IT SECURITY MEASURES

Applicable from 16 April 2024

The following describes .legals technical and organisational security measures for the Services. In addition, an audit statement, ISAE-3402 or equivalent, is prepared annually and can be downloaded here.

A.4 RISK MANAGEMENTS

Annual risk assessment

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

Guidelines and control objectives

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

The control objectives include:

- **A.** Purpose: Describes why the control objective is established and ensure that it reflects the overall guideline for the ISO section.
- **B.** 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.
- **C.** Threshold: Shows what is required to meet the control objective.

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

A.5 INFORMATION SECURITY POLICIES

IT security policy

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

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

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

A.6 ORGANISATION OF INFORMATION SECURITY

IT security manager

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

Segregation of duties

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

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

A.7 HUMAN RESOURCE SECURITY

Confidentiality

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

A.8 ASSET MANAGEMENT

Inventory of assets

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

A.9 ACCESS CONTROL

Principles of access control

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

Secure login with two-factor authentication

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

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

Roles and rights management

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

Privileged access management

An employee with a need for access to production data or production infrastructure (privileged access) must, in addition to a work-related need, have separate approval from the Executive Board. Employees with privileged 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 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 "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 SECURITY

Physical security of premises and machines

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

A.12 OPERATIONS SECURITY

Secure hosting

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

A. The code is stored and managed in Azure DevOps.
B. Data is stored in Azure Storage, Azure SQL and Azure Cosmos DB in European data centres.
C. 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 (e.g., 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

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. In addition, there is a monthly backup that is stored for 3 months.

Privacy and DPA Service 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, several 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 Storage: 99,99%

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

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 penetration tests 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 product owner with responsibility for planning and prioritising as well as a permanent development team with responsibility for the 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 discussions that address any challenges and help each other to effective solutions. We have more eyes on the changes we make and actively try to constantly improve our skills and improve the systems we work with.

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

Quality assurance

Quality assurance elements from the common .legal development process:

A. Structured process

i. All work, regardless of character, is visualised as tasks in our task management. All tasks must go through the same overall process with several phases, including code review, internal testing, and acceptance testing.

B. Automated quality assurance
   i. Version-controlled code
   ii. Continuous integration which continuously builds the code to ensure the integrity
   iii. Automated tests that runs continuously to minimise regression errors
   iv. Automated deployment pipelines which mean that we can safely and with high traceability deploy new code for tests and production environments.

C. Development, test, and production environment
   i. Dedicated development, testing and production environments to be able to ensure quality on several levels before new code reaches the production environment.

D. Monitoring and alerting
   i. Our environments are monitored so that we can ensure high uptime and receive alarms about any errors or vulnerabilities as quickly as possible.

A.15 SUPPLIER CONDITIONS

Supplier agreements

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

Supplier agreements

A. .legal performs an annual security check of third 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:
   i. When the incident took place
   ii. What the incident was actually about
   iii. Who reported the incident

3. The incident is then analysed with a view to the following:
    i. Determine how extensive the incident is
    ii. Which customers are affected
    iii. 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.

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:

A. 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)

B. 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 the security policy and/or the system. The result of the request is noted at the board meeting and any resulting changes are implemented.