



## **iATM® PRIVACY POLICY**

Protecting your privacy is very important to us. Please review our Privacy Statement in order to better understand our commitment to maintaining your privacy, as well as our use and disclosure of your information.

---

### **Languages and translation of agreement**

We will communicate with you in English only.

This user agreement is concluded in English only. Any translation of this user agreement is provided solely for your convenience and is not intended to modify the terms of this user agreement. In the event of a conflict between the English version of this user agreement and a version in a language other than English, the English version shall be the definitive version.

---

### **Your use of information; Data protection laws**

If you receive information about another iATM customer, you must keep the information confidential and only use it in connection with the iATM services. You may not disclose or distribute any information about IATM users to a third party or use the information for marketing purposes unless you receive that user's express consent to do so. You may not send unsolicited emails to a iATM customer or use the IATM services to collect payments for sending, or assist in sending, unsolicited emails to third parties.

To the extent that you (as a seller) process any personal data about a iATM customer pursuant to this user agreement, you agree to comply with the requirements of any applicable privacy and data protection laws. You have your own, independently determined privacy policy, notices and procedures for any such personal data that you hold as a data controller, including a record of your activities related to processing of personal data under this user agreement.

### **WHAT WE COLLECT**

We get information about you in a range of ways.

Information You Give Us. Information we collect from you may include:



Identity information, such as your first name, last name, username or similar identifier, title, date of birth and gender;

Contact information, such as your postal address, email address and telephone number;

Profile information, such as your username and password, interests, preferences, feedback and survey responses;

Feedback and correspondence, such as information you provide in your responses to surveys, when you participate in market research activities, report a problem with Service, receive customer support or otherwise correspond with us;

Financial information, such as your credit card or other payment card details;

Transaction information, such details about purchases you make through the Service and billing details;

Usage information, such as information about how you use the Service and interact with us;

Marketing information, such as your preferences for receiving marketing communications and details about how you engage with them;

Financial information, such as bank account number and bank routing number; financial assets holdings; and

Technical information, such as your Ethereum wallet address, application programming interface (API)-key and network information regarding transactions.

The privacy and data protection laws that may apply include any associated regulations, regulatory requirements and codes of practice applicable to the provision of the services described in this user agreement. If you process personal data from Europe pursuant to this user agreement, we must comply with the EU Directive 95/46 EC or the General Data Protection Regulation (EU) 2016/679 (GDPR).

In complying with such laws, we will:

- implement and maintain all appropriate security measures for the processing of personal data;
- maintain a record of all processing activities carried out under this user agreement; and



- not knowingly do anything or permit anything to be done which might lead to a breach of any privacy data protection laws by iATM.

The EU General Data Protection Regulation (GDPR), which governs how personal data of individuals in the EU may be processed and transferred, went into effect on May 25, 2018. GDPR is a comprehensive privacy legislation that applies across sectors and to companies of all sizes. It replaces the Data Protection Directive 1995/46. The overall objectives of the measures are the same – laying down the rules for the protection of personal data and for the movement of data.

GDPR is broad in scope and uses broad definitions. “Personal data” is any information that relates to an identified or identifiable living individual (data subject) such as a name, email address, tax ID number, online identifier, etc. “Processing” data includes actions such as collecting, recording, storing and transferring data.

A company that is not established in the Union may have to comply with the Regulation when processing personal data of EU and EEA residents (EEA countries are Norway, Lichtenstein and Switzerland):

- a) If the company offers goods or services to data subjects in the EU; or,
- b) If the company is monitoring data subjects’ behavior taking place within the EU.

The mere accessibility of a company’s website in the EU is insufficient to subject a company to GDPR, but other evidence of the intent to offer goods or services in the EU would be relevant.

As a general rule, companies that are not established in the EU but that are subject to GDPR must designate in writing an EU representative for purposes of GDPR compliance. There is an exception to this requirement for small scale, occasional processing of non-sensitive data.

Fines in case of non-compliance can reach up to 4% of the annual worldwide revenue or 20 million euros – whichever is higher. Companies of all sizes and sectors should consider GDPR as part of their overall compliance effort with assistance of legal counsel.

The European Commission and Data Protection Authorities are releasing official guidelines to help companies with their compliance process. These documents relate, for instance, to the role of the data protection officer, personal data breach notification, data protection impact assessment.



## **UK Corporate customers**

When we refer to “PSD2” in this section we mean the Second EU Payment Services Directive ((EU)2015/2366).

We consider you to be a “Corporate Customer” if, on the date you entered into this user agreement, you are not:

- a consumer, (being an individual acting for purposes other than a trade, business or profession); and
- a micro-enterprise (being an enterprise which employs fewer than 10 persons and has an annual balance sheet that does not exceed 2 million EUR); and
- a UK registered charity with an annual income of less than 1 million GBP.

We may disapply certain provisions of PSD2 for your use of our service if you are a Corporate Customer.

If you are a Corporate Customer:

- you are not entitled to a refund for billing agreement payments;
- where you identify a problem you have up to 60 days from the date on which the problem happened to notify us about it, after which time we have no obligation to investigate and refund you;
- you will only be entitled to lodge a claim through the UK Financial Ombudsman Service where you fulfil the UK Financial Ombudsman Service’s claimant criteria from time to time;
- we are not obliged to comply with the information requirements set out in Title III of PSD2 and their equivalents in any implementation of PSD2 in member states of the European Economic Area that may apply to you (“PSD2 transpositions”); and
- articles 72 and 89 of PSD2 and equivalent provisions in PSD2 transpositions do not apply to your use of our service, meaning that, even where we may say so otherwise in this user agreement, we are not liable to you for the losses or damage you may suffer under those articles and provisions.

The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law. This law secures privacy rights for California consumers, including:



- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.
- Businesses are required to give consumers certain notices explaining their privacy practices. The CCPA applies to many businesses, including data brokers.
- 
- If you are a California resident, you may ask businesses to disclose what personal information they have about you and what they do with that information, to delete your personal information and not to sell your personal information. You also have the right to be notified, before or at the point businesses collect your personal information, of the types of personal information they are collecting and what they may do with that information. Generally, businesses cannot discriminate against you for exercising your rights under the CCPA. Businesses cannot make you waive these rights, and any contract provision that says you waive these rights is unenforceable.
- By using the Services, you accept the terms of this Policy and our Terms of Use, and consent to our collection, use, disclosure, and retention of your information as described in this Policy. If you have not done so already, please also review our terms of use. The terms of use contain provisions that limit our liability to you and require you to resolve any dispute with us on an individual basis and not as part of any class or representative action. IF YOU DO NOT AGREE WITH ANY PART OF THIS PRIVACY POLICY OR OUR TERMS OF USE, THEN PLEASE DO NOT USE ANY OF THE SERVICES.

---

## **Complete agreement and third party rights**

This user agreement sets forth the entire understanding between you and us with respect to our service.

If any provision of this user agreement is held to be invalid or unenforceable, such provision shall be struck out and the remaining provisions shall be enforced.

A person who is not a party to this user agreement has no rights under the Contracts (Rights of Third Parties) Act 1999 to rely upon or enforce any term of this user agreement (except for the third parties falling under the definition of “iATM” in the **Indemnification and Limitation of Liability** section above, in respect of their



rights as specified in this user agreement) but this does not affect any right or remedy of third parties which exists or is available apart from that act.

---

### **iATM as Login Method**

We may allow you to authenticate with iATM when you log into certain external websites or mobile apps. If we do so, we may share your login status with any third party enabling you to log in in this way, as well as the personal and other wallet information that you consent to being shared so that the third party can recognize you. iATM will not give the third party access to your wallet and will only make payments from your wallet to that third party with your specific authorization and instruction.

If you enable visitors to authenticate with iATM when they log into your website, app, or your customer wallets, you must agree to any specific terms applicable when this functionality is made available to you and comply with any specifications in any integration manual or guideline. We do not guarantee or otherwise represent the identity of any user of this login method. We will not share with you the personal and other wallet information of the user (including login status) held by iATM unless the user has consented to our disclosure of that information to you.

---