

# PRIVACY POLICY

UNDER EU REGULATION 2016/679 OF APRIL 27, 2016 (GDPR) AND FRENCH LAW N°78-17 OF JANUARY 6, 1978

## PREAMBLE

This Privacy Policy (hereinafter referred to as the “**Privacy Policy**”) shall be effective as of January 1, 2025.

The Privacy Policy’s primary objective is to provide Users with comprehensive information regarding the processing of their personal data by INFLOW PAY during their utilization of the Services, when placing orders related to the Services, or more generally when accessing the website accessible at <https://www.inflowpay.com/> (hereinafter referred to as the “**Website**” or the “**Site**”). This Privacy Policy constitutes an integral component of the Terms and Conditions (hereinafter referred to as the “**T&Cs**”) available upon clicking [here](#).

All terms not defined herein have the meaning given to them in the T&Cs.

INFLOW PAY is a simplified joint-stock company with a capital of 100 euros, having its registered office at 58 Monceau street in Paris 75008 (FRANCE), registered at the French Companies Register (« **RCS** ») under number 928 877 349 (hereinafter the « **Company** »).

Its email address is: [legal@useinflow.com](mailto:legal@useinflow.com).

The use of the Site, any application or software provided by the Company, or any Service offered on it by any User constitutes full acceptance by the User of these terms. Consequently, any User who does not wish to consent to these terms is free to refrain from visiting or using the Site, the Application, or the Services.

## 1. PERSONAL DATA SUBJECT TO COLLECTION

The categories of personal data collected are as follows:

### 1.1. DATA PROVIDED BY THE USER

1. **Identification Data** : The User may provide identification data when registering to use the Services, such as name, first name, gender, date and place of birth, nationality, social security number, geographical location, personal description and photograph ;
2. **Contact Data** : The User may provide contact data, including postal address, email address, social media identifiers, and telephone number(s) ;
3. **Service-Related Data** : This includes login credentials for the Service (such as username, password, and other information related to the security of these credentials, including security question answers), invoices, preferred language, purchase history, purpose of payment, information provide by the User through his continued use of the Services, included discussion boards or other social media functions, information sent during a promotion or survey, comments, requests, questions, and information sent to customer service ;
4. **Financial Informations** : Bank details to ensure payment for the Services or when using the Services, such as bank account details, credit or debit card number, expiration date, cardholder name, verification code, one-time passwords and any identifier enabling the use of a payment service provided by a third party (e.g., Visa, Mastercard, PayPal, Apple Pay, Google Pay).
5. **Non-Custodial Wallet Credentials** : Details pertaining to non-custodial cryptocurrency wallets employed for transactions, such as wallet public keys or unique identifiers and transaction records.
6. **Information Regarding Third Parties** : When providing personal data of any third party (such as individuals or business entities who may receive payments through the Services), it must be ensured that consent from such individuals has been obtained to disclose their personal data to the company, as well as their consent to the collection, use, and disclosure of such data, for the purposes outlined in this Privacy Policy.

7. **Commercial and/or Identification Information** : Additional commercial and/or identification information may be required, particularly if conducting high-value or high-volume transactions, or to comply with anti-money laundering obligations under applicable law.

## 1.2. INFORMATION COLLECTED ABOUT USERS

1. **Transaction Data** : Details of the transactions executed when utilizing the Services, including the geographical location from which the transaction originates ;
2. **Technical Data** : Internet Protocol (« **IP** ») address used to connect the device to the Internet, login credentials, browser type and version, time zone setting, browser plug-in types and versions, and operating system and platform ;
3. **Visit Data** : Information regarding the visit, including the full Uniform Resource Locators (« **URL** ») clickstream to, through, and from the Website or App (including date and time); products viewed or searched for; page response times, download errors, duration of visits to specific pages, page interaction details (such as scrolling, clicks, and mouse-overs), methods used to navigate away from the page, and any telephone number used to contact Customer Support.

## 1.3. INFORMATION FROM OTHER SOURCES

Personal data about users may also be collected through any subsidiary or affiliated company, or any other party, including third parties, as listed below :

1. **Social Media Data** : Any data accessible on the user's social networks when the user grants the Site permission to access their data on a social network ;
2. **Geolocation Data** : Any data transmitted by a geolocation service provider to personalize the provision of the Services based on the user's location, provided the user agrees to share their location ;
3. **Partner Data** : Any data transmitted by a partner company or business in the context of providing a Service ;
4. **Public and Supplier Data** : Any data accessible publicly and/or from data suppliers, allowing validation or completion of the information being processed ;
5. **Blockchain informations** : any data readily available on public blockchains.

## 1.4. INFORMATION COLLECTED DURING THE USE OF THE SITE OR SERVICES

During the use of the Site or Services, particularly for audience measurement and/or targeted advertising purposes, the following data and information may be automatically collected using cookies, trackers, or any other equivalent technical means :

1. **Connection Information** : Computer model, connection environment, IP address, type and version of the internet browser, version of the operating system, other software installed in the environment, version of the mobile platform, technical identifiers, error reports and execution data, geolocation (region, city, or village) ;
2. **Usage Data** : Features used, settings selected, data viewed, times and dates of consultation, search terms, pages visited and searched by the User.

Please note that cookies are text files which may be read by a web server from the domain of the Website or the App and are placed directly on the User's hard drive or SSD. These files can be utilized to store User preferences and settings, facilitate login processes on the Site, and enable the use of the Services. Additionally, cookies allow for targeted advertising and the analysis of operations performed on the Site. Users have the ability to control cookies through their browser preferences and other tools. However, blocking certain cookies may result in a diminished user experience on the Site and/or restricted access to the Services.

## 2. CONTACT

### 2.1. IDENTITY AND CONTACT DETAILS OF THE DATA CONTROLLER

The data controller is the Company:

**INFLOW PAY**

a French simplified joint-stock company with a share capital of 100 euros  
58 rue Monceau - 75008 PARIS  
R.C.S. PARIS 928 877 349  
Intra-community VAT FR54928877349  
NAF / APE Code 6201Z

Its telephone number is: +33 (0)7 80 97 97 31 and its email address is: [contact@inflowpay.xyz](mailto:contact@inflowpay.xyz).

## 2.2. IDENTITY AND CONTACT DETAILS OF THE DATA PROTECTION OFFICER

The Data Protection Officer is Mr. Hanafi ISSAHANE. Requests from Users concerning personal data can be sent to the email address: [hanafi@inflowpay.xyz](mailto:hanafi@inflowpay.xyz), or to the attention of Mr. Hanafi ISSAHANE at the postal address :

INFLOW PAY SAS, 58 rue Monceau - 75008 PARIS, FRANCE.

## 3. COMPLAINT TO THE CNIL

Users affected by the processing of personal data have the right to lodge a complaint with the supervisory authority, which is the National Commission for Information Technology and Civil Liberties (CNIL) :

CNIL, 3 Place de Fontenoy - TSA 80715 - 75334 PARIS 07, FRANCE.

## 4. PURPOSES OF PROCESSING PERSONAL DATA

The purposes of processing Users' personal data are as follows:

1. **Contractual obligations** : To carry out obligations related to the contract with the Company and to provide Users with information, products, and services ;
2. **User account creation** : Registration, identifiers, and passwords ;
3. **User account management** : Activation and management of access to the Site and the User's profile, management of subscriptions, sending information about offers, updates, sending commercial proposals, offering personalized content, organizing events ;
4. **Notifications** : To notify Users about changes to the Services ;
5. **Customization** : To customize the Services and the information provided to Users, addressing their needs based on factors such as country of address and transaction history. For example, if Users frequently send funds from one particular currency or token to another, this information may be used to inform Users of new product updates or features ;
6. **Advertising** : Providing targeted advertising, promotional messages, invitations to participate in surveys or lotteries, notifications, and other information related to the Services and Users' interests, offering specific content based on the User's location, and more generally to deliver relevant advertising to Users ;
7. **Use of Services** : To process requests, orders, downloads, subscriptions to services, billing, payment, and execution of transactions or contracts ;
8. **Provision of technical support** : Ensuring the proper functioning and security of the Site and Services, technical support, customer service for Services and products ;
9. **Improvement and development** : Improvement of Services and products and creation of new products and services, identifying usage trends, data analysis, auditing, research, reporting, determining the effectiveness of promotional campaigns, and evaluating commercial performance ;
10. **Safety and security** : As part of efforts to keep the Services safe and secure ;
11. **Administration and internal operations** : Administering the Services and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes ;
12. **Effectiveness measurement** : To measure or understand the effectiveness of advertising served ;
13. **Interactive Features** : Allowing participation in interactive features of the Services, when chosen by the User ;
14. **Third-party information** : Providing Users, or permitting selected third parties to provide, with information about goods or services that may be of interest ;
15. **Combining information** : Combining information received from other sources with the information provided by Users and information collected about Users, using the combined information for the purposes set out above, depending on the types of information received ;

16. **Financial and insurance** : To assess financial and insurance risks, and to protect operations and those of any affiliates or partners, to recover debt or in relation to insolvency ;
17. **Compliance with legal obligations under GDPR** : Compliance with obligations arising from Articles 15 and following of Regulation EU 2016/679 of April 27, 2016 (GDPR), including legal compliance, resolution of potential disputes, fulfillment of contractual commitments, fraud prevention, and execution of tasks in the public interest.
18. **Remedies and enforcement** : To allow the pursuit of available remedies or limiting the damages that may be sustained and enforcing terms and conditions ;
19. **Fraud and crime prevention** : To assist in conducting or cooperating in investigations of fraud or other illegal activity where it is reasonable and appropriate to do so, to prevent and detect fraud or crime.
20. **Legal and regulatory compliance** : To comply with any applicable legal and/or regulatory requirements, including laws outside of the user's country of residence or to comply with any legal process, or to enforce or apply any applicable agreement, or to protect the rights, property, or safety of the Company, customers, or others, and in response to a subpoena, warrant, court order, or as otherwise required by law.

In the event that personal data is processed for purposes other than those identified in this article, the data controller designated in Article 2.1 above will inform the concerned Users of this new purpose.

## 5. LEGAL BASES FOR PROCESSING PERSONAL DATA

The legal bases for processing personal data are the User's consent, the necessity of executing pre-contractual or contractual measures to benefit from the Services, as well as the necessity for the Company to pursue its legitimate interest, particularly in managing its relationship with the User and retaining proof of transactions.

The User is informed that within the framework of any contractual relationship they wish to establish with the Company, their refusal to provide the requested personal data may prevent access to the Services and proper execution of the contract.

## 6. DATA DESTINATION

All data is stored in data centers located in Europe.

### 6.1 THIRD-PARTY APPLICATIONS AND APIS

User access to a third-party application available on the Site, the App, or a Service, as well as the use of APIs through the Website or the App, may result in the sharing of personal data concerning the User with the publisher of this third-party application or API. This sharing is primarily for the purpose of granting the User access to the application or API, subject to the terms, license agreements, and privacy policy of the third-party application or API.

### 6.2 THE COMPANY AND SERVICE PROVIDERS

Personal data concerning a User may be shared or disclosed with :

1. The Company and any company within its group, including but not limited to any subsidiary, holding or affiliated company ;
2. Any service provider, supplier, distributor, agent, and representative, including but not limited to credit and financial institutions, customer support, email service providers, event venues and service providers, IT service providers (including hosting providers), marketing service providers, research firms, mailing companies, shipping agents, on and off ramp partners, wallet holders, merchants, and authenticators, analytics and search engine providers, advertisers and advertising networks solely to select and serve relevant advertisements to the User ;
3. Courts, law representatives, police, regulatory authorities, and other law enforcement agencies (in the event of a duty to disclose or share personal data in order to comply with any legal obligation) ;
4. In the event of selling or buying any business or assets, personal data may be disclosed to the prospective seller or buyer of such business or assets.

A published list of all third parties with whom the Company shares User data is not available, as this heavily depends on the specific use of the Services. However, Users seeking further information about entities with whom their data has been shared, or a specific list, can request this information by writing to [hanafi@inflowpay.xyz](mailto:hanafi@inflowpay.xyz).

In any case, the Company shall always ensure that, to the best of its knowledge, recipients of disclosed personal data have an adequate level of data protection.

## 7. DATA TRANSFER

The User is informed that the data controller may, if applicable, transfer personal data to a third country or to an international organization that is subject to an adequacy decision by the European Commission. It is specified that, in the event of a transfer to a country or international organization that is not subject to an adequacy decision, this can only be carried out provided that appropriate safeguards are in place and that the individuals concerned by the personal data processing have enforceable rights and effective legal remedies, in accordance with the applicable regulations.

## 8. RETENTION OF PERSONAL DATA

Personal data of Users is retained for as long as necessary to provide and complete the Service and fulfill the Company's obligations under a contract, law, or regulation. The User's data is only accessed internally on a need to know basis, and it will only be accessed or processed if absolutely necessary.

Personal data shall be deleted when no longer required by a relevant law or jurisdiction in which the Company operates.

The main retention periods for the storage of personal data relating to Users of the Site are as follows:

1. **Identification and contact data of a User** : For the duration of the contractual relationship (as long as the User has not expressed the intention to no longer be a User of the Services or to no longer have their personal data retained, which must be done via a request sent to the following address : [hanafi@inflowpay.xyz](mailto:hanafi@inflowpay.xyz), up to a maximum of three (3) years from either the last order of services made by the User on the Site, or the date of termination of the last Service used by the User (whichever is most recent), after which personal data is no longer retained ;
2. **Data collected during the registration for a Service (interrupted registration process)** : Thirty (30) days from the entry of the email address by the User ;
3. **Bank details** : For the duration of the contractual relationship, with subsequent retention of five (5) years for banking documents related to transactions ;
4. **Bank card data (processed by payment service providers as processors)** : Retained by payment service providers for as long as necessary to provide the service as processors ;
5. **Data related to the execution of the contract (invoices, purchase history, payments, etc.)** : Ten (10) years from either the last order of services made by the User via the Site, or the date of termination of the last Service concluded by the User (whichever is most recent) ;
6. **Data related to the exercise of a right by a User** : Five (5) years on top of the year of the request.

## 9. DATA SECURITY

The Company employs technical and organizational measures to ensure the appropriate security level for processed personal information. These measures are designed to maintain the integrity, confidentiality, and availability of personal data.

The Company takes extensive steps to secure personal data on its systems. Dedicated staff are responsible for upholding data protection and security policies, conducting periodic reviews, and ensuring employees are informed about these practices.

Personal information is stored on secure servers. All data provided by Users is kept on these secure servers, and any information related to payment transactions is encrypted.

While every effort is made to safeguard personal information, the Company cannot guarantee the security of data during transmission, and any transfer is at the User's risk. Upon receipt, stringent procedures and security measures are implemented to prevent unauthorized access.

The Company has established policies and procedures to securely manage information and protect personal data from unauthorized access. Regular assessments are conducted to ensure data privacy, information management, and security practices are maintained. These practices include :

1. Setting policies and procedures for secure information management ;
2. Restricting employee access to only the information necessary for their duties ;
3. Utilizing data encryption, authentication, and virus detection technology to prevent unauthorized access ;
4. Ensuring service providers comply with relevant data privacy laws and regulations ;
5. Monitoring websites through recognized privacy and security organizations ;
6. Conducting regular third-party audits of policies and practices ;
7. Performing background checks on employees and providing them with relevant training.

## 10. USER RIGHTS THAT CAN BE EXERCISED WITH THE DATA CONTROLLER

Based on the legal grounds for processing, which includes the User's consent, the User has the following rights under applicable regulations :

1. **Right of access** : The right to obtain from the data controller confirmation as to whether or not personal data concerning the User is being processed, and, where that is the case, access to the personal data ;
2. **Right to rectification** : The right to obtain from the data controller the rectification of inaccurate personal data concerning the User and to have incomplete personal data completed ;
3. **Right to erasure** : The right to obtain from the data controller the erasure of personal data concerning the user without undue delay, subject to legal retention obligations, especially when the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, when the User has withdrawn consent on which the processing is based, or when the processing is unlawful ;
4. **Right to restriction of processing** : The right to obtain from the data controller restriction of processing where the accuracy of the personal data is contested by the User, where the processing is unlawful, and the User opposes the erasure of the personal data and requests the restriction of their use instead, or where the data controller no longer needs the personal data for the purposes of the processing but they are required by the User for the establishment, exercise, or defense of legal claims ;
5. **Right to object** : The right to object, on grounds relating to the User's particular situation, at any time to the processing of personal data concerning them, including profiling ;
6. **Right to object to direct marketing** : The right to object, at any time, to the processing of personal data concerning the User for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing ;
7. **Right to data portability** : The right to receive the personal data concerning the User, which they have provided to a data controller, in a structured, commonly used, and machine-readable format, and to have the right to transmit that data to another data controller ;
8. **Right to withdraw consent** : The right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal ;
9. **Right to give instructions regarding the post-mortem use of data** : The right to define instructions regarding the fate of their personal data after their death.

The exercise of these rights, as identified in this article, is conducted by the User with the data controller by making a request addressed to the Company at the following address : [hanafi@inflowpay.xyz](mailto:hanafi@inflowpay.xyz).

It is specified that the exercise by a User of their right to erasure of their personal data and/or their right to object to the processing of their personal data and/or their right to restrict the processing of their personal data and/or their right to withdraw their consent to the processing of their personal data at any time (in accordance with the above stipulations) will result in the User being unable to access the Services. Therefore, in such cases (i) if these rights are exercised at the time of using a Service, the said Service won't be fulfilled ; (ii) in any case, from the moment the User exercises these rights, they will no longer be able to access the Services.

## 11. CHILDREN'S PRIVACY PROTECTION AND MINIMUM USER AGE

The collection of personal data may only concern individuals who are at least fifteen (15) years old at the time of collection, unless the minor under fifteen (15) years old consents to this collection and this consent is accompanied by the consent of at least one holder of parental authority concerning them (parental authority is understood in the sense given by Article 371-1 of the French Civil Code). The collection of personal data is essential for the use of the Site and Services, so minors under fifteen (15) years old can only access the Services if they are authorized to do so by the holder(s) of parental authority concerning them.

Therefore, by requesting the Services and/or providing personal data on the Site, Users declare and guarantee that they are at least 15 years old or that they are authorized to use the Site and provide their personal data by the holder of parental responsibility concerning them.

The Company will not knowingly collect information from any person under fifteen (15) years of age. If any information is collected from such person without verification of parental consent, it will be deleted.

## **12. MODIFICATIONS AND UPDATES**

The Privacy Policy may be subject to corrective modifications or updates. Any changes will be accompanied by the indication, on this page, of the last revision date. As such, the User is invited to regularly review the latest version of this document, accessible in real-time on the Site.

Changes to the Privacy Policy may be subject to temporary notification on the Site or by any written means, including by email. Changes may only occur after a thirty (30) days' prior written notice, unless they are required by law, more favorable to you or related to the addition of a new service or an extra functionality to the existing Service that did not exist prior to its introduction.