tomhrm

tomHRM Security

March 2025

Table of Contents

Introducing tomHRM

tomHRM is a comprehensive SaaS platform that supports numerous companies worldwide in optimising HR processes. We safeguard your organisation's valuable data, allowing you to focus on the most critical aspects—team and organisational development. Discover the specifics of our data security approach and understand why hundreds of companies entrust us with their most valuable assets: employee information.

Physical Security

The tomHRM application and its data are hosted in data centres operated by OVH and Amazon (AWS S3). The data centres serve tens of thousands of clients worldwide and meet the highest security standards.

Location
All data is stored within the European Union.
To enhance security, backups are encrypted and stored across several locations.

Our data centre providers hold a range of certifications attesting to their compliance with the highest standards of security, data processing, and adherence to legal regulations.

ISO 27001	ISO 27017	ISO 27018
ISO 27701	SOC 2	SOC 3

Network Security

Network security is a critical layer of protection for server infrastructure and the application against threats such as malware and DDoS attacks. We employ Cloudflare*, which optimises data flow and implements advanced rules and access controls through an integrated Web Application Firewall (WAF).

Guaranteed availability of 99.95%.
We ensure a 24/7 operational continuity of tomHRM and 99.95% service availability thanks to technical solutions such as load balancing, infrastructure redundancy, systematic backups, and regular data recovery testing.

We have also implemented a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP).

App Availability Status
You can find information on the current service availability and scheduled maintenance at https://status.tomhrm.app/

*For more details on Cloudflare security solutions, visit https://www.cloudflare.com/trust-hub/

Application Security

Single Sign-On Authentication (SSO)
tomHRM allows traditional credential-based authentication and SSO authentication via SAML (Okta, OneLogin) or with Google Login, Microsoft Login, or Slack Login.

Two-Factor Authentication (2FA)
tomHRM supports Two-Factor Authentication with Google or Microsoft account. The 2FA can be implemented as either mandatory for all users, or optional.

Flexible Access Control System
tomHRM provides an advanced access control system. The first tier, based on permission groups, allows a matrix-like setup for access to modules, actions, and data. The second tier employs user roles, enabling access to specific data or actions within individual modules. With full flexibility in security configuration, the system can be tailored to organisations of all sizes.

Login and Passwords Policy Management
tomHRM allows you to define a number of user log-in parameters, such as:

- password validity
- account lockout after unsuccessful login attempts
- automatic login after session expiry
- automatic logout after a period of inactivity
- forcing a password when downloading documents

Audit Logs and Change Logs
The application provides audit logs and change logs, which contain critical information about events.

Antivirus
Antivirus scanning is employed universally when uploading or downloading files.

Application Testing
We conduct both manual and automated testing, focusing on verifying functional integrity. We run penetration tests, including configuration security analysis, API security assessments, and vulnerability checks for attacks such as Cross-Site Scripting, SQL/JS/HTML Injection, Cross-Site Request Forgery, Session Weaknesses, among others.

Contact us if you would like to receive our penetration test certificate

Backups

Backups ensure the continuity and availability of tomHRM service and are an element of our *Business Continuity Program* (BCP) and *Disaster Recovery Plan* (DRP).

Backup Policy

- Backups are executed twice a day.
- Data is stored in two indepentend geographical locations* by two separate providers.
- Backups are categorised into *Warm* and *Cold* types.
- Backups are stored in encrypted form (AES methodology).

*If you need to store data in a country or region other than the default, contact us.

Data Security

Encrypted Data
AES-256 encryption is used for data at rest and TLS for data in transit, ensuring an encrypted connection between the server and the browser.

Backups
Bi-daily backups minimise the risk of data loss.

Multi-tenant Architecture
The use of multi-tenant architecture, with individual client databases, significantly increases the data access security, as compared to traditional solutions. Additionally, each client's files are stored in separate locations, with access strictly governed by a unique, account-specific key.

Company Security

Asset and Digital Resource Management
We maintain a register of assets and digital resources that are subject to access management procedures.

Employee Training
All our employees attend both internal and external training sessions on data security and the handling of personal data.

HR Security
All new hires undergo onboarding, which includes essential training in key areas such as internal security policy, GDPR compliance, and AI solutions. Each employee is required to sign a Non-Disclosure Agreement (NDA) and accept workplace security regulations.

Procedures
We have implemented a Business Continuity Plan (BCP), which also encompasses a Disaster Recovery Plan (DRP), and we conduct risk identification. In compliance with the GDPR, we maintain a record of security incidents.

IT Security

- We have implemented an access management procedure for digital/IT resources.
- We utilise SSO and 2FA wherever feasible.
- We employ authorisation keys and other safeguarding mechanisms.
- We deploy antivirus/anti-malware software and firewalls on workstations.
- We enforce a clean desk policy.

Legal Compliance

tomHRM is fully compliant with the European data protection regulations:

- the GDPR Regulation (EU) 2016/679 and the EU-US Data Privacy Framework
- the Whistleblower Protection Directive (EU) 2019/1937

We adhere to personal data processing principles:

- lawfulness, transparency, and fairness,
- data minimisation and purpose limitation,
- data accuracy,
- storage limitation,
- integrity, confidentiality, and accountability.

The use of our service is regulated by two documents:

- Terms and Conditions outlining the principles of service provision
- Data Processing Agreement (DPA) for delegating personal data processing

We collaborate with third-party data processors
after a thorough evaluation of their practices.

- We conduct analysis and risk assessment of subcontractors in terms of security, privacy and data confidentiality
- A list of the categories of data processors is available in the data processing agreement.
- Customers are notified of any changes in subcontractor structure.
- We respect client autonomy and provide a period for objecting to the changes.

Contact Details

The provider of tomHRM is

ENNOVA Mirosław Nowoszewski Spółka Jawna
ul. Sadowa 7/13
82-300 Elbląg

NIP: 5782976225
REGON: 280216540
KRS: 0000282777

The company was registered in June 2007, at the District Court in Olsztyn, Division VIII of the National Court Register.

Data Protection Officer
Mirosław Nowoszewski

tomhrm.com

This document is intended solely for informational purposes and does not guarantee freedom from errors, nor is it subject to any other warranties.

FOR FURTHER INFORMATION
Please contact our Sales Department or your account manager.