

# Data Privacy Policy

This Privacy Policy is established by Digiteal SA (hereinafter referred to as "the Controller").

Its purpose is to inform visitors to the website hosted at the following address: [www.digiteal.eu](http://www.digiteal.eu) (hereinafter referred to as the "Website") of the way in which the data are collected and processed by the Controller.

This Privacy Policy is in line with the Controller's wish to act in complete transparency, in compliance with its national provisions and with Regulation (EU) 2016/679 (hereinafter referred to as the "General Data Protection Regulation" or "GDPR") of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC. This policy is subject to periodic review and updates to reflect changes in legislation, business practices, or user feedback.

The Controller pays particular attention to protecting the privacy of its users and, therefore, undertakes to take the reasonable precautions required to protect the personal data collected against loss, theft, disclosure, or unauthorized use.

## What do you not see when visiting our Website?

Each time you visit our Website (request or attempt to request data from our server), the information concerning this request is stored in a log file (Logfile).

**In particular, the following data is recorded for each request:**

- IP address
- Name of requested data
- Date and hour of the request
- Volume of data transmission
- Indication of successful completion
- Indication why an application has failed
- Operating system and browser software on your computer
- Screen resolution
- Browser language
- Color depth
- Plugins of the browser (JavaScript, Flash Player, Java, Silverlight, Adobe Acrobat Reader etc.)
- As well as the website from which you consult us.

For statistical purposes, the data is stored in log files (Log-Files). We can not link the recorded data to your person. Nor do we pass the data on to third parties. It is only in case of breach of the law that we

reserve the right to transmit certain registrations to the competent authorities to allow the prosecution of the offenses.

In order to be able to assist you online, we use the Zoho Corporation chat service.

## Usage of Cookies

On our Website, we use so-called "cookies" to make browsing more useful and reliable. Some of these cookies are essential to the operation of the Website, others improve the user experience.

Most web browsers are configured to automatically accept cookies. If the user wishes to customize their management, he must modify the settings of his browser.

Google Analytics™ uses internal cookies to generate reports on users' interactions with Google Analytics™ customers' websites. These cookies are used to store information that does not personally identify users. Internal cookies stored in browsers are not valid from one domain to another.

## What do you not see when you use our platform?

### Privacy Statements for the use of the Digitéal web platform

In addition to the privacy statements on our Website (see above), we would like to inform you of the following:

- Access to the platform:
  - When accessing the platform, we identify you through various personal data:
    - Email address
    - IP address, browser agent and cookies
  
- Linking a bank account:
  - To take full advantage of the Digitéal billing and payment platform, you will be offered to link one or more of your bank accounts.  
Since Digitéal is recognized as a banking institution by the Belgian National Bank, our company is subject to the various rules applicable to the sector, such as the fight against money laundering, combating the financing of terrorism, etc.
  - For these reasons, we are legally obliged to identify the natural person linked to the bank account of the latter or linked to a legal person. In this context personal data are requested such as:
    - Identification via identity card
    - Last Name/First Name
    - Address

- Bank account(s)
- “KYC” (Know Your Customer) Rules
- Bill presentment
  - As Peppol Access Point Provider, Digiteal will send and receive B2B invoices. These invoices may contain personal data as the contact person details for example.
- “One-Click-Pay”
  - Information about the status of the payment will be sent to the creditor of the invoice (the issuer): payment initiated, outstanding, paid, rejected payment, programmed automatic payment.
- Bank Account Access Service (PSD2)
  - If you link a bank account to access the transactions of that account, we collect the following data:
    - Name and surname
    - Internal identifiers (client access token, API token)
    - Third party identifiers (authorization token from your account management payment service provider) and your IP address
    - IBAN of your bank accounts
    - Bank account information (including history of payments sent and received)
    - Security, access and activity logs
    - User agent for your web browser.
- Payment Initiation Service (PSD2)
  - If you initiate a transfer through Digiteal, we collect the following data:
    - The same data as for the bank account access service.
    - Information about the payment you wish to make (IBAN and name of the beneficiary, amount, communication)

## What do you not see when using our app?

### Privacy Statements for the Use of the Digital APP

To take advantage of Digiteal's services, we provide you with a mobile app.

In addition to the statements on privacy in relation to the web platform (see above), we would like to inform you of the following points :

- When using the app, we collect the following personal data for statistical purposes and to improve the functions of the app :
  - identification of your device, your mobile device number / PUSH (IMEI = International Mobile Equipment Identity),
  - Your IP address (in case of onboarding on the platform).

We do not pass on your data to third parties for commercial purposes but only

- for operational purposes and in order to improve the safety of our services to third parties providing, directly or indirectly, services in relation to the platform
- for regulatory reasons towards the competent authorities.
  
- Storage: the data you provide us during registration or the ones that your supplier provides us are securely stored in Europe (Germany) with the Amazon Web Services (AWS) provider. The purpose of this processing is to allow the archiving of your information and documents so that you can access them at any time.
- Automation: some documents you provide to us during registration or that your suppliers provide to us might be transmitted to Google (OCR service) and Amazon Web Services (image analysis service); both with European storage. The purpose of this data processing is to check the concordance between two images, the degree of readability, to detect potential cases of fraud, to automatically prefill fields in order to facilitate onboarding, etc. If you do not wish to allow this processing, you can make an opt-out in "My profile".
- Support: some of the data you provide us during registration can be securely stored in Europe (Ireland) with our supplier Atlassian. The purpose of this data processing is to enable our compliance department to check the compliance of the provided data in order to fight against fraud, money laundering, etc.
- External control: certain data, typically financial transactions, may be passed on to third parties such as your accountant or his software supplier provided you have given us your explicit consent to share this data.
- Regulatory: In order to fulfill our reporting obligations, personal data may exceptionally be disclosed to third parties who carry out regulatory control missions such as our external auditor and government institutions such as the NBB and CTIF.
- Services: for the service "access to banking movements" and connection with banks (AIS and PIS), we work with Exthand SRL. For the Loyaltch service, we work with Promcom BV.

In order to make the app work properly, the app uses the following functions and sensors via the interfaces of your mobile device :

- Localization information: When you use the app outside of the European Union, we may collect and process information about your location in real time, if you have enabled the location function for this app beforehand on your mobile device. We use different technologies such as IP addresses, GPS or other sensors to locate you.
- The purpose of this processing is for the purposes of potential evaluation of fraud and alert generation in our system.
- If your mobile device has a camera, the latter is used to scan QR Codes. It can also be used to do pictures of your identity documents while subscribing to the service.
- When the app's messaging service is enabled, you receive push notifications on your mobile device. This service saves your linked keywords and the push ID of your mobile device in a database. The sending of messages is done through the push services of Apple (iOS devices) or Google (Android devices).
- The wireless connection of your mobile device is used by the app to establish a connection to the Internet.

- By accessing other functions and sensors on your mobile device, the app can access data from the internet and process error messages.
- In the event that you consult the websites of partners (billers) from the Digitéal platform, the privacy policy in force on these sites is independent of that of Digitéal.
- For payments:
  - to proceed to a card-based payment, we use services of Payment Service Providers (PSP). For the time being, those are:
  - MultiSafepay: [www.multisafepay.com](http://www.multisafepay.com)
  - Shift4 : [www.shift4.com](http://www.shift4.com)

## Why collect and process this data?

Personal data is only used when you make it available to us, for example when you subscribe to our newsletter, when you make a request on our contact page or when you register on the Digitéal platform to take advantage of our services.

The information provided is transmitted in a safe manner. This protects the communication between your computer and our web server, and this makes it possible to prevent the misuse of data by third parties. For encryption, we use SSL (Secure Socket Layer), a system recognized and widely used on the Internet, which is also used by banks and the current version of which still offers the necessary security.

All personal data on our Website is collected, processed and used on our Website in accordance with the legal provisions concerning the protection of personal data and only for the provision of the services requested by you and for the processing of your requests. As part of payments processing, we work with a banking partner. This bank is contractually bound and has an obligation to respect these rules of protection of the private life. More generally, we process personal data on the basis of our legitimate interest (for instance, communication of personal data to entities providing services in relation to our platform).

## Retention period

The Controller shall keep personal data only for as long as is reasonably necessary for the purposes for which they are collected and in accordance with legal and regulatory requirements.

At the end of the storage period, the Controller shall make every effort to ensure that the personal data have been made unavailable.

## Data Subject rights

Under the GDPR the users have some important rights.

In summary, these include rights to:

- (a) access your personal data;
- (b) require us to correct any mistakes in your information which we hold;
- (c) request the erasure of personal data concerning you in certain situations;
- (d) request the data to be transferred to a third party in certain situations;
- (e) object at any time to processing of personal data concerning you for direct marketing;
- (f) object in certain other situations to our continued processing of your personal data;
- (g) otherwise restrict our processing of your personal data in certain circumstances; and
- (h) claim compensation for damages caused by our breach of any data protection laws.

To access, modify and erase your personal data, you can exercise your rights through the menu “My Profile”.

You can delete your Digiteal account to exercise your right to be forgotten. Minimal data will be kept by the Controller according to the EU payments logging requirements.

To exercise your other rights, please send an email to [support@digiteal.eu](mailto:support@digiteal.eu)

## Security

The Controller shall implement appropriate technical and organisational measures to ensure a level of security of the processing and data collected with regard to the risks represented by the processing and the nature of the data to be protected appropriate to the risk. It takes into account the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the processing operation as well as the risks to users' rights and freedoms.

The Controller always uses encryption technologies that are recognized as industry standards within the IT sector when transferring or receiving data on the Website.

The Controller has put in place appropriate security measures to protect and avoid the loss, misuse or alteration of the information received on the Website.

## What rights do you have regarding the transmitted data?

As Digitel is **responsible for the processing** of personal data, you can ask your questions to our DPO (data protection officer ) via [dpo@digiteal.eu](mailto:dpo@digiteal.eu)

As a customer, in addition to all your rights detailed in [Data Subject rights](#), you can always question us about your personal data and ask which data are concerned (your personal data is what you gave us).

You have the possibility to ask for the right to the deletion of your data, or the right to forget.

Digitel S.A.  
Rue Emile Francqui 6/9  
1435 Mont-Saint-Guibert  
Belgium

*This version of the Privacy Policy is dated 28/02/2025.*