GDPR-Aligned Development & Data Protection Practices

Introduction

We follow GDPR-aligned engineering and operational practices while designing, developing, deploying, and maintaining software systems for businesses serving users in the European Union (EU).

While we are not a certified GDPR authority, our development processes are aligned with GDPR principles to help our clients build compliant, secure, and privacy-first digital products.

1. Data Minimization & Purpose Limitation

- We collect and process only data that is necessary for defined business purposes.
- Personal data fields are reviewed during system design to avoid unnecessary data capture.
- Clear documentation is maintained for data usage within the application.

2. Consent & User Rights Support

Our systems are designed to support:

- Explicit user consent mechanisms
- Consent withdrawal flows
- User access requests
- Data correction and deletion workflows

These features can be customized based on client requirements and regulatory needs.

3. Role-Based Access Control (RBAC)

- Access to sensitive data is restricted based on user roles.
- Admin, operator, and user permissions are clearly defined.
- Least-privilege access principles are followed across systems.

4. Data Storage & Hosting Practices

- Systems can be configured to use EU-based servers when required.
- Data residency requirements are discussed and implemented during project planning.
- Secure cloud infrastructure (AWS, Azure, GCP) is used following best practices.

5. Security Measures

We implement industry-standard security practices including:

- Encrypted data transmission (HTTPS / TLS)

- Secure authentication mechanisms
- Password hashing and token-based authentication
- Regular dependency and vulnerability reviews

6. Logging, Monitoring & Audit Trails

- Application logs are implemented for operational transparency.
- Sensitive data is excluded from logs wherever possible.
- Audit trails can be enabled for critical user actions.

7. Data Retention & Deletion

- Data retention policies are configurable based on business and regulatory needs.
- Automated or manual data deletion mechanisms can be implemented.
- Backups follow defined retention cycles.

8. Third-Party Integrations

- Third-party services are evaluated for security and data handling practices.
- Only required data is shared with external systems.
- Integrations are documented clearly.

9. Confidentiality & IP Protection

- Strict internal confidentiality policies are followed.
- Client intellectual property remains fully owned by the client.
- Code repositories and access credentials are secured.

Disclaimer

This document describes our internal development and operational practices aligned with GDPR principles. It does not constitute legal advice or formal GDPR certification. Clients are encouraged to consult legal professionals for compliance validation specific to their jurisdiction.