To ensure correct and reliable operation of information processing facilities.* ▶ *To protect against data loss.* ▶ *To record incidents and obtain evidence.*		
Control Activity	**Test performed by BDO**	**Result of test**
	We have inspected that there is a dashboard of events that are reviewed by the operating organisation daily.	
12.6.1 Vulnerability Scanning ▶ Vulnerability scans are conducted at least twice a year. 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	By inquiry we have been informed that the Data Processor performs vulnerability scanning each month. We have inspected the Data Processors scanning history and observed that vulnerability scans have been conducted multiple times in the declaration period. We have inspected the vulnerability scanning report and observed that identified vulnerabilities are reported. We have on a sample basis inspected that identified vulnerabilities has been mitigated or reduced in criticality.	No deviations identified.

A.13 Communications security		
Control Objective ▶ *To maintain information security when transferring internally in an organisation and to an external entity.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.13.2.2 Agreements on information transfer ▶ Agreements shall address the secure transfer of business information between the organisation and external parties.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for supplier security and observed that when entering into a supplier agreement, a declaration must be signed in compliance with the service provider's security policy. Furthermore, have we inspected the service provider's encryption policy and observed that data transfer over the internet as a minimum must use a SSL SHA-2 SSL certificate with a minimum of 2048 bit encryption. We have inspected the supplier agreement template. We have inspected system configuration that the communication between the browser and the rest of the system takes place using HTTPS with an SSL SHA-2 certificate with a 2048-bit encryption. We have inspected system configuration that exchange of data between the customers and the system takes place using SFTP with an RSA-SHA256 certificate with a 3072-bit encryption. Upon request, we have been informed that no agreements have been made or have been entered into with suppliers during the declaration period. Therefore, we have not been able to test for implementation and effectiveness of the procedure.	We have upon request been informed that no service or supplier agreements have been made within the declaration period. Therefore, the control activity has not been possible to test. No deviations identified.
A.13.2.4 Confidentiality or non-disclosure agreements ▶ Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed, and documented.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for personnel security and observed that new employees must sign a declaration of compliance with the service provider's safety policy when hiring.	No deviations identified.

A.13 Communications security		
Control Objective ▶ *To maintain information security when transferring internally in an organisation and to an external entity.*		
Control Activity	**Test performed by BDO**	**Result of test**
	We have further inspected that the service provider's template for employment contracts contains requirements for confidentiality, both during and after employment. On a sample basis we inspected that new employees have signed a confidentiality agreement.	

A.14 System acquisition, development, and maintenance of systems		
Control Objective ▶ *To ensure that information security is organised and implemented within the information systems development life cycle.* ▶ *To ensure the protection of data used for testing.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.14.2.2 System change control procedures ▶ Changes to systems within the development lifecycle shall be controlled using formal Change Management procedures.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's development procedure and observed that changes to systems within the development life cycle must be managed using formal change management procedures. We have inspected that the procedure is implemented so that changes to systems are controlled through an approved process. On a sample basis we inspected, that changes followed the procedure for change management.	No deviations identified.
A.14.2.3 Technical review of applications after changes to operating platforms ▶ Formal processes and procedures have been implemented for all changes made in the company's own IT environment.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for development and observed that all changes must first be approved by another developer and then by the task manager. On a sample basis we have inspected that changes are approved according to the procedure.	No deviations identified.
A.14.2.6 Secure development environment ▶ Organisations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for development and observed that there are formal requirements for development throughout the entire life cycle.	No deviations identified.

A.14 System acquisition, development, and maintenance of systems		
Control Objective ▶ *To ensure that information security is organised and implemented within the information systems development life cycle.* ▶ *To ensure the protection of data used for testing.*		
Control Activity	**Test performed by BDO**	**Result of test**
	We have inspected the service providers development tool, version history and code review are compliant with the service providers development procedure. We have inspected the service providers test environment and observed that data are non-production data.	
A.14.2.8 System security testing ▶ Testing of security functionality shall be carried out during development.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for development and observed that regression tests must be performed to ensure that these do not have a negative impact on the organization's operation or safety. On a sample basis we inspected that tests have been performed for changes in accordance with the development procedure	No deviations identified.
A.14.3.1 Securing test data ▶ A fixed procedure has been implemented for the protection of test data.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for development and observed that the test environment must be segregated and only contain fake data. We have inspected the service providers test environment and observed that data are non-production data.	No deviations identified.

A.15 Supplier relationship		
Control Objective ▶ *To ensure protection of the organisation's assets that suppliers have access to.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.15.1.1 Information security policy for supplier relationships ▶ Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets shall be agreed with the supplier and documented.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for supplier security and observed that when entering into a supplier agreement, a declaration must be signed in compliance with the service provider's security policy. We have inspected the template for the statement. Upon request, we have been informed that no new agreements have been entered into with suppliers during the declaration period. Therefore, it has not been possible to test for implementation of the procedure. We have inspected that the service provider has obtained and reviewed the SOC 2 and bridge letter from Microsoft Azure regarding their compliance with the security requirements.	Upon request, we have been informed that no new agreements have been or have been entered into with suppliers during the declaration period. Therefore, the control activity has not been possible to test. No deviations identified.
A.15.1.2 Addressing security within supplier agreements ▶ All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for supplier security and observed that when entering into a supplier agreement, a declaration must be signed in compliance with the service provider's security policy. We have inspected the template for the statement. Upon request, we have been informed that no new agreements have been or have been entered into with suppliers during the declaration period. Therefore, it has not been possible to test for implementation of the procedure. We have inspected that the service provider has obtained and reviewed the SOC 2 and bridge letter from Microsoft Azure regarding their compliance with the security requirements.	Upon request, we have been informed that no new agreements have been or have been entered into with suppliers during the declaration period. Therefore, the control activity has not been possible to test. No deviations identified.

A.16 Information security incident management

Control Objective

- *To ensure a uniform and effective method of managing information security incidents, including communication on security incidents and weaknesses.*

Control Activity	Test performed by BDO	Result of test
A.16.1.1 Responsibilities and procedures ▶ Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for security breaches and observed that roles and responsibilities for incidents handling in case of a security breach has been dictated by management.	No deviations identified.
A.16.1.2 Reporting of information security incidents ▶ Information security events shall be reported through appropriate management channels as quickly as possible.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for security breaches and observed that a report is required whenever a security breach occurs. Upon request, we have been informed that the service provider has not had any security breaches during the declaration period. Therefore, it has not been possible to test the control activity.	Upon request, we have been informed that the service provider has not had any security breaches during the declaration period. Therefore, it has not been possible to test the control activity. No deviations identified.
A.16.1.6 Learning from information security incidents ▶ Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for security breaches and observed that as a part of the reporting from an IT-Security breach an evaluation of the handling of the incident must be included in the report. Upon request, we have been informed that the service provider has not had any security breaches during the declaration period. Therefore, it has not been possible to test the control activity.	Upon request, we have been informed that the service provider has not had any security breaches during the declaration period. Therefore, it has not been possible to test the control activity. No deviations identified.

A.16 Information security incident management		
Control Objective ▶ *To ensure a uniform and effective method of managing information security incidents, including communication on security incidents and weaknesses.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.16.1.7 Collection of evidence ▶ Evidence of information security breaches is collected.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for security breaches and observed that in case of an IT-Security breach evidence must be collected when possible. Upon request, we have been informed that the service provider has not had any security breaches during the declaration period. Therefore, it has not been possible to test the control activity.	Upon request, we have been informed that the service provider has not had any security breaches during the declaration period. Therefore, it has not been possible to test the control activity. No deviations identified.

A.18 Compliance		
Control Objective ▶ *To ensure that information security and data protection is implemented and run in accordance with the organisation's policies and procedures.*		
Control Activity	**Test performed by BDO**	**Result of test**
A.18.1.1 Identification of applicable legislation and contractual requirements ▶ All relevant legislative, statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented, and kept up to date for each information system and the organisation.	We have interviewed relevant personnel at .legal A/S. We have inspected the service provider's procedure for compliance with legal and contractual requirements and observed that once a year the service provider's management asks the law firm Bech-Bruun to assess whether there have been changes in the above legislation in a way that changes in security policy. and/or in the system. We have inspected that the law firm Bech-Bruun in the Áudit period have reviewed that the service provider's procedures and policies are in accordance with applicable law. We have inspected that the service provider's management has reviewed Bech-Bruun's review.	No deviations identified.
A.18.1.4 Privacy and protection of personally identifiable information ▶ Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	We have interviewed relevant personnel at .legal A/S. We have inspected that in the Audit period, the law firm Bech-Bruun reviewed the service provider's procedures and policies are in accordance with applicable law.	No deviations identified.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

PENNEO

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

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

Brian Østberg
CEO
Serienummer: dab750c2-1b99-4493-8e2f-4e0c44e45883
IP: 217.116.xxx.xxx
2024-11-14 15:12:58 UTC

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 188.177.xxx.xxx
2024-11-14 15:53:00 UTC

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 62.66.xxx.xxx
2024-11-14 15:53:14 UTC