JS Plus – Privacy Policy

Last Updated: January 1, 2025

1. Introduction

This Privacy Policy describes how **JS Plus** (“JS Plus,” “we,” “us,” or “our”) collects, uses, stores, protects, and discloses information when providing software development, consulting, infrastructure, and related technical services, as well as when operating our website located at **jsplus.dev**.

JS Plus is a software development company based in Bosnia and Herzegovina serving clients worldwide, including organizations regulated by United States federal agencies. By accessing our website or engaging with us professionally, you acknowledge this Privacy Policy. For clients subject to specific regulatory or contractual requirements, those obligations take precedence.

---

2. Definitions

For clarity and consistency:

“Personal Data” means any information relating to an identified or identifiable individual.

“Client Data” means any data, files, credentials, content, documents, code, or other materials provided to us by or on behalf of a client, including any regulated or sensitive information handled strictly under client instructions.

“Processing” means any operation performed on Personal Data, including collection, storage, access, transfer, or deletion.

“Sub-processor” means a third party engaged by JS Plus to support the delivery of our services.

---

3. Information We Collect

3.1 Information You Provide

We collect information voluntarily provided when you contact us or engage our services, including:

- Name, email address, phone number, and other contact details
- Company information
- Project specifications, documentation, and technical requirements
- Access credentials needed for development or integration, handled solely for project purposes and subject to appropriate security controls.
- Billing and invoicing information
- Test data, sample files, logs, and QA materials
- Any additional instructions, communications, or materials necessary for project delivery

We do **not** collect or process end-user consumer information unless explicitly provided for development, testing, or debugging, and such information is processed only under client instructions.

3.2 Information Collected Automatically

When you access our website, we may collect:

- IP address
- Browser type, device type, and version
- Pages viewed and timestamps
- Server logs and diagnostic data

We do **not** use third-party advertising networks, behavioral profiling tools, or marketing analytics.

Our website and hosting infrastructure may use strictly necessary technical cookies and server-side logging for security and performance.

---

4. Legal Basis for Processing (GDPR/UK GDPR)

When we process Personal Data relating to individuals in the EU, EEA, or UK, we rely on one or more of the following legal bases:

- **Contract Performance:** To deliver our services, respond to inquiries, and fulfill obligations under agreements.
- **Legitimate Interests:** Including security, fraud prevention, service improvement, and business operations.
- **Legal Obligation:** To comply with applicable laws, regulatory requirements, and governmental requests.
- **Consent:** When explicitly requested and legally required for specific processing activities.

For clients outside these regions, including US-based and SEC-regulated entities, processing is based on applicable contract terms and relevant legal obligations.

---

5. How We Use Information

We process information solely for legitimate business purposes and only as instructed by the client, including:

- Providing software development, consulting, and infrastructure services
- Communicating with clients and responding to inquiries
- Setting up and maintaining development or production environments
- Security, authentication, and access control
- Accounting, invoicing, and internal business administration
- Compliance with contracts, legal requirements, and industry regulations

We do **not**:

- Sell Personal Data
- Use client data for advertising or marketing
- Share information with unrelated third parties

---

6. Confidentiality

All client information is treated as strictly confidential. Access is restricted to employees and contractors who require it for their role and are bound by confidentiality and security obligations.

We do not disclose client information to third parties unless required by law or explicitly approved by the client, and we do not use client information for any internal purpose unless authorized.

---

7. Client Project Data

7.1 Use of Client-Provided Data

Client Data such as credentials, documents, recordings, datasets, or system access is used strictly for:

- Development
- Testing
- Debugging
- Support
- Deployment
- Maintenance

and is **not used for any other purpose** without client authorization.

7.2 AI Tools, Generative Models, and Code Assistants

- We **do not upload** client data into public AI models.
- AI-assisted tools may be used **only through client-controlled accounts** or with client approval.
- AI tools are not permitted to retain or store client data unless explicitly authorized by the client.
- Tools such as GitHub Copilot or ChatGPT are used **only in a manner compliant with client requirements**, and never with sensitive client data unless explicitly authorized.
- A complete list of AI tools used in your project is available upon request.

7.3 Storage and Access Controls

- Data is stored using encrypted storage solutions or client-approved platforms, and any client credentials are handled and stored using secure, encrypted methods.
- Access is controlled using role-based permissions.
- Access is revoked immediately upon project completion or personnel reassignment.

7.4 Retention and Deletion

Unless the client specifies otherwise, we retain project-related materials for up to 12 months after project completion to support continuity and maintenance, or for any shorter period required by client policies or applicable regulatory obligations.

Upon request, we promptly delete:

- Credentials
- Test data
- Logs
- Backups
- Any other client-specific materials

For clients subject to regulatory retention requirements (such as SEC-regulated entities), we follow the retention period defined in the contract or client instructions.

---

8. Sub-Processors and Third-Party Services

We use reputable third-party providers to support our services, including:

- **GitHub** – source code hosting and repository management
- **AWS, Hetzner, DigitalOcean** – infrastructure, compute, networking, and storage
- **CI/CD platforms** – automated builds, deployments, and testing
- **Email and communication platforms** – secure communication and support
- **Project management tools** – Jira, Notion, Trello, and similar tools

These providers may process limited Personal Data or project information as necessary to provide their services. All sub-processors are required to meet appropriate confidentiality, security, and data protection standards.

We do not introduce new sub-processors with access to client data without notifying the client and obtaining required approvals where required by contract or regulation.

---

9. Security Measures

We apply industry-standard technical and organizational measures to safeguard information, including:

- TLS/SSL encryption
- Encrypted storage and secure credential handling
- Role-based access controls
- Access logging and monitoring
- Segregation of development, staging, and production environments

- Regular updates, patches, and secure coding practices
- Intrusion-detection and firewall measures where applicable

These controls apply to both our own systems and any approved third-party platforms used to deliver services. Although no system can guarantee absolute security, we use commercially reasonable safeguards to protect all information entrusted to us.

---

10. Data Breach Notification

If a confirmed data breach affects client information, we will:

- Notify affected clients without undue delay
- Provide details regarding the nature, scope, and impact
- Outline mitigation measures taken
- Cooperate with clients to fulfill any regulatory reporting obligations

For GDPR-governed data, we follow the 72-hour notification requirement.

---

11. International Data Transfers

We may process Personal Data in Bosnia and Herzegovina or in jurisdictions where our cloud providers operate. For clients outside the EU/EEA or UK, including US-based and SEC-regulated entities, cross-border processing occurs only as permitted under applicable contracts and security controls.

For clients in the EU/EEA or UK, we rely on:

- Standard Contractual Clauses (SCCs)
- Client-approved transfer mechanisms
- GDPR/UK GDPR-compliant safeguards

---

12. GDPR and UK GDPR Rights

Individuals in the EU/EEA or UK may:

- Request access to their Personal Data
- Request correction or deletion
- Request restriction or objection to processing
- Request data portability
- Withdraw consent where applicable

We may require reasonable identity verification before processing such requests.

---

13. California Privacy Rights (CCPA/CPRA)

We do not sell or share Personal Data as defined under the CCPA/CPRA.

California residents may request:

- Disclosure of the categories of data collected
- Deletion of applicable Personal Data
- Information on the purposes of collection
- Equal treatment and non-discrimination for exercising privacy rights

Requests may be submitted by email.

“Do Not Track” Disclosure:
Because we do not use tracking cookies or behavioral profiling tools, our services do not respond to browser “Do Not Track” signals.

---

14. Children’s Privacy

Our services are not directed to children under 13. We do not knowingly collect Personal Data from children under 13 years of age, and we do not process children’s information in client projects unless explicitly provided by the client for development or testing purposes.

---

15. Changes to This Privacy Policy

We may update this Privacy Policy to reflect changes in our practices or legal requirements. Updates will be posted on our website with a revised “Last Updated” date, and we will notify clients of any material changes that affect how we process or safeguard client data.

---

16. Contact Information

For questions, requests, or concerns regarding this Privacy Policy, your data, or any privacy, security, or compliance matter, contact us at:

JS Plus
Sime Šolaje 1A
78000 Banja Luka
Bosnia and Herzegovina
Email: **info@jsplus.dev**
Website: **https://jsplus.dev**