

# Tech & Security

Non functional information regarding technical and security issues. GDPR, terms and technical descriptions in our SaaS "My Pages".

- Non Functional Matrix
  - Tech Matrix
- Technical Descriptions
  - Tech behind the SaaS
  - Single Sign On

# Non Functional Matrix

# Tech Matrix

## General security requirements

Requirements	Yes, No, N/A	Comment from Leasify
<b>General security requirements</b>		
Do you have a specific contact person for all security related issues and escalations in relation to Customer data?	Yes	Claes Ivarsson is our single contact for the application issues.
Have all personnel with access to Customer data signed an NDA?	Yes	Via company policy and employment agreement
Are you certified to any relevant security standard (e.g. SS-ISO/IEC 27000)? What context have been certified?	No	
Have you been subject to any investigations by data protection authorities the last three years? If yes, specify.	No	
Do you have an internal data protection and security handbook/ policy for your employees?	Yes	
Do you regularly provide training to staff on data processing obligations, identification of breaches and risks?	Yes	Our team is continuously working with these issues.
Do you have cyber security/data protection insurance coverage?	Yes	
Do you have an audit trail of the processing of Customer data (who, what, when, why) and access logs to all Customer data and applications and do you monitor the audit trail for suspicious or disallowed behaviour?		Partial not all data, only essential, eg contracts, reports. We are working on extending logs and audits.
How long do you store log data?		12 months
<b>Process and logging requirements</b>		
Do you have a process for returning or permanently destroying Customer data? If yes, please describe.	No	We have a manual process step/checklist for deleting customer data after requests.
Do you have an incident management and notification process in place for the services provided to the Customer? If yes, please describe	Yes	We have a status monitoring for customer access and support via email/phone.
Do you have a vulnerability and patch management process in place for all components used to provide the service to Customer? If yes, please describe	No	We make use of Githubs component check (vulnerable dependencies and security checks) and reports. And we continuously upgrades any external package used in our application via composer.
Do you have measures in place to maintain the capability to proactively prevent, monitor, detect, investigate, and respond to IT security and privacy incidents associated with Customer data?	Yes	
How often do you regularly test the security and effectiveness of your security and privacy controls?	1/year	Pen-tests planned to spring 2023
Do you have documented and tested backup and restore processes to ensure Customer data can be restored?	Yes	Services via Cloudnet concept.

Are your backups encrypted and protected from tampering with secure cryptographic algorithms and key lifecycle management? Describe the solution and the key management process.	Yes	All access to backup is stored via SSH-key access and logged by Cloudnet.
Are you able to protect Customer data from unauthorized access in all phases of the information lifecycle, including but not limited to service test, deployment, incident processing and disposal?	Yes	We have this issue as an ongoing and continuous work forward, doing our best.
Have you ensured physical security on premises including policy for personnel to manage information and data in locked-away and secure facilities?	Yes	No physical access to servers possible.
Do you have a process for secure data disposal?	No	We do not use our own physical hardware for the SaaS-service. But the developers computers are stored and cleared out in the service program.
Are you able to, in a timely manner, apply decommissioning and secure wiping of old software, hardware and deployments?	Yes	All our software and code is version controlled and under continuous delivery / management.
Do you have real-time protection against intrusion and malware installed in infrastructure and on all hosts? If yes, please describe which type of controls are deployed.	Yes	We have WAF and DDOS monitoring via CloudFlare.
Do you apply encryption of all managed or unmanaged devices that can access or store Customer data, ensuring appropriate protection of the encryption/decryption keys?	Yes	
Do you apply encryption of personal data or data by Customer classified as sensitive in transit by using suitable encryption solutions (e.g. TLS 1.2+ and IPsec VPN, SSH2+ or PGP), using only best practice configurations and key management?	Yes	This is an ongoing work daily to get the data more safe and encrypted.
Have you implemented a versioned secure configuration (hardened) on all devices?	Yes	Cloudnet provides all active servers with their concept.
Do you support the use and enforcement of multi-factor authentication for accessing Customer data if requested?	Yes	Customers can activate 2FA on their accounts and make use of SSO if wanted.
Do you have sufficient DDoS protection to ensure service availability?	Yes	We use third party Cloudflare to protect us from DDOS attacks.
Is your service developed in a manner enabling you to follow a good practice model e.g. OWASP Top 10?	Partial	This is a continuous work forward. But we do not follow everything in 100%, really hard to get full OWASP-coverage.
Do all users have personal accounts? If not, specify which accounts are shared/anonymous and not personal.	Yes	
Do you have measures in place where access to Customer data must be granted only based on relevant needs and revoked when not used?	Yes	Partial and continuously increased after need.
Do you have a policy for strong, unique passwords of sufficient complexity and regular expiry on all devices, along with password management guidelines for all staff?	Yes	It's a balance of usability and security. The best is 2FA forced to all users in a company. We have custom level of password settings/req.
Are shared authentication secrets (keys, passwords etc) protected from unauthorised use and is any use of them fully audited?	Yes	We store all pass and keys encrypted and locked from external access. And it is an audited access.

<p>Is the location where Customer data is stored equipped with appropriate physical security controls? Please comment.</p>	<p>Yes</p>	<ul style="list-style-type: none"> <li>• Access to the data center floor is restricted to data center employees and authorized visitors.</li> <li>• Data Centers are staffed 24/7/365 with security guards and technicians.</li> <li>• All employees and visitors are identified using biometrics and state issued Ids before entering the facility.</li> <li>• HVAC and power have redundant systems, so if one goes out, the others keep our systems powered and within operating temperature.</li> <li>• All of the systems are segregated from other tenants by locking cabinets. Only datacenter staff assigned to supporting the systems have access to the keys.</li> <li>• Multiple Internet carriers using independent fiber connections to the data center floor.</li> <li>• Our networks within the data centers have redundant routers, switches, and service providers. Multiple systems can fail without affecting downtime or performance.</li> </ul>
<p>Are your servers used for Customer data located in, and only accessible from, EU/EES? If not please specify locations and legal ground for transfer.</p>	<p>Yes</p>	<p>█</p>
<p>Do you have a disaster recovery plan for services provided to Customer that are in accordance with best industry practice and regularly updated?</p>	<p>Yes</p>	<p>Automatic backups and "fire" practice evert Q.</p>
<p>Do you engage sub-processors for the service provided to Customer? If yes, please list identity and location of all sub-processors.</p>	<p>Yes</p>	<p>We use:• Cloudnet servers for hosting and database storage with backup. • AWS North-1 for S3 long term data storage (prim documents) • AWS Ireland for OCR-scanning with Textract (will move to Sweden as soon as available)</p>
<p>Have you executed data processing agreements covering GDPR requirements for all sub-processors involved in the services?</p>	<p>Yes</p>	<p>We hope so but following the latest Schrems II –act it is somewhat impossible. More to come in this area...</p>
<p>Have you ensured that all sub-processors a) process Customer data in line with legal requirements? b) only process Customer data to the extent necessary to fulfil the contract between you and Customer? c) have established technical and organizational measures at least as strict as the obligations between you and Customer? d) have implemented measures to maintain the retention times for Customer data? e) have established incident/ disaster recovery plans regarding Customer data? f) will, on Customer request, return or destroy any Customer data?</p>	<p>Yes</p>	



# Technical Descriptions

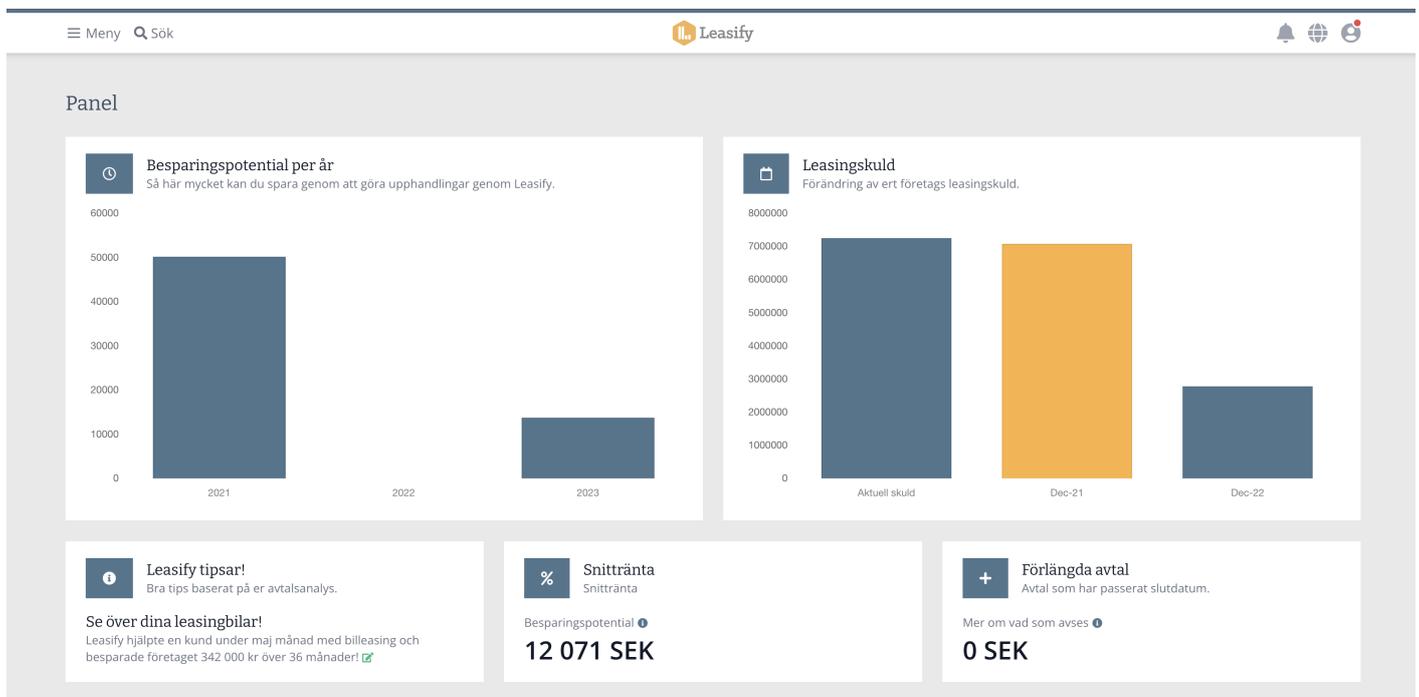
# Tech behind the SaaS

**Stockholm, 13 Sept 2023**

Leasify's SaaS service "My pages" is described here in a technical basic perspective and the document should be seen as a living document as development progresses rapidly with new requirements and versions over time.

**Remember that we have GDPR including the PUB agreement which is the basic agreement for the regulation of data handling, security and requirements. This document in no way supersedes these agreed upon agreements.**

<https://wiki.leasify.se/books/tech-security/chapter/general-terms-and-conditions>



## Hosting

Leasify manages the operation on its own and it is located in the cloud environment at Amazon Web Services (AWS) with a location in Stockholm / eu-north-1. We monitor, adjust, and manage our primary operating environment <https://app.leasify.se>.

All access is via encrypted SSH access with logging and ongoing personal control.

The server environment and databases are located in eu-north-1 / Stockholm for the best response time and uptime.

Amazon's AWS (data center eu-north-1 / Stockholm) is also used for long-term storage of documents, OCR scanning, and AI services with programmatic access for the highest control and logging.

## Security and Backup

All services Leasify uses have 2-factor authentication turned on.

The traffic towards operation servers goes via Cloudflare and WAF to be able to quickly block unauthorized traffic if necessary.

As option we will require either BankID or the 2FA option for all Leasify users in the system.

Backup takes place continuously (3 times a day) with rotation with a 6-month possibility of restoration according to a specific schedule. Total backup restore is handled manually upon request.

Access logging takes place on an ongoing basis partly against web servers, but also against the work steps that take place in the application, such as contract changes and report extraction.

Operational monitoring can be visited from outside via <https://status.leasify.se/>

## Continuous Delivery

All code is versioned and set up with continuous delivery (CI) via tests across version notations. We minimize interruptions during deliveries and thus have no specific time windows for taking down the service during upgrades.

If longer interruptions are required, messages about this will be sent out well in advance of the event and these major upgrades are usually made outside Swedish office hours, more specifically before 07:00 and after 17:00 (Stockholm, GMT+1).

## Development Methods

The development takes place according to Scrum with 3-week sprints with delivery schedule and demo as well as retro. We use tools for all development with epics, boards, burndown reports and documentation.

Developed functions are demonstrated via "What's new" in the application which comes as notifications for all users.

# Integrations

We communicate with various services for interest rates, rates and financial data. Examples of these are Banksigtering, Riksbanken, Fixer/Morningstar. Full third party service list can be acquired if needed.

The service today offers limited integration in the form of certain data over CSV and DTO.

We are happy to see future partners for integrations with our service. We have a very malleable platform with possibilities for communications over REST API with the desired services.

# Language Localization

The SaaS application is primarily developed in Swedish and support is available for English.

The application language for user selection has support for sv,en,da,nb,fi,it,lv,ee and can be extended upon request.

# Development Roadmap

The following development points are currently in focus:

- Extended AI-chat support as complement to the wiki.
- Wiki about all functions of the service.
- External integrations with partners and other systems.
- Procurement and financial requests.

# Technical Contact

For further information, questions and requests regarding this information, the easiest way to contact:

Andreas Ek, CTO, +46703032203, [andreas.ek\[a\]leasify.se](mailto:andreas.ek@leasify.se).

# Single Sign On



## What is Single Sign On?

Single Sign On (SSO) is a function for easier login and authorization control via third party. Often, companies already have a centralized management of accounts that is controlled continuously.

It is also convenient as a user not to have to remember yet another password for the next service.

Above all, this raises the minimum level for security in external applications.

## How can we get SSO?

Activate the "Single Sign On" module under company settings. You can test it for free for 10 days. Go to company settings and "Change information". There, after activation, there will be a "Single

Sign On" tab.

Select Azure and save, try logging out and then logging in again via SSO.

If it works well, activate "Require from all" and email login will no longer be possible for your company to "My Pages" at Leasify.

## Future upgrades?

The following development plan applies to SSO, which will arrive shortly:

- Auto-create accounts according to domain specification.
- Customer-specific AAD providers.
- Google Apps as provider.
- LinkedIn as provider.
- Automatic connection from AAD groups to Leasify groups.

## Wishes

If you have requests or feedback regarding SSO, please contact Andreas Ek, andreas.ek[a]leasify.se, +46703032203!