

Privacy Policy

1. Our Commitment to Data Privacy

Protecting the privacy of individuals who provide us with personal information (“**Personal Data**”) is of sincere importance to Payfit and to the way we do business. You have shown your trust in us by interacting with our Site and Application and we value that trust. To this end, we are committed to respecting data privacy legislation, and in particular the (EU) 2016/679 General Data Protection Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of persons with regard to the processing of personal data (the “**Applicable Law**”).

2. General provisions

This Privacy Policy (the “**Policy**”) describes how PayFit SAS/Ltd/SL/GmbH (“**PayFit**”, “**we**”, or “**us**”) collects, uses, stores, shares and protects your information in connection with services offered by PayFit as a data controller including, but not limited to, services provided at or using the domain PayFit.com (the “**Site**”) and/or the PayFit application (the “**Application**”) (collectively, the “**Services**”).

This Privacy Policy applies when you (“**you**”, the “**Customer**”, the “**User**”) access, visit or use any portion of the Services.

For the purposes of this Privacy Policy:

- a “**Customer**” is a person who uses the application on the basis of a subscription contract,
- a “**Prospect**” is a person who browses the Website out of interest for the Services and/or signs up for a demo.

3. Changes to this Privacy Policy

We may amend this Privacy Policy from time to time to ensure transparency on all processing operations relating to you and your Personal Data in real-time. We may notify you of any substantial changes to this Privacy Policy, before the effective date of the changes, by sending an email or in another conspicuous manner reasonably designed to notify you.

Therefore, we recommend that you read this Policy regularly.

4. Data Privacy Officer

We appointed a Data Privacy Officer (the “**DPO**”), whose duties are to ensure that our processing operations comply with this Policy and, more generally, with the Applicable Law.

Our DPO helps every PayFit team before, during and after any processing operation, deals with requests related to the protection of Personal Data and raises awareness about data privacy among PayFit’s staff members.

Browsing the Site and/or the Application	Strictly necessary cookies	To ensure proper functioning of the Services.	Your Consent when you agree to use cookies on the Services.
	Preference cookies	To store information already entered and personalize and optimize your experience on our Website.	
	Statistics cookies	To help us understand how the Services are used and anonymously report this information.	
	Marketing Cookies	To track your use of the Services and help us improve your user experience.	

6. How long will we retain your Personal Data ?

Your Personal Data will be handled in accordance with this Policy as long as it is needed in order to :

- perform the Services;
- provide you with personalized Services;
- comply with the law and namely prevent fraud, collect any fees owed, resolve disputes, troubleshoot problems, assist with any investigation and take other actions permitted by law.

Therefore, PayFit shall only retain your personal data for the following periods:

FRANCE

	Categories of personal data	Retention period	Reason for retention period
Customer	Identification data (name, surname, email address etc...)	3 years after termination of the contract	To make statistics and more generally for evidentiary purposes
	Any contractual document entered into by you and PayFit	5 years after termination of the contract	Most claims are subject to a 5 years statute of limitation
	Billing and financial information (payment, refunds...)	10 years after termination of the contract	To collect unpaid debts and more generally for evidentiary purposes in accordance with the law.
Prospect	Prospect information (name, surname, contact	3 years after they were first collected	To make statistics, to give you access to a

	details, request for a demo...)	or upon your request to be deleted, whichever is the soonest	demo account and otherwise contact you.
Browsing the Site/Application	Cookies	13 months after they were first installed on your terminal	To allow proposer functioning of the Services.

United Kingdom

	Categories of personal data	Retention period	Reason for retention period
Customer	Identification data (name, surname, email address etc...)	6 years after termination of the Contract	To make statistics and more generally for evidentiary purposes, given that most claims are subject to a 6 year statute of limitation.
	Any contractual document entered into by you and PayFit		
	Billing and financial information (payment, refunds...)		
Prospect	Prospect information (name, surname, contact details, request for a demo...)	3 years or upon request from subject for data to be deleted, whichever is soonest	To make statistics, to give you access to a demo account and otherwise contact you.
Browsing the Site/Application	Cookies	13 months after they were first installed on your terminal	Allows proper functioning of the Services

Spain

	Categories of personal data	Retention period	Reason for retention period
Customer	Identification data (name, surname, email address etc...)	6 years after termination of the Contract	To make statistics and more generally for evidentiary purposes, given that most claims

	Any contractual document entered into by you and PayFit		are subject to a 6 year statute of limitation.
	Billing and financial information (payment, refunds...)		
Prospect	Prospect information (name, surname, contact details, request for a demo...)	3 years or upon request from subject for data to be deleted, whichever is soonest	To make statistics, to give you access to a demo account and otherwise contact you.
Browsing the Site/Application	Cookies	13 months after they were first installed on your terminal	Allows proper functioning of the Services

GERMANY

	Categories of personal data	Retention period	Reason for retention period
Customer	Identification data (name, surname, email address etc...)	6 years after termination of the Contract	To make statistics and more generally for evidentiary purposes, given that most claims are subject to a 6 year statute of limitation.
	Any contractual document entered into by you and PayFit		
	Billing and financial information (payment, refunds...)		
Prospect	Prospect information (name, surname, contact details, request for a demo...)	3 years or upon request from subject for data to be deleted, whichever is soonest	To make statistics, to give you access to a demo account and otherwise contact you.
Browsing the Site/Application	Cookies	13 months after they were first installed on your terminal	Allows proper functioning of the Services

When we have no ongoing legitimate business need to process your personal data, we will delete it as soon as it is technically possible.

7. Do we share your personal data with any third parties?

In connection with the use of the Services, some of your Personal Data may be processed by Third Parties for the purpose of carrying out some of the processing operations listed out above.

7.1 Third Party Service Providers

We may disclose your personal data to third-party service providers (the “**Subprocessors**”). When we do so, we make sure to work only with companies that safeguard and protect your personal data and comply with the Applicable Law in the same way that we do. Therefore, in accordance with Article 28 of the GDPR, access to your Personal Data by our Subprocessors is subject to the signature of a written agreement which allows us to monitor and control the way our Subprocessors handle your personal data.

7.1.1 Operational Services

Subprocessors	Categories of Data	Why do we use them?
Amazon Web Services (AWS)	All Data.	For hosting and back-up purposes.
Bugsnag		To track, locate and fix any bugs or errors you may encounter while using the Services.
FullStory		
Sentry io		

7.1.2 Improving the Services

Subprocessors	Categories of Data	Why do we use them?
Pendo.io	All Data.	To improve your user experience on the Services, make statistics and measure the activity.
Chart io		
Kibana		
G Statistics		

7.1.3 Sales, business development

Subprocessors	Categories of Data	Why do we use them?
Pandadoc	Customer identification details (name, surname, email address, etc...)	For contract management purposes.
Drift	Any information you may share with us while using our chatbot on our Site.	To chat with unlogged users and help them with any question they have.

7.1.4 Customer Success

Subprocessors	Categories of Data	Why do we use them?
Zendesk	Name, email address, and any data you disclose when contacting us through the help section of the Services.	To manage customer support and keep track of your requests.

7.1.5 Marketing

Subprocessors	Categories of Data	Why do we use them?
Segment	Email and IP address	To make statistics and manage data.

7.1.6 Productivity Tools

Subprocessors	Categories of Data	Why do we use them?
G Suite	Name, email address and any other personal data you share with us when contacting us via mail.	To manage our emails and daily operations.
Tresorit	Any information you send us for a successful onboarding on the Services.	For file storage and management purposes.
Jira	Name, email address.	For bug management purposes.

7.1.7 Accounting

Subprocessors	Categories of Data	Why do we use them?
Quickbooks	Identification information and any financial or billing information related to invoices and payments.	To make sure payments and invoices are in order and to comply with legal requirements.

7.2 Other Recipients

In addition to our Subprocessors, your Personal Data may be disclosed to independent contractors in order to perform part of the Services.

Recipients	Categories of Data	Why do we use them?
Independent contractors	The data strictly necessary for them to perform their duties.	To perform part of the Services.

8. Where do we store your Personal Data ?

The Personal Data we process is stored by our hosting provider Amazon Web Services on servers located within the European Union (in France).

In order to perform the Services, we may transfer some of your Personal Data to third party service providers located or using servers located outside the European Union (the "EU") and the European Economic Area (the "EEA"). In such a case, we make sure that:

- they are located in a country considered having an adequate level of protection by the European Union in terms of personal data or,
- if located in the United States:
 - they are registered in the "Privacy Shield" register and that they comply with its provisions or,
 - they abide by contractual provisions ensuring an equivalent level of protection of your Personal Data (such as standard contractual clauses established by the European Commission).

9. How do we protect your Personal Data ?

Here at PayFit, we care about the security of the Personal Data we process. Therefore, we adopt technical and organizational security measures to guarantee the security of your Personal Data by ensuring a security level adapted to the risks related to the processing and nature of such Personal Data, in particular:

- **Ultra-secure encryption:**

All data and information transmitted to our service via the secure TLS 1.2 protocol is encrypted using RSA-4096 keys, offering you the best guarantee of confidentiality.

- **Secure servers:**

Our servers use OAuth2 authentication via JWT tokens, ensuring the integrity, security and authenticity of the data we process at all times. Our database is also highly encrypted and requires multiple keys to operate.

- **Backups**

We use replication mechanisms to permanently safeguard your information and guarantee you a service that is always available. Your data is in good hands.

- **Continuous Monitoring**

Alert and verification systems guarantee you highly reliable calculations. An internal team is entirely dedicated to legal and conventional monitoring to ensure that all developments are taken into account in real time.

You can find further details about the way we protect your personal data in our Security Policy (Security Policy - PayFit).

10. Your rights

Unless stated otherwise by the Applicable Law or any other legal provision or applicable regulations, you may exercise the following rights:

- **Right to access:** the right to be informed and to request access to your Personal Data;
- **Right to data portability:** the right to request a copy of your Personal Data in a structured and machine-readable format in order to hand it over to a third party ;
- **Right to rectification:** the right to ask us to modify or update inaccurate or incomplete Personal Data;
- **Right to erasure (right to be forgotten):** the right to ask us to permanently delete Personal Data when the data subject considers that we no longer have any reason to do so collect/process;
- **Right to restriction of processing:** the right to ask us to stop temporarily or the processing of all or part of the Personal Data;
- **Right to object:** the right to object at any time, for reasons related to the situation of the data subject, to the processing of Personal Data concerning him/her having as its legal basis the pursuit of a legitimate interest. Unless we demonstrate a legitimate and compelling interest justifying such processing, we will only process plus the Personal Data concerned;
- **Right to decide the fate of your data after death:** the right to impose the fate that you wish to reserve your Personal Data in the event of death;
- **Right to file a complaint with the supervisory authority** or to get compensation from the competent courts.

To exercise your right, please send their request directly to us:

- by email at legal@payfit.com;
- or by post to PayFit SAS, Data Protection Officer, 75 rue de Tocqueville, 75017 Paris.

In accordance with Applicable Regulations, we will ask you to prove your identity.

11. Contact the competent supervisory authority

We remind you that you have the possibility to file a complaint with the competent supervisory authority:

- in France, this authority is the Commission National Informatique et Libertés (CNIL), whose website address is: www.cnil.fr;
- in the United Kingdom, this authority is the Information Commissioner's Office (ICO), whose website address is: <https://ico.org.uk>;
- in Germany, this authority is Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, whose website address is: <http://www.bfdi.bund.de/>;
- in Spain, this authority is Agencia de Protección de Datos (AGPD), whose website address is: <https://www.agpd.es/>.