BRIDGE DIGITAL PLATFORM

Privacy Policy

Version 2.2
Effective Date: 25 February 2026

Bridge Digital Platform d.o.o.
Strossmayerova 16, 51000 Rijeka, Croatia
Privacy contact: info@bridgedigitalplatform.com

Primary hosting location: European Union

1. Introduction

This Privacy Policy explains how Bridge Digital Platform d.o.o. ("Bridge", "we", "us" or the "Controller") collects, uses and protects personal data in connection with the Bridge Digital Platform (the "Platform").

This Policy forms part of, and must be read together with:

- the Terms of Use;
- the Professional Partnership Agreement;
- Annex E (Lead Tracking, Variable Compensation and Data Minimisation).

2. Scope

This Policy applies to personal data processed in connection with:

- user account creation and access management;
- lead generation and routing;
- platform security and operational integrity;
- partner onboarding and relationship management;
- analytics and service optimisation.

It does not apply to third-party websites or services not controlled by Bridge.

3. Roles and Allocation of Responsibility

3.1 Bridge as Controller

Bridge acts as Data Controller in relation to:

- account registration and authentication;
- partner profile administration;
- lead intake and technical attribution (including Lead ID systems);
- platform security, logging and abuse prevention;
- contractual and administrative management of partner relationships.

3.2 Partners as Independent Controllers

Professional services rendered by Partners to end clients fall outside the scope of the Platform.

Bridge:

- does not provide legal or professional services;
- does not access case files or mandate content;
- does not request or process data revealing the substance of professional advice.

Partners act as independent Controllers in relation to their professional mandates.

3.3 Data Minimisation and Aggregation

For reporting and compensation purposes:

- Bridge relies on technical identifiers (e.g., Lead ID);
- financial and activity reporting is aggregated;
- no client-level professional details are processed by Bridge.

Where verification is required, pseudonymised documentation may be used.

4. Categories of Personal Data

Depending on use of the Platform, Bridge may process:

4.1 Account Data

Name, email address, organisational role, authentication credentials (securely hashed), access tokens.

4.2 Professional Profile Data

Qualification details, practice areas, and information voluntarily published by the Partner.

4.3 Lead Data

Contact information submitted through forms (e.g., name, email, country, subject matter), together with technical metadata and Lead ID.

4.4 Technical and Security Data

IP address, device information, access logs, system events and anomaly detection data.

4.5 User-Generated Content

Documents and materials voluntarily uploaded within Platform functionality.

Special Categories of Data

Bridge does not intentionally collect special categories of data (Art. 9 GDPR).
If such data are submitted, they must be strictly necessary and lawfully processed. Enhanced safeguards may apply.

5. Legal Bases for Processing

Bridge processes personal data on the following grounds:

Contract (Art. 6(1)(b) GDPR)
For account management, partner onboarding and service delivery.

Legitimate Interest (Art. 6(1)(f) GDPR)
For platform security, abuse prevention, lead attribution and service improvement.

Legal Obligation (Art. 6(1)(c) GDPR)
Where required by applicable law.

Consent (Art. 6(1)(a) GDPR)
Where required, including certain analytics or communications.

6. Artificial Intelligence

The Platform may incorporate AI-assisted functionalities for drafting or operational support.

AI tools:

- operate under human supervision;
- are not used for discriminatory profiling;
- do not produce legally binding automated decisions.

Bridge does not use partner or user data to train external general-purpose AI models unless explicitly agreed and lawfully justified.

7. Data Sharing

Personal data may be disclosed to:

- authorised Bridge personnel;
- authorised partners (within defined permissions);
- IT service providers acting as processors;
- competent authorities where legally required.

8. International Transfers

Primary hosting occurs within the European Union.

Where data are transferred outside the EU, Bridge implements appropriate safeguards, including Standard Contractual Clauses and supplementary measures.

9. Data Retention

Retention periods are determined by operational necessity and legal risk management.

Indicative periods:

- Account data: duration of account + 24 months post-closure;
- Partner contractual data: duration of relationship + 24 months;
- Lead metadata: 12 months (extendable to 24 months for dispute resolution);
- Security logs: 180 days;
- Backups: 60-day rolling cycle.

Retention may be adjusted where legally or operationally required.

10. Cookies and Analytics

The Platform uses:

- strictly necessary technical cookies (no consent required);
- analytics tools subject to consent where applicable.

Users may manage preferences through the cookie management interface.

11. Data Subject Rights

Data subjects may exercise their rights under the GDPR, including:

- access;
- rectification;
- erasure;
- restriction;
- objection;
- portability.

Requests may be submitted to:
info@bridgedigitalplatform.com

Data subjects have the right to lodge a complaint with a competent supervisory authority.

12. Security

Bridge implements appropriate technical and organisational measures, including:

- access control and privilege management;
- encryption in transit;

- monitoring and logging;
- backup and recovery procedures;
- vulnerability management.

Personal data breaches are handled in accordance with GDPR obligations.

13. Amendments

Bridge may update this Policy to reflect legal, technical or organisational developments. Material changes will be communicated appropriately.

14. Contact

Bridge Digital Platform d.o.o.
info@bridgedigitalplatform.com