Security at PayFit

Whitepaper

— Public document —
Version 1.4 - Last edition: 06/02/25

PayFit

Summary

PayFit

Introduction

PayFit is a Software-as-a-Service solution to friendly and efficiently help companies handling human resources and payroll management.
By nature of its services, PayFit processes highly confidential information about its customers' finances, leaves, contracts, etc. Therefore, protection of customer data is part of PayFit product, just like delivering payroll every month.

PayFit is dedicated to implement and enforce effective controls and continual improvement of its Information Security Management System.
In line with this mission statement, PayFit provides:

- Global engagement compliant to ISO/IEC 27001 on each point of data security
- Systematic protection of data confidentiality, by several monitored and logged mechanisms of access protection and information encryption
- Strict control of data integrity, to guarantee that documents are protected against any unauthorized access, alteration or loss
- Robust infrastructure offering constant data availability
- Traceability of every user's main action, as of every action on databases.

PayFit controls, restricts and monitors that only authorized employees and partners have access to confidential or sensitive information, in strict proportion to the need to know, as to the goal of their mission and only during its duration.
PayFit is committed to protecting users' personal data according to the General Data Protection Regulation (GDPR), by processing it lawfully, fairly, in a transparent and secure manner in relation to the data subject.
PayFit is willing to continually increase all employees' and outside parties' awareness of information security benefits and their daily contribution to it.

The Information Security team is in charge of designing, coordinating, applying, monitoring and auditing all the processes and operations necessary to enforce this Information Security Policy.

Firmin Zocchetto
CEO & Co-founder

ISO 27001

PayFit is ISO 27001 certified, demonstrating thereby its engagement to maintain a secure platform for its customers, under strict design, procedures, controls and continual improvement.

Certificate No IS 706245 - Effective date: 2023-09-09 - Expiry date: 2025-10-31

Therefore, in line with its mission statement and Information Security Policy, PayFit provides a global engagement that conforms to the international ISO 27001 norm:

- In all its provisions and more than 114 points of controls, without any exception
- For all PayFit operations and products
- In every actual site as to come.

PayFit has been audited by BSI, a world leader in standards and certification, and is ISO 27001 certified since September 2020 with the latest review in August 2023: the certificate can be obtained on our dedicated page on information security.

Information security policies

- A set of policies for information security has been defined, approved by management, published and communicated to employees and relevant external parties.

- All information security policies contain statements concerning:

    - Definition of information security, objectives and principles to guide all activities relating to information security inside PayFit

    - Assignment of general and specific responsibilities for information security management to defined roles.

    - Processes for handling deviations and exceptions.

- At a lower level, the information security policies are supported by topic-specific policies including:

    - Access and asset management
    - Physical and environmental security.
    - Communication security
    - Information classification
    - Operations security
    - Suppliers security
    - Incident management
    - Secure development
    - Continuity management
    - Change management
    - Configuration management

People

- All candidates' backgrounds are checked, according to relevant laws and aligned with the business requirements, on employment history as on degrees and qualifications.

- All employees are required to sign a confidentiality agreement and to follow the internal digital policy, as part of the global internal regulation.

- Security training for all employees is regularly performed.

- Each development and management tasks, and their relative duties, follow a RACI matrix structure, allowing to segregate the roles of developing, consulting and validating.

Facilities

- Physical access to PayFit facilities is protected by individual identification badges.
- Offices are monitored 24x7 by an alarm system with video-surveillance capabilities.
- Physical accesses are logged for 30 days.
- Visitors and external staff are under the mandatory direct supervision of a PayFit staff member.

Assets

- Centralized management with global inventory, monitoring and alerting capabilities.
- Device security policy globally enforced and managed (auto-lock, password complexity and rotation, real-time protection against malware, firewall, disk encryption, restriction on software installation, auto-updates, remote lock and erase capabilities).
- Global policy of tools authorized to handle assets by information types and classification frame.
- Access to source code strictly controlled, with systematic peer review on new code merging.
- Mandatory global Procurement Policy prior to any supplier employment, with systematic security, legal and finance authorization.

Data

- All data, including backups, are stored in France.
- All stored data are encrypted in transit and at rest, including any backup copies of the data. Besides, sensitive data are anonymized or not transmitted to sub-processors.
- Users must authenticate themselves by email and password (controlled by a strict policy), with the option of a second factor of authentication (2FA) received by SMS.
- Internally, access to data, by authorized staff members only, happens through a VPN, protected by 2FA authentication.
- Data transmission is performed through TLS/SSL only with HSTS and Perfect Forward Secrecy fully enabled. PayFit certificates score an "A" rating on SSL Labs' tests.
- Only the onboarding team, support team and technical teams are authorized to access customer data, with a proportional and justified reason to do so. Such accesses are systematically logged.

Legal

- Payroll system accuracy and compliance tested by the best experts in the field.
- Computation reliability is ensured by automatic testing and verification.
- An internal team is solely dedicated to legal and conventional monitoring.

Privacy & GDPR

Protecting the privacy of individuals who provide us with personal information is of utmost importance to PayFit and the way we do business.

To this end, we are committed to respecting data privacy legislation, and in particular the General Data Protection Regulation. Please read more about our engagements below.

payfit.com/en/privacy-policy

payfit.com/en/gdpr

Suppliers

- All new information systems are controlled by a procurement process, which includes security, financial and legal review.

- Information security risks requirements are addressed in every contract, defining the frame to access to and exchange confidential and/or sensitive data, as to communicate without delay about security events.

- Specific contractual dispositions allow PayFit to assess regularly if the supplier is maintaining existing information security policies, procedures, and controls.

Hosting & Network

- All hosting facilities are managed directly by Amazon Web Services in the EU-based data centers, in respect of ISO 27001 and SOC2 type II controls, among other certifications.

- All transmissions between client and server and to external systems are performed through end-to-end HTTPS encryption.

- PayFit network is split into sub-networks, each handling a specific function, both for performance and security enhancement. Testing and production environments are strictly separated.

- PayFit network is isolated from the Internet, with the exception of a single entry point (proxy). Each point inside the network follows strict firewall rules.

- Accesses to PayFit systems are protected through AWS and Kubernetes rights management. Access to data, by authorized staff members only, happens through a VPN, protected by 2FA authentication.

- Data transmission from IT system that stores or processes personal data is monitored and logged.

- All servers are synchronized through an AWS NTP server.

Logging

- Audit logs are deployed to trace authentication and monitor logical system access, as well as data access and modifications.
- Systems technical events, like errors, are monitored and logged separately.
- Access to logs happens through a specific namespace, a VPN, with mandatory 2FA authentication and is password protected.
- Logs data are automatically replicated on 3 nodes in 3 different areas in France (AWS servers, certified ISO 27001). All those data are handled on servers with automatic failover system.
- Retention of audit logs is set as required by regulations.

Availability & Resilience

- All data are continually replicated on 2 nodes for our databases and 3 nodes for our AWS S3 storage. Each node is hosted in a specific data center, separated from others. All data are handled on servers with automatic failover system.

- Backups are performed every 1 hour and their full recovery process verified daily.

- Backups are transmitted through end-to-end HTTPS encryption.

- Backups are replicated 3 times. All accesses are protected through AWS and Kubernetes rights management.

Incident & Continuity

- PayFit has implemented a formal procedure for security events and has educated internally all staff members on it.

- When security events are detected, they are escalated to our emergency alias, teams are paged, notified and assembled to rapidly address the event.

- The analysis is reviewed in person, distributed across the company and includes action items that will make the detection and prevention of a similar event easier in the future.

- Security events must be systematically reviewed for closing by engineering, security and specifically concerned departments if any, like legal and/or communication.

Audits

- PayFit uses technologies such as Sentry and AWS Cloudtrail to provide an audit trail over its infrastructure and the PayFit application. Auditing allows to perform ad hoc security analysis, track changes made to PayFit setup and audit access to every layer of the stack.

- PayFit runs a private bug bounty program on HackerOne to identify and mitigate security threats. Access to this program is by invitation only.

- As part of the continual ISO 27001 certification process, PayFit's Information Security Management System is audited every year by independent third parties.

Contact

- James Moos — VP of IT & Security
- security@payfit.com
- Twitter

payfit.com/en/security