

INSTABRIDGE PRIVACY NOTICE

Please read the following carefully to understand our practices regarding your personal data and how we will treat it.

1. INSTABRIDGE

- 1.1 This Privacy Notice is issued by, and applies to all services provided by, Metaverse (Radix) Limited (“Metaverse”, “us”, or “we”).
- 1.2 Metaverse (Radix) Limited whose registered office is First Floor La Chasse Chambers, 10 La Chasse, St Helier, JE2 4UE, Jersey, will process personal data in accordance with the provisions of this Notice.
- 1.3 The Instabridge service is provided by Metaverse and facilitates the transfer of Radix tokens from the Radix ledger to and from other crypto ledgers.

2. THIS PRIVACY NOTICE

- 2.1 This Privacy Notice describes what personal data the Instabridge service (“Instabridge”) will collect about you, why we collect that information, how we may use that information, and the steps we take to ensure that it is kept secure.
- 2.2 This notice may be amended from time to time and new versions will be published on our website which can be found at: <http://instabridge.io/terms/privacy>

3. HOW DOES INSTABRIDGE COLLECT DATA?

- 3.1 **You provide information directly to us:** places where you directly provide us with personal data include:
 - (a) filling in forms on the Instabridge website;
 - (b) corresponding with us (for example, by email or submitting job applications);
 - (c) accessing the Instabridge website;
 - (d) sharing data via Instabridge’s social media accounts;
 - (e) reporting a problem with the Instabridge website; or
 - (f) when you sign up to Instabridge mailing lists.
- 3.2 **By communicating with you:** we collect the content of all communications between yourself and us, this may include the recording of any calls, email conversations or other communications.
- 3.3 **Through cookies and technology tracking:** each time you visit the Instabridge website, we will automatically collect technical data and usage data. We collect this data using cookies and other similar technologies.
- 3.4 **Through third parties and publicly available sources:** we will receive personal data about you from various third parties and public sources as set out below:
 - (a) Third party partners of Instabridge – this includes third parties who you consent to share their data with us, such as Instapass; and
 - (b) Publicly accessible sources such as international sanctions lists, electoral registers, company registers, online directories, social networks and internet searches; and

- (c) We also work with third parties (including, for example business partners, sub-contractors in services, search information providers or email marketing providers) and we may receive certain information about you from them.

4. WHAT PERSONAL DATA DO WE COLLECT?

4.1 We collect personal data throughout our relationship with you.

4.2 We collect the following types of personal data:

- (a) Identity Data such as your first, middle and last names, date of birth, gender identity, nationality;
- (b) Personal Identification Data such as your National Insurance Number, Citizen Number, Unique National identity number, social insurance number, Passport, Driving Licence, residency card, ID card;
- (c) Contact Data such as your personal email address, residential address, phone number;
- (d) Professional Data such as your employment status, employer, role details, professional affiliations, whether you are a politically exposed person (“**PEP**”), or a close affiliate of a PEP, sanctions or disqualifications;
- (e) Demographic Data such as age, date of birth, nationality;
- (f) Financial Data such as your income, history of bankruptcy filings, history of insolvency filings, source of funds, source of wealth, bank statements, utility bills;
- (g) Technical Data including online identifiers such as Internet Protocol (IP) address, type of device you use, mobile network information, browser information, operating system, server logs, language;
- (h) Details of services provided, tokens or assets received and exchanged; and
- (i) Information on criminal offences which may include data or information concerning criminal activity; allegations; investigations and proceedings; unproven allegations; personal data of victims and witnesses of crime; information about penalties, conditions or restrictions placed on an individual as part of the criminal justice process; or civil measures which may lead to a criminal penalty if not adhered to.

4.3 The list above is not exhaustive, and Instabridge may also collect and process other data to the extent that this is considered necessary for the provision of our services or our compliance with legislative requirements.

5. SPECIAL CATEGORIES OF PERSONAL DATA

5.1 The only special category personal data collected by Instabridge is personal data relating to your criminal activity.

5.2 Instabridge will only collect data relating to your criminal activity where we have lawful grounds to do so. Where we collect data relating to your criminal activity, we rely on one, or both, of the following grounds:

- Your consent: where you provide your explicit consent to the processing;
- The prevention of unlawful acts;
- The processing is necessary for a legal obligation of Instapass (other than a contractual obligation); and/or
- Information has been made public as a result of any step deliberately taken by you.

6. DOES OUR WEBSITE USE COOKIES?

Cookies are pieces of information that your web browser transfers to your computer's hard drive for record keeping purposes. They can be used to store information about your preferences on a particular website. Most browsers are initially set to accept cookies, but you can set your browser to refuse them if you want to. Instabridge uses cookies to give a more efficient and personalised service to its clients.

7. HOW DOES INSTABRIDGE USE PERSONAL DATA?

7.1 Our use of your personal data will always have a lawful basis, and this will be determined by the purpose for which your personal information is processed. We use and collect personal data on the basis of:

- (a) **Consent:** we will obtain your consent to use your personal data wherever necessary;
- (b) **Contractual necessity:** to enter or perform a contract with you or any contracting entity;
- (c) **Legitimate Interest:** we will use your personal data where we have a legitimate interest, this is where we use your personal data in a way that you would reasonably expect; or
- (d) **Obligation:** where we need to use your personal data to comply with our legal obligations.

8. CONTRACTUAL NECESSITY

8.1 We may process your information during the provision of services, including:

- (a) our agreement with you to facilitate the bridging of your tokens – this involves conducting financial risk assessments and background checks for regulatory and compliance purposes;
- (b) administering your account with us;
- (c) to provide the Instabridge service;
- (d) to perform, or to satisfy identity verification services including anti-money laundering checks and know-your-client checks;
- (e) securing validation of the information you provide to us from multiple third-party sources;
- (f) required in the course of your employment by Instabridge;
- (g) to maintain and manage our relationships with you and for ongoing customer service;
- (h) communications with you regarding Instabridge, through any forum, including through Instabridge social media accounts; and
- (i) delivery of marketing and promotional offers and notification of partner events.

9. LEGAL OBLIGATIONS

9.1 When you or another party apply to use the Instabridge services, we are required by law to collect and process certain personal information about you. This may include processing to:

- (a) verify your identity;
- (b) perform checks and monitor transactions and location data for the purposes of preventing and detecting crime and to comply with laws relating to money

laundering, fraud, terrorist financing, bribery and corruption and international sanctions. This may require us to provide information about criminal convictions and offences, to gather intelligence on crimes and threats and to share data with law enforcement and regulatory bodies;

- (c) share data with law enforcement, tax authorities and other government and fraud prevention agencies where we have a legal obligation to do so, including reporting suspicious activity and complying with production and other court orders;
- (d) delivering mandatory communications to customers or providing updates to terms and conditions of the provision of services;
- (e) investigate and resolve complaints;
- (f) conduct investigations into breaches of conduct and corporate policies by our employees;
- (g) manage contentious regulatory matters, investigations, and litigation;
- (h) perform assessments and analyse customer data for the purposes of managing, improving, and fixing data quality;
- (i) provide assurance that Instabridge has effective processes to identify, manage, monitor, and report the risks it is or might be exposed to;
- (j) investigate and report on incidents or emergencies on Instabridge's properties and premises; and
- (k) coordinate responses to business disrupting incidents and to ensure facilities, systems and people are available to continue to provide services.

10. LEGITIMATE INTERESTS OF INSTABRIDGE

10.1 Instabridge will process your personal data where it is necessary for us to:

- (a) manage our risks and determine what services we can offer and the terms of those services;
- (b) carry out financial risk assessments and for risk reporting and risk management;
- (c) protect our business by preventing financial crime, or from being used to facilitate financial crime;
- (d) develop, test, monitor and review the performance of services, internal systems and security arrangements offered by Instabridge;
- (e) assess the quality of services to clients;
- (f) provide staff training;
- (g) analyse your use of our site and gathering feedback to enable improvement of our site and your experience including development of user experience;
- (h) provide you with access to our corporate literature and information about our services;
- (i) prevent and detect fraud and abuse; and
- (j) enable third parties to carry out technical, logistical and other functions on our behalf.

11. WHO DOES INSTABRIDGE PROVIDE INFORMATION TO?

11.1 To provide services to you, Instabridge may be required to share personal data with third parties.

- 11.2 Instabridge may disclose or transfer personal data collected by Instabridge insofar as reasonably necessary for the purposes of providing or receiving services or for compliance purposes as well as on the legal basis set out in this notice.
- 11.3 Except as described below, Instabridge will not disclose, transfer, or sell your personal data to any third party without your consent.
- 11.4 The following are potential recipients of data:
- (a) Instabridge's affiliated and related companies (which means, for the purposes of this Privacy Notice, any of the Radix Foundation's subsidiary companies, including subsidiaries of subsidiaries, and any of the Radix DLT Limited's subsidiary companies, including subsidiaries of subsidiaries) including, without limitation:
 - (i) Metapass (Radix) Limited, a company incorporated in Jersey, and a wholly owned subsidiary of Radix Tokens (Jersey) Limited, for the purposes of providing the Instapass service;
 - (ii) Radix DLT Limited, a company incorporated in England and Wales, for the purposes of providing support and assistance for the development and maintenance of the Radix ledger; and
 - (iii) Radix Tokens (Jersey) Limited, a company incorporated in Jersey, for the purposes of providing compliance staff and services.
 - (b) Mongo DB, Inc, who provides document database and storage services. Your data will be stored in a Mongo database hosted in the EU;
 - (c) HelpScout PBC, who provides customer support services. Your data will be stored in a Mongo database hosted in the United States;
 - (d) Twilio Inc. (trading as Sendgrid), a Delaware corporation, for the purposes of delivering transactional and marketing emails via their Sendgrid services. Your data will be stored in a Twilio database hosted in the EU;
 - (e) Mailerlite Limited, an Irish registered company who provide email marketing services. Your data will be stored in a Mongo database hosted in the EU;
 - (f) Bitpanda Custody, a UK registered company who provide custody and wallet services and receive data under Travel Rule regulations. Your data will be stored in the EU.
 - (g) service providers such as lawyers, accountants, banks, investment managers security consultants, on-chain investigation service providers, compliance service providers, sales agents, and exchanges, etc, who provide services to Instabridge, where disclosure is necessary to provide those services;
 - (h) sub-contractors, agents or service providers to Instabridge and its subsidiaries;
 - (i) courts or tribunals;
 - (j) regulators, registrars or other governmental or supervisory bodies with a legal right to the data or where necessary to fulfil Instabridge's legal and/or regulatory obligations;
 - (k) law enforcement agencies where disclosure is necessary for Instabridge or its subsidiaries to fulfil their legal and/or regulatory obligations; and
 - (l) intermediaries, including fiduciary agents, escrow agents, custody providers.

12. THIRD PARTY PROVIDERS WHO USE THE DATA

- 12.1 Where Instabridge employs another company or individual to perform any function on its behalf or to provide services to you, that third party will have access to personal data needed to perform their function, but they may not use it for other purposes.

- 12.2 Such functions include, administrative, computer, data processing, screening, debt collecting and compliance services. Such third parties must process the personal data in accordance with this Privacy Notice and applicable laws.
- 12.3 Instabridge does not allow third-party service providers to use your personal data for their own purposes. Instabridge only permits them to process your personal data for specified purposes and in accordance with our instructions.
- 12.4 Instabridge will seek to enter into an agreement with each third party setting out the respective obligations of each party, to ensure they process personal data with the same level of security and confidentiality as Instabridge and to be reasonably satisfied that the third party has measures in place to protect data against unauthorised or accidental use, access, disclosure, damage loss or destruction.
- 12.5 If authorised by you, Instabridge will disclose data to any third party that you request. Instabridge is not responsible for any such third party's use of your data, which will be governed by their agreement with you.
- 12.6 The personal data that Instabridge holds will be used and stored principally in Jersey and the European Economic Area (EEA). When Instabridge discloses data to third parties to satisfy the purposes outlined above, the third parties are generally located within Jersey or the European Economic Area (EEA).
- 12.7 However, Instabridge may disclose or transfer personal data to third parties located outside Jersey and the EEA; if such third parties are located in countries that do not ensure an equivalent level of protection for your personal data, Instabridge will use best endeavours to ensure that the third party will protect the personal data to an equivalent standard as is in force in Jersey and/or the EEA. You may contact us for an explanation of the basis on which we have transferred your personal information and, where relevant, to request a copy of the legal safeguards we have put in place.

13. RETENTION OF PERSONAL DATA

- 13.1 Instabridge will process and store your personal data for the duration of our services to you in accordance with financial services legislation and the data protection legislation in place in Jersey from time to time.
- 13.2 Instabridge will endeavour to delete any personal data where it is not necessary for it to be held. Instabridge will continue to store your personal data as long as necessary to fulfil legal (e.g., anti-money laundering, proceeds of crime and countering the financing of terrorism legislation), regulatory, contractual or statutory obligations, for the establishment, exercise or defence of legal claims and in general where Instabridge has a legitimate interest for doing so.

14. PROTECTION OF YOUR PERSONAL DATA

- 14.1 Instabridge regards the lawful and appropriate treatment of your personal data as fundamental to our successful operation and to maintaining confidence and trust between Instabridge and its customers. In fulfilling this objective, Instabridge will:
- (a) ensure that your personal data is not used for any purposes that is incompatible with this Privacy Notice;
 - (b) ensure that any processing of your personal data is fair and transparent and sufficient for the uses set out above;
 - (c) endeavour to keep your personal data up to date;
 - (d) retain your personal data no longer than necessary;
 - (e) ensure that our staff are trained to handle personal data appropriately and securely;

- (f) implement appropriate technical and organisational measures to:
 - (i) enable inaccuracies to be corrected and minimise the risk of errors;
 - (ii) secure personal data appropriately;
 - (iii) protect your personal data against unauthorised or unlawful access or processing and against accidental loss or destruction.

14.2 The transmission of information via the internet is, unfortunately, not completely secure. Although Instabridge will do its best to protect your personal data, we cannot guarantee the security of your data transmitted to our website. Any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

15. YOUR RIGHTS

15.1 You have the following rights:

- (a) **Right of access to your information** (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- (b) **Request correction of the personal data that we hold about you.** This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- (c) **Request erasure of your personal data.** This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- (d) **Object to processing of your personal data** - where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which means you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
- (e) **Right to data portability** – you have the right to request that a copy of the personal data that Instabridge holds about you is sent to another entity, or to you.
- (f) **Right to object to direct marketing** – you have the right to object at any time to the processing of your personal data for direct marketing purposes by Instabridge. We will obtain your express opt-in consent before we share your personal data with any third party for any marketing purpose.
- (g) **Right to withdraw consent** - where the processing of your personal data is based on consent, you have the right to withdraw that consent without detriment at any time by contacting us.
- (h) **Right to object to automated decision making and/or profiling** - Instabridge does not currently profile data, nor make decisions by purely automated means, but should we do so, you have the right to object to your data being used in automated decision making and/or profiling.

16. RIGHT TO REQUEST THAT INSTABRIDGE RESTRICTS THE PROCESSING OF YOUR PERSONAL DATA

16.1 You have the right to ask Instabridge to restrict processing of your personal data where:

- (a) you contest the accuracy of the personal data held by Instabridge;
- (b) the processing is unlawful, but you objected to the deletion of the personal data and requested that the use be restricted instead;
- (c) Instabridge no longer needs the personal data for the processing purpose, but you require them for legal reasons; or
- (d) you objected to processing and Instabridge is investigating whether there are legitimate grounds to override your objection.

17. CONTACTING US

17.1 If you do not wish to receive email or other mail from Instabridge or for Instabridge to use personal data that we gather, please contact support@instabridge.io in the first instance.

17.2 If you contact us in relation to your rights, we will do our best to accommodate your request or objection. You can help us maintain the accuracy of your information by notifying us of any change at support@instabridge.io (or via your usual contact).

17.3 If you have any questions, concerns or complaints with respect to this Privacy Notice, the way Instabridge is handling your data or have any other queries or concerns, please contact our Data Protection Officer directly at support@instabridge.io or in writing at Metaverse (Radix) Limited, First Floor, La Chasse Chambers Ten La Chasse, St Helier, Jersey, JE2 4UE.