

# 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.  |

|   |     |  |
|---|-----|--|
| Is the location where Customer data is stored equipped with appropriate physical security controls? Please comment.   | Yes | <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> |
| 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.  | Yes |  |
| Do you have a disaster recovery plan for services provided to Customer that are in accordance with best industry practice and regularly updated?  | Yes | Automatic backups and "fire" practice every Q.   |
| Do you engage sub-processors for the service provided to Customer? If yes, please list identity and location of all sub-processors.   | Yes | 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)   |
| Have you executed data processing agreements covering GDPR requirements for all sub-processors involved in the services?  | Yes | We hope so but following the latest Schrems II –act it is somewhat impossible. More to come in this area...  |
| 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? | Yes |  |

Revision #1

Created 13 September 2022 12:42:51 by Andreas Ek

Updated 13 September 2022 12:55:40 by Andreas Ek