GDPR SECURITY MEASURES

Applicable from 16 November, 2022

The following describes .legals technical and organisational GDPR security measures for the Services. In addition, an audit statement, ISAE-3000 or equivalent, is prepared annually and is available here.

Our technical and organisational IT-security measures are described here.

A.4 Risk management

Annual risk assessment

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

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

Guidelines and control objectives

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

The control objectives include:

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

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.

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.

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 unauthorized physical access and environmental incidents.

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.

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

Supplier control

.legal performs an annual security check of third party service providers that are part of the overall 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 to stop and contain the incident:

1. The security incident is registered in the company's task management.
2. In the description of the task, the security incident/weakness is noted in as detailed as possible, including as a minimum:

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

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

3.1 Determine how extensive the incident is
3.2 Which customers are affected
3.3 What needs to be done to either stop the incident or accommodate the incident in the future e.g., for code corrections

4 Customers identified in point 3 are then informed about the incident and the consequences of the incident, as well as what measures have been taken in the future.
5 The measures that have been decided are prioritised and implemented
6 Once the measures have been implemented, the task is closed.
7 After the problem is solved, the process is described as an incident in the project's incident log. The purpose is to investigate whether there is an underlying problem that may give rise to further improvements or help remedy similar future problems.

Procedures have been implemented based on the data processing agreements with our customers. This is done to ensure correct management of security incidents within the agreed frame. A template has also been implemented to be used for reporting of breach of the Regulation to the

data controller which ensures that all necessary information is provided, for the purpose of further consideration on the part of the data controller.

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

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

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 subprocessors. 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 authorized by the data controller.

Deletion and return of customer's data

.legal has implemented instructions which ensure that personal data are deleted or returned according to the data controller's instructions 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.