# Security at PayFit

## Whitepaper

PayFit

# Summary



PayFit

# Information Security Policy

PayFit is a Software-as-a-Service solution to friendly and efficiently help companies handling human resources and payroll management.

PayFit is dedicated to maintain a secure platform for its customers, by satisfying information security requirements, in terms of effective controls and continual improvement of its Information Security Management System.

In line with its mission statement, PayFit will provide:

- a global engagement conform to ISO 27001 on each point of data security: people, physical security, data access, hosting & networks, logs, availability, audits
- a systematic protection of data confidentiality, by several monitored and logged mechanisms of access protection and information encryption
- a strict control of data integrity, to guarantee that documents are protected against any unauthorised access, alteration or lost
- a robust infrastructure offering constant data availability

PayFit will control, restrict and monitor that only authorised employees and partners can 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 secured 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.

# 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 intern regulation.

- Security training for all employees are performed regularly. Intern security policies are quarterly reviewed.

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

# Physical

- 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 during 45 days.
- Visitors and external staff are under mandatory direct supervision of a PayFit staff member.

# Assets

- Centralised 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 malwares, firewall, disk encryption, restriction on softwares installation, auto-updates, remote lock and erase capabilities).
- Global policy of tools authorised to handle assets by information type and classification frame.
- Access to source code strictly controlled, with systematic peer review on new code merging.
- Centralised rights management on all Software-as-a-Service.
- Mandatory global Procurement Policy prior to any supplier employment, with systematic security, legal and finance authorisation.

# 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 anonymised 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 authorised staff members only, happens through a VPN, protected by 2FA authentication.
- Data transmission are performed through TLS/SSL only with HSTS and Perfect Forward Secrecy fully enabled. PayFit certificates score an "A" rating on SSL Labs' tests.
- Only onboarding team, support team and technical teams are authorised to access customer data, with a proportional and justified reason to do so. Such accesses are systematically logged.

# Legal

- Payroll system tested by the best experts in the field (especially Pierre-Jean Fabas, editor in chief of legisocial.fr).
- Computation reliability is ensured by automatic testing and verifications.
- An internal team is solely dedicated to legal and conventional monitoring.

# Hosting & Network

- All hosting facilities are managed directly by Amazon Web Services, in respect of ISO 27001 controls.
- All transmission between client and server and to external systems are performed through end-to-end HTTPS encryption.
- PayFit network is split into subnetworks, 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.
- Access to PayFit systems are protected through AWS and Kubernetes rights management. Access to data, by authorised 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 synchronised 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 name space, a VPN, with mandatory 2FA authentication and is password protected.

- Logs data are automatically replicated on 3 nodes in 3 different area in France (AWS servers, certified ISO 27001). All those data are handled on servers with automatic failover system.

- Retention of audit logs is set to one year.

# Availability & Resilience

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

- Backups are performed on an hourly basis and their full recovery process verified on a daily basis.

- 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 Response

- 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, legal, communication and specifically concerned department if any.

# Security 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.

# ISO 27001

PayFit is dedicated to maintain a secure platform for its customers, by satisfying information security requirements, in terms of effective controls and continual improvement of its Information Security Management System (ISMS).

To this end, in line with its mission statement, PayFit will provide a global engagement conform to ISO 27001 on each point of data security: people, physical security, data access, hosting & networks, logs, availability, audits.

PayFit has undertaken the certification process with BSI, a world leader in the field. PayFit aims to obtain the certification in Q1 2020.

# Contact

- Guillaume Gohin - Security Manager
  guillaume.gohin@payfit.com
- security@payfit.com
- Facebook | Twitter

payfit.com/en/security