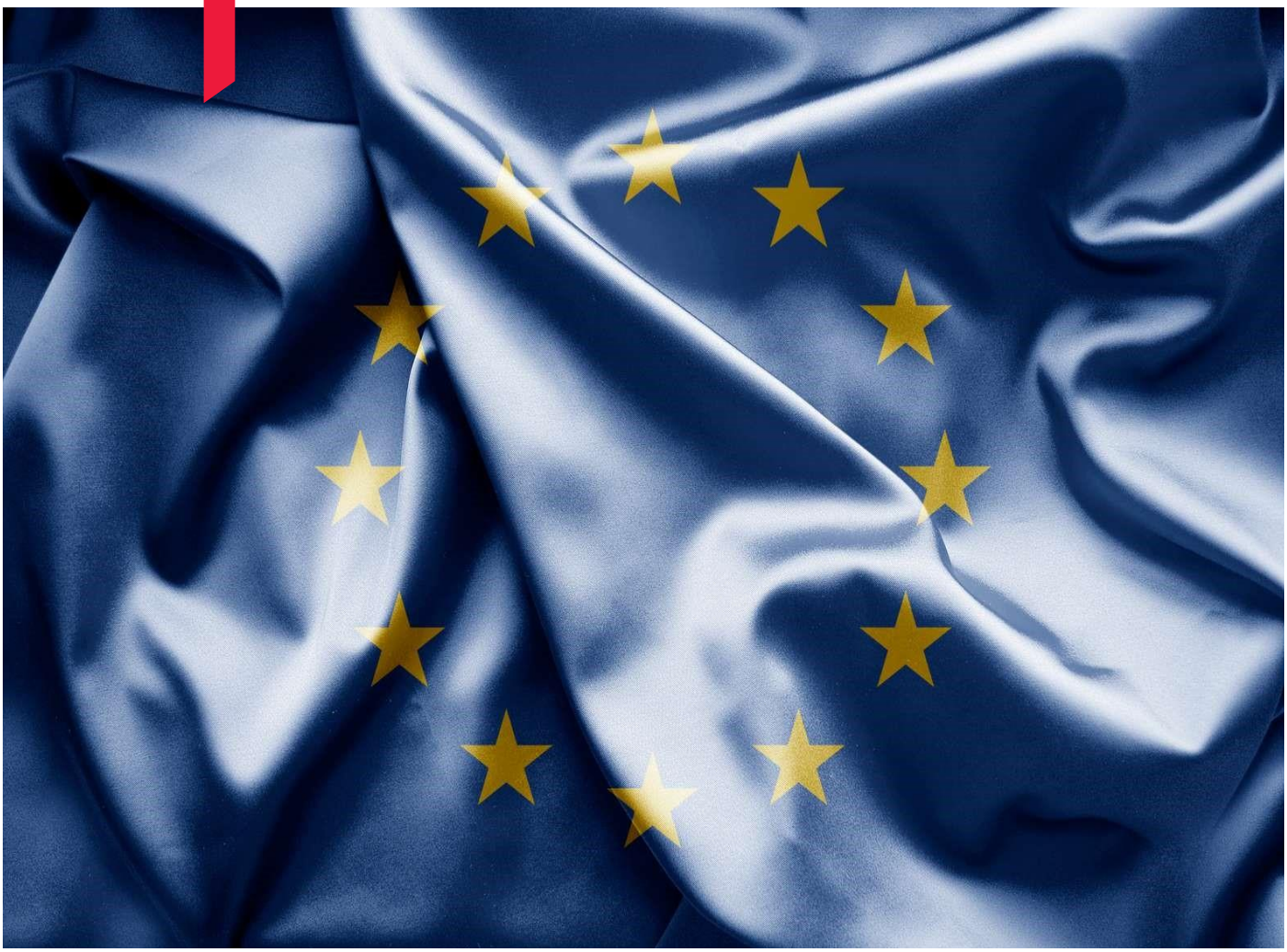

.LEGAL A/S

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT ON 10 AUGUST 2022 ON THE DESCRIPTION OF PACTIUS AND PRIVACY AND THE RELATING TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DATA PROTECTION ACT

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

CONTENTS

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3000 ASSURANCE REPORT ON 10 AUGUST 2022 ON THE DESCRIPTION OF PACTIUS AND PRIVACY AND THE RELATING TECHNICAL AND ORGANISATIONAL MEASURES AND OTHER CONTROLS AND THEIR DESIGN RELATING TO PROCESSING AND PROTECTION OF PERSONAL DATA IN ACCORDANCE WITH THE EU GENERAL DATA PROTECTION REGULATION AND THE DATA PROTECTION.

To: Management of .legal
.legal's Customers (Controllers)

Scope

We have been engaged to issue an assurance report on the description in section 3 of .legal's and the relating technical and organisational security measures and other controls prepared by .legal (data processor) on 10 August 2022, aimed at 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 General Data Protection Regulation) and law on supplementary provisions to the General Data Protection Regulation (the Data Protection Act), and on the design of the technical and organisational security measures and other controls relating to the control objectives stated in the description.

We have not performed procedures regarding the operating effectiveness of the controls stated in the description, and consequently, we do not express an opinion on this.

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 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 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.

We are subject to the international standard on quality control, ISQC 1, and accordingly use and maintain a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's Responsibilities

Based on our actions, it is our responsibility to express an opinion on the data processor's description and on the design of the controls relating to the control objectives stated in this description.

We have performed our work in accordance with ISAE 3000 on other assurance engagements with certainty than audit or review of historical financial information. This standard requires that we plan and execute our actions to achieve a high degree of certainty of whether the description in every aspect is true, and whether the controls in all material aspects are appropriately designed.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

An assurance engagement with certainty on issuing a report on the description and design of controls with a data processor includes performance of actions to achieve evidence for the information of the data processor's description and for the design of the controls. The actions selected depend on the assessment of the data processor's auditor, including the assessment of the risks of the description not being fair and that the controls are not appropriately designed. In addition, an assurance engagement with certainty of this type includes assessment of the total presentation of the description, the appropriateness of the herein stated control objectives as well as the appropriateness of the criteria specified and described in section 2.

As mentioned above, we have not performed procedures regarding the operating effectiveness of the controls stated in the description, and consequently, we do not express an opinion on this.

In our opinion, the evidence obtained is sufficient and suitable to form basis for our conclusion.

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, therefore, not include every aspect of the use of PACTIUS and Privacy, that the individual data controllers may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches.

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 PACTIUS and Privacy 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 on 10 August 2022.

b. The technical and organisational measures and other controls, relating to the control objectives stated in the description were appropriately designed on 10 August 2022.

Description of Test of Controls

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

Intended Users and Purpose

This report is intended solely for data controllers who have used the Data Processors systems PACTIUS and Privacy, 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 in assessing whether the requirements of the EU General Data Protection Regulation and the Danish Data Protection Act have been complied with.

Copenhagen, 26 august 2022

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
State Authorised Public Accountant

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

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

.LEGAL' STATEMENT

.legal processes personal data in relation to PACTIUS and Privacy 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 PACTIUS and Privacy, 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 uses a sub-processor. This sub-processor's relevant control objectives and related technical and organisational measures and other controls are not included in the accompanying description.

.legal confirms that the accompanying description fairly presents PACTIUS and Privacy and the related technical and organisational measures and other controls on 10 August 2022. The criteria used in preparing this statement were that the accompanying description:

1. Presents how PACTIUS and Privacy, 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 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, in reference to the scope of PACTIUS and Privacy, have assumed would be designed and implemented by the data controllers and which, if necessary in order to achieve the control objectives stated in the description, 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. Does not omit or distort information relevant to the scope of PACTIUS and Privacy 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, therefore, not include every aspect of PACTIUS and Privacy that the individual data controllers might consider important in their particular circumstances.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

.legal confirms that the technical and organisational measures and other controls related to the control objectives stated in the description were appropriately designed at 10 August 2022. The criteria used in preparing this statement were the accompanying description:

1. The risks that threatened achievement of the 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.

.legal confirms that appropriate technical and organisational security measures and other controls have been implemented for the purpose of complying with the agreements made with the data controllers, generally accepted data processing principles and relevant demands on data processors in accordance with the General Data Protection Regulation and the Data Protection Act.

Aarhus, 26 august 2022

.legal A/S

Brian Østberg
Managing Director

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

.LEGAL'S DESCRIPTION OF PACTIUS AND PRIVACY

GENERAL DESCRIPTION OF .LEGAL

.legal A/S (hereinafter ".legal") is a Danish-founded company located in Aarhus and Copenhagen. .legal develops and provides a range of Software-as-a-Service (SaaS) solutions including PACTIUS and Privacy (hereinafter "The Services") within legaltech to support legal and compliance work within both private and public organisations.

It is .legal's objectives, that The Services are ensuring a solid and trustworthy foundation, both in terms of service and security. This report is part of our endeavor 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 Services 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 Services provision of IT operations.

DESCRIPTION OF PACTIUS AND PRIVACY' AND PROCESSING OF PERSONAL DATA

The Services, which .legal provides are a variety of cloud-based Software-as-a-service (SaaS) solutions and are developed to provide tools for various legal issues within compliance, such as contract management, compliance tools for documentation and management of an organisation's processing of personal data. The Services consist of digital systems for managing internal legal and compliance tasks and workflows tasks.

The Services are 100% decoupled systems but are still a part of the same .legal product family. Therefore, we have chosen to let them assess according to the same standard, as we want all, both existing and future, products from .legal to live up to a uniform high standard in relation to IT operations, security and processing of personal data.

Hosting centre and sub data processors:
Microsoft Azure is sub data processor for .legal.

Microsoft Azure provides the overall IT platform for the services in .legal, where data is stored in Azure Storage, Azure SQL, and Azure Cosmos DB in European data centres.

For use of third-party services outside Azure, these are selected based on high security standards (e.g., ISO27001 certification) and GDPR compliance. In general, we try to reduce the need for third-party services outside of Microsoft Azure.

How data is used
.legal is processing personal data on behalf of .legal's costumers, when the costumers use The Services 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 controller expressly that The Services are not designed to process sensitive or other confidential data and the processor cannot take into account how the controller uses The Services to process personal data, including what types of personal data the controller processes when using The Services other than described in Data Processor Agreement.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

.legal is processing, using and collecting personal data from the data controller/the costumer to operate effectively and provide The Services. .legal will process personal data as necessary to perform and provide The Services, 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 services, which .legal offers and to perform essential business operations related to The Services. This includes operation, maintaining and improving The Services and providing customer service.

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	• Risk assessment	• Art. 28(3)(c)
A.5: Information security policies	• Information Security Policy • Review of policies	• Art. 28(1)
A.6: Organisation of information security	• Roles and responsibilities • Remote workplaces and mobile equipment	• Art. 28(1) • Art. 28(3)(c)
A.7: Human resource security	• Before employment • During employment • Non-disclosure and confidentiality agreements • Resignation of employment	• Art. 28(1) • Art. 28(3)(b)
A.8: Asset management	• Record of categories of processing activities • Classification of information	• Art. 30(2), (3) & (4)
A.9: Access management	• Policy for access management • Allocation of user rights • Management of privileged access rights • Management of password requirements	• Art. 28(3)(c)

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

ISO 27001	Control activities	GDPR article
A.10: Cryptography	• Encryption	• Art. 28(3)(c)
A.11: Physical and environmental security	• Physical perimeter safety guarding • Clean desk and screen saver	• Art. 28(3)(c)
A.12: Operations security	• Backup • Incident logging • Administrator and operator logs	• Art. 28(3)(c)
A.13: Communication security	• Policies and procedures for transfer of information	• Art. 28(3)(c)
A.14: Acquisition, development, and maintenance of systems	• Development and maintenance of systems	• Art. 25
A.15: Supplier relationships	• Agreements with sub-processors • Approved sub-processors • Changes to approved sub-processors • Supervision of sub-processors	• Art. 28(2) & (4)
A.16: Information security incident management	• Handling of information and personal data security incidents • Reporting of information and personal data security incidents	• Art. 33(2)
A.17: Information security aspects of disaster recovery, contingency and restore management	• Implementation of information security continuity • Verify, review, and evaluate the information security continuity	• Art. 28(3)(c)
A.18: Compliance	• Privacy and protection of personally identifiable information • Instruction for processing of personal data • Assistance to the customers • Deletion and return of customers data • Independent review of controls	• Art. 28(3)(a), (c), (e)-(h) • Art. 29 • Art. 32(4) • Art. 28(10)

RISK MANAGEMENT OF PACTIUS AND PRIVACY

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.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

- 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.

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

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

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

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.

A.6 Organisation of information security

IT security manager
.legal has dedicated an employee 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, which complies with the services security policy relating to protection against malicious code.

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
As regards employees, they commit themselves, at their employment, to comply with 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

The employees at .legal are informed on how to manage the work with personally identifiable data through the IT Security Policy and through annual awareness training.

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.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.8 Asset management

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

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 only encrypts the 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 controls to ensure that IT equipment is properly protected against unauthorised physical access and environmental incidents.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

Physical security of premises and machines

.legal's premises are locked at all times. .legal does not host solutions itself, which means that the physical security primarily concerns the employees' machines and the hosting partner Microsoft Azure.

We refer to separate SOC 2 report on the description of controls, their design and operating effectiveness relating to Microsoft Azure.

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 Operations security

Secure hosting

Microsoft Azure is the overall IT platform for the systems in .legal.

- 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 in Western Europe.
- 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.

Data redundancy

The primary data location for the production environment for documents is Azure Western Europe. At this 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

PACTIUS and Privacy performs a nightly backup of data in the production environment which is stored for 7 days. In addition, there is a monthly backup, which is stored for 3 months. Backup is replicated 3 times within the same datacentre as the database is running in Western Europe.

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.

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.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

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

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 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 relationships

Supplier agreements

.legal uses Microsoft Azure as sub-supplier of backup.

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.

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 solely according to instructions from .legal and .legal's customer. Thus, .legal's sub-suppliers com-

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

mit 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 system.

A.16 Information security incident management

All safety and personal data 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 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.

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

.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.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

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 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 available all information required to prove compliance with the requirements for data processors to the data controller. .legal also enables and contributes to audits, including inspections, made by the data controller or other parties authorised by the data controller.

Deletion and return of customers' 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 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.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

COMPLEMENTARY CONTROLS FOR .LEGAL'S CUSTOMERS

The 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 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 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 Controller is not recommended to use the platforms for processing, including retention, of sensitive personal data, and it is the Controller's responsibility to ensure that such personal data are not entered into or uploaded to the platforms

.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND RESULT OF TESTS

Objective and scope

BDO has performed their work in accordance with ISAE 3000 on other assurance engagements with certainty than audit or review of historical financial information.

BDO has performed procedures to obtain evidence of the information in .legal's description of PACTIUS and Privacy and the design 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.

BDO's test of the design of the relating technical and organisational measures and other controls and their implementation has included the control objectives and related control activities selected by PACTIUS and Privacy, 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 the related controls were appropriately designed and implemented on 10 August 2022.

Test procedures

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

Type	Description
Inquiry	Inquiries of relevant personnel 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.

For the services provided by Microsoft Azure within backup and hosting, we have from an independent auditor received an SOC 2 report on technical and organisational security measures relating to backup and hosting.

This sub-processor's relevant control objectives and related controls are not included in .legal's description of services and relevant controls related to operation of backup and hosting. Accordingly, we have solely assessed the report and tested the controls at .legal that monitor the operating effectiveness of the sub-processor's controls and ensure proper supervision of the sub-processor's compliance with the data processing agreement made by the sub-processor and the data processor and compliance with the General Data Protection Regulation and the Danish Data Protection Act.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

Result of test

The result of the test made of technical and organisational measures and other controls has resulted in the following exceptions noted.

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective,
- Technical and organisational measures and other controls related to a control objective are not suitably designed and implemented.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

Risk assessment		
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.*		
Control Activity	**Test performed by BDO**	**Result of test**
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 have made inquiries to relevant staff at the data processor. We have inspected that the data processor has prepared a procedure for annual review of 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 past year.	No exceptions noted.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.5: Information security policies

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
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 made inquiries to relevant staff at the data processor. We have inspected that the data processor has a management-approved IT security policy containing a policy for information security and personal data protection. We have randomly inspected that all employees have signed that they have read and approved the data processor's IT security policy. We have inspected that the policy was reviewed and updated on yearly basis.	No deviations identified.
Review of policies for information security ▶ The data processor has implemented an annual plan of controls which ensures periodical review of the information security policy. ▶ A written information security policy has been drawn up which is reassessed annually. ▶ The information security policy is updated and approved by Management.	We have made inquiries to relevant staff at the data processor. We have inspected that the data processor has set up a procedure for annual review and approval of the IT security policy. We have inspected that the policy has been reviewed and updated within the past year.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

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. GDPR art. 37, paragraph 1.*
- *To secure remote workplaces and the use of mobile equipment. GDPR art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
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 have made inquiries to relevant staff at the data processor. We have inspected that the data processor in their IT security policy has placed the responsibility for information security at the data processor's CEO and Head of Development. We have randomly inspected the data processor agreement and observed the specified contact information.	No deviations identified.
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 have made inquiries to relevant staff at the data processor. We have inspected that the data processors IT security policy and observed that they have guidelines for mobile equipment. We have by random sampling inspected that security measures are implemented for all workstations.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.7: Human resource security

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, art. 37, paragraph 1.*
- *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, point c.*
- *To protect the organisation's interests as part of the change or termination of the employment relationship. GDPR art. 28, paragraph 3, point b.*

Control Activity	Test performed by BDO	Result of test
Before employment ▶ A background check is made of all job candidates in accordance with business requirements and the function to be held by the employee.	We have made inquiries to relevant staff at the data processor. 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 the company has not hired new employees with access to personal data within the past 12 months. We have therefore not been able to test the procedure for implementation.	No deviations identified.
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 several times a year to ensure continuous focus on data protection and security.	We have made inquiries to relevant staff at the data processor. We have inspected that the employees must read and approve the IT security policy. We have randomly inspected that all employees have signed that they have read and approved the data processor's IT security policy. We have inspected that the data processor has a procedure to ensure that there is annual awareness in data protection and security. We have been informed that the data processor's procedure for ongoing awareness is new and no awareness has been held subsequently, we have therefore not been able to test the procedure for implementation.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.7: Human resource security

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, art. 37, paragraph 1.*
- *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, point c.*
- *To protect the organisation's interests as part of the change or termination of the employment relationship. GDPR art. 28, paragraph 3, point b.*

Control Activity	Test performed by BDO	Result of test
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 have made inquiries to relevant staff at the data processor. 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 inspected for one employee and observed that there are requirements for confidentiality during and after employment applicable to everything related to their work.	No deviations identified.
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 have made inquiries to relevant staff at the data processor. We have inspected that the data processor has a procedure for offboarding, which ensures that all accesses are closed, and material is handed over. We have inspected extracts of the data processor's employees with access to the data controllers' personal data and observed that the rights of the resigned employees have been removed.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.8: Asset management

Control Objective

- *To identify the organisation's assets and define appropriate responsibilities for its protection. GDPR art. 30, paragraph 2, art. 30, paragraph 3, art. 32, paragraph 2.*
- *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, point c.*

Control Activity	Test performed by BDO	Result of test
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 have made inquiries to relevant staff at the data processor. 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 observed that the record is updated regularly and by inquiry, we were informed that the record is made available to the supervisory authority upon request.	No deviations identified.
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 have made inquiries to relevant staff at the data processor. 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 deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.9: Access management

Control Objective

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

Control Activity	Test performed by BDO	Result of test
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 have made inquiries to relevant staff at the data processor. We have inspected the data processor's procedure for access control and observed that rights must be granted according to a work-related need. Upon request, we have been informed that no access has been granted within the last 12 months. We have inspected that one employee with rights to personal data has stopped within the last 12 months. We have inspected that the former employee with rights to personal data has been removed as a user.	No deviations identified.
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 CEO	We have made inquiries to relevant staff at the data processor. 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 recent periodic review of users and associated rights.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.9: Access management

Control Objective

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

Control Activity	Test performed by BDO	Result of test
Management of privileged access rights ▶ The data processor has implemented granting of administrative access to entities according to the functional need which is authorised. ▶ The data processor has implemented logging of accesses with privileged accounts (administrative rights).	We have made inquiries to relevant staff at the data processor. 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. We have inspected the most recent allocation of privileged rights and observed that it has been approved by a member of Management. We have inspected that the data processor has implemented logging of accesses with privileged accounts.	No deviations identified.
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.	We have made inquiries to relevant staff at the data processor. We have inspected the IT security policy and observed that all employees must use the password manager, LastPass. On sample basis we inspected that the users with access to personal data use LastPass and with a requirement for two factor authentication. On sample basis we inspected that all workstations have password requirements.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.10: Cryptography

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, point c.*

Control Activity	Test performed by BDO	Result of test
Encryption ▶ The data processor uses a SHA-2 SSL certificate with a minimum of 2048bit encryption	We have made inquiries to relevant staff at the data processor. We have inspected the data processor's encryption policy and observed that the systems must use a SHA-2 SSL certificate with a minimum of 2048bit encryption. We have inspected that the systems use a SHA-2 SSL certificate with a minimum of 2048bit encryption. We have further inspected that Azure also uses data encryption.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.11: Physical and environmental security

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, point c.*
- *To avoid loss, damage, theft or compromise of assets and disruptions in the organisation. GDPR art. 28, paragraph 3, point c.*

Control Activity	Test performed by BDO	Result of test
Physical perimeter safety guarding in office ▶ The established physical perimeter safety guarding agrees with the adopted security requirements.	We have made inquiries to relevant staff at the data processor. We have been informed upon request that the data processor does not have the data controllers' personal data located elsewhere than in Azure Europa. We have inspected that the data processor´s overview of sub-processors and observed that they have outsourced all hosting and backup to Microsoft Azure. 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.
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 have made inquiries to relevant staff at the data processor. We have inspected the data processor's policy for clean desk and automatic screen saver. We have randomly inspected documentation to automatically set up the screen saver on the employees' workstations.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.12: Operations security

Control Objective

- *To ensure proper and safe operation of information and data processing facilities. GDPR Art. 25, Art. 28, paragraph 3, point c.*
- *To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR Art. 28, paragraph 3, point c.*
- *To protect against data loss. GDPR Art. 28, paragraph 3, point c.*
- *To record events and provide evidence. GDPR Art. 33, paragraph 2.*
- *To ensure the integrity of operating systems. GDPR Art. 28, paragraph 3, point c.*
- *To prevent technical vulnerabilities being exploited. GDPR Art. 28, paragraph 3, point c.*
- *To minimise the impact of audit activities on operating systems. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
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 have made inquiries to relevant staff at the data processor. We have inspected the data processor's backup procedure and observed that it is in Azure. We have observed that the system must perform nightly backup of data in the production environment which is stored for seven days. In addition, there is a monthly backup that is stored for three months. In addition, we have inspected that annual residual test of the backup must be performed. We have inspected that the interval for backup has been implemented and that a restore test has been performed within the past year.	No deviations identified.
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 in order to sort these cases from other incidents.	We have made inquiries to relevant staff at the data processor. We have inspected that logging has been established and this happens in Azure, where events are logged. We have inspected that the data processor gets alert by mail regarding. We have inspected that the data processor has a separate process for dealing with breaches of personal data security.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.12: Operations security

Control Objective

- *To ensure proper and safe operation of information and data processing facilities. GDPR Art. 25, Art. 28, paragraph 3, point c.*
- *To ensure that information and personal data, including information and data processing facilities are protected against malware. GDPR Art. 28, paragraph 3, point c.*
- *To protect against data loss. GDPR Art. 28, paragraph 3, point c.*
- *To record events and provide evidence. GDPR Art. 33, paragraph 2.*
- *To ensure the integrity of operating systems. GDPR Art. 28, paragraph 3, point c.*
- *To prevent technical vulnerabilities being exploited. GDPR Art. 28, paragraph 3, point c.*
- *To minimise the impact of audit activities on operating systems. GDPR Art. 28, paragraph 1.*

Control Activity	Test performed by BDO	Result of test
Administrator and operator logs ▶ Procedures are implemented to ensure that all activities performed by systems administrator or employees with administrative rights are recorded.	We have made inquiries to relevant staff at the data processor. We have been informed upon request that all activity performed by administrators is logged. On sample basis we inspected that all activity performed by administrators is logged.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.13: Communications security

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
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). ▶ 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.	We have made inquiries to relevant staff at the data processor. We have inspected that the communication between the browser and the rest of the system takes place via HTTPS. We have inspected that exchange of data between the customers and the system takes place via SFTP.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

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

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
Development and maintenance of systems ▶ Formal processes and procedures have been implemented for all changes made in PACTIUS and Privacy. ▶ Development of PACTIUS and Privacy is based on principle of privacy-by-design and privacy-by-default based on risk assessment. ▶ Development of PACTIUS and Privacy 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 have made inquiries to relevant staff at the data processor. 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. We have been presented with an overview of changes within the past year and inspected on a random basis that all changes follow the change management procedure, so that all changes are tested and approved before they are rolled out. We have inspected that the data processor has separated production-, development- and test environments. We have inspected that fake data is used in the development and test environment and only personal data is used in the production environment.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.15: Supplier relationships

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
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 the data processor.	We have made inquiries to relevant staff at the data processor. We have inspected the data processor's supplier overview, and observed that only one sub-data processor, Microsoft Azure, is used for hosting and operation. We have inspected the data processor's data processor agreement with Microsoft Azure and observed that it places the same demands on Microsoft as the data controllers make on the data processor. We have inspected the data processor agreement and data processor agreement with Microsoft regarding the use of Microsoft Azure. We have observed that according to the agreement, only data centres in the EU may be used, and we have inspected documentation for this. From the Schrems II ruling of the European Court of Justice, it can be deduced that the use of a US cloud provider involves a transfer of personal data to the USA and thus a third country, regardless of whether the personal data is stored in the cloud provider's data centres in the EU. Furthermore, it can be deduced that a valid basis for the transfer of personal data to the United States requires the conclusion of EU standard contractual provisions as well as the introduction of effective, complementary measures. We have inspected that the data processor in collaboration with their owners and lawyer have jointly prepared a TIA. We have inspected that the data processor, in addition to the already implemented technical measures, has turned on the Customer lockbox so that the data processor must always approve if the sub-data processor needs to access data.	The data processor has stated that no personal data is transferred to third countries and that they have configured security measures to protect personal data using Azure as a sub-data processor. However, there is a risk of potential unintentional transfer of data from the sub-processor Azure to the third country USA, as Azure as a US-owned company is subject to US law. Based on the Danish Data Protection Agency's Cloud guidelines, an unintentional transfer will have to be considered as a personal data breach for the data processor. No further deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.15: Supplier relationships

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
Approval of sub-processors ▶ The data processor uses only approved sub-data processors.	We have made inquiries to relevant staff at the data processor. We have inspected the data processor's standard data processor agreement, and observed that the following sub-data processors are specified: ▶ Microsoft Azure We have inspected the data processor's supplier overview and observed that no other sub-data processors appear. We have randomly inspected two data processing agreements entered with the data processor's customers and observed that the agreements do not contain further sub-data processors than Microsoft Azure.	No deviations identified.
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 processor can object to the replacement of a sub-processor.	We have made inquiries to relevant staff at the data processor. 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. Upon request, we have been informed that there are no examples of change of sub-processors, which is why we have not been able to test for the implementation of the procedure.	No deviations identified.
Control with sub-processor ▶ The data processor uses a sub-processor for backup solutions, who provides an annual auditor's report.	We have made inquiries to relevant staff at the data processor. We have inspected the data processor's procedure for supervising sub-data processors and observed that the data processor annually checks that sub-data processors' auditor's statements	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.15: Supplier relationships

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
▶ The data processor performs an annual security check of third-party service providers that are part of the overall system.	and certifications are satisfactory, based on the data processor's risk assessment. We have inspected the data processor's supplier overview and observed that there is one supplier. We have inspected the SOC 2 report for Azure for and observed that no discrepancies were found. We have inspected that the data processor has supervised the sub-data processor and have assessed the SOC 2 report satisfactorily.	

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.16: Information security incident management

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
Handling of information security incidents ▶ All 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 have made inquiries to relevant staff at the data processor. We have inspected the data processor's procedure for breaches of personal data security and observed that breaches of information security breaches are the data processor's security officers who are responsible for the process in the event of a breach of personal data security. Upon request, we have been informed that there are no examples of breaches of personal data security, which is why we have not been able to test for the implementation of the procedure.	No deviations identified.
Reporting of information security 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 have made inquiries to relevant staff at the data processor. 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. Upon request, we have been informed that there are no examples of breaches of personal data security, which is why we have not been able to test for the implementation of the procedure.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

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

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
Implementation of information security continuity ▶ Contingency plans are prepared for relevant functions to ensure business continuance in connection with security incidents.	We have made inquiries to relevant staff at the data processor. We have inspected the data processor's contingency plan and observed that this ensures the continuation of the business in connection with security incidents.	No deviations identified.
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 have made inquiries to relevant staff at the data processor. We have inspected the data processor's procedure for annual testing. We have observed that it needs to be implemented and updated annually. Upon request, we have been informed that the procedure for testing the contingency plan is now, which is why we have not been able to test for the implementation of the procedure.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.18: Compliance

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
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 have made inquiries to relevant staff at the data processor. 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 inspected an extract of the data processor's customers for Privacy and PACTIUS. We have sampled two concluded data processor agreements. We have inspected the data processor agreements and observed that they have been accepted. We have inspected the data processor's data processor template and samples and observed that it contains information on the use of sub processors.	No deviations identified.
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 with us. ▶ Data processing agreements provide terms to the effect that the data controller must be informed of instructions which are not compliant with legislation.	We have made inquiries to relevant staff at the data processor. 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 randomly selected data processing agreements entered with customers and observed that the data processing agreements are in accordance with the service provided, are stored electronically, and include information on the use of sub-processors.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.18: Compliance

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
	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, we have therefore not been able to test the procedure for the implementation.	
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 have made inquiries to relevant staff at the data processor. We have inspected the data processor's data processor template and observed that the data processor must provide assistance regarding request for the rights of the registers and Articles 32 and 36. Upon request, we have been informed that the data processor has not received inquiries regarding the rights of data subjects and the specific requirements of the regulation. We have therefore not been able to test the procedure for the implementation.	No deviations identified.
Deletion and return of customers data ▶ Policies have been implemented to ensure protection of customer's confidential and sensitive information when offboarding a customer.	We have made inquiries to relevant staff at the data processor. We have inspected the procedure for offboarding of customers and observed that data processor has a procedure for deleting data upon customer termination. Upon request, we have been informed that upon termination of agreements, the data controllers can withdraw data themselves. We have inspected extracts of discontinued collaborations within the past year.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

A.18: Compliance

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
	We have randomly inspected that the data processor has followed their procedure for offboarding a customer, including has deleted the data controller's data.	
Independent review of controls - The data processor conducts an annual compliance check of policies, procedure an independent law firm to ensure compliance with the EU General Data Protection Regulation (GDPR).	We have made inquiries to relevant staff at the data processor. We have inspected the data processor's procedure for compliance with legal and contractual requirements and observed that once a year the data processor's management asks their lawyer to assess whether there have been changes to the above legislation in a way that requires changes to the security policy and / or to the system. We have inspected that the law firm in August has reviewed and confirmed that the data processor's procedures and policies are in accordance with applicable law. We have inspected that the data processor has reviewed the law firm's evaluation.	No deviations identified.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

HAVNEHOLMEN 29
1561 KØBENHAVN V

CVR NO. 20 22 26 70

BDO Statsautoriseret revisionsaktieselskab, a Danish limited liability company, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO in Denmark employs almost 1,300 people and the worldwide BDO network has more than 97,000 partners and staff in 167 countries.

Copyright - BDO Statsautoriseret revisionsaktieselskab, CVR No. 20 22 26 70.

Penneo dokumentnøgle: 7EVCF-8TZHV-TL7PZ-WF7LZ-222TG-EAOD7