Primalt

PRIVACY POLICY TERMS

1. Introduction and Commitment to Privacy

Primalt International Limited ("Primalt", "Company", "we", "us", "our") is an international technology and software development company registered in Malta, the United States, and Albania.

Primalt provides intelligent digital solutions including:

- Artificial Intelligence systems
- Web and mobile applications
- DevOps and cloud infrastructure
- Cybersecurity and digital transformation services
- Data analytics and software engineering.

Primalt recognizes that personal data protection is a fundamental right under European Union law. We are committed to processing personal data lawfully, fairly, transparently, and securely.

This Privacy Policy explains:

- What personal data we collect
- Why we collect it
- How it is used and protected
- International transfers
- Individual rights
- Legal safeguards and limitations.

2. Scope of Application

This Policy applies to:

- Website visitors
- Clients and prospective clients
- Business partners
- Service users
- End users of systems where Primalt acts as Controller.

Where Primalt acts solely as Data Processor, processing is governed by applicable contractual agreements and Data Processing Agreements (DPA).

3. Legal Framework

Processing is conducted in accordance with:

European Union

- GDPR (Regulation EU 2016/679)
- E-Privacy Directive
- EU Charter of Fundamental Rights
- EU Artificial Intelligence Act (where applicable)

Malta

- Data Protection Act (Cap. 586)

United States

- CCPA/CPRA where applicable
- FTC consumer protection standards.

Where conflicts arise, the higher standard of protection may be applied.

4. Roles and Responsibilities

4.1 Data Controller

Primalt acts as Controller when determining purposes and means of processing, including:

- Website operations
- Marketing communications
- Recruitment
- Business development.

4.2 Data Processor

Primalt acts as Processor when:

- Developing SaaS systems
- Managing cloud environments
- Implementing AI systems for clients.

The Client remains Controller and responsible for lawful data collection.

5. Categories of Personal Data

We may process:

Identity and Contact Data

- Name
- Email
- Phone number
- Company details.

Technical Data

- IP address
- Device information
- Usage logs.

Business Communications

- Project requirements
- Contractual information.

AI System Data

- Client-provided datasets
- Development metadata.

Special category data is processed only when legally permitted.

6. Principles of Processing

All processing follows GDPR Article 5:

- Lawfulness and fairness
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability.

7. Legal Bases for Processing

Processing relies on:

- Contract performance
- Legal obligation
- Legitimate interests
- Consent where required.

Legitimate interest assessments are conducted where applicable.

Primalt

8. Privacy by Design and Default

Privacy is integrated into:

- Software architecture
- Secure development lifecycle
- DevOps processes
- Access controls.

9. Artificial Intelligence and Automated Processing

Primalt develops AI systems and implements:

- Human oversight mechanisms
- Bias risk assessments
- Transparency measures
- GDPR Article 22 safeguards.

AI outputs are probabilistic and must be independently validated by users.

10. Cookies and Tracking

We may use:

- Necessary cookies
- Analytics cookies
- Performance cookies.

Non-essential cookies require consent for EU users.

11. Data Sharing and Sub processors

Data may be shared with:

- Cloud providers
- Security vendors
- Legal authorities.

Sub processors must meet GDPR Article 28 requirements.

12. International Data Transfers

Transfers outside the EEA rely on:

- Standard Contractual Clauses
- Transfer Impact Assessments
- Supplementary safeguards.

Compliance reflects CJEU Schemes II requirements.

13. Data Retention

Data is retained only as necessary for:

- Contractual obligations
- Legal compliance
- Legitimate business purposes.

After expiration, data is deleted or anonymized.

14. Security Measures

Primalt applies:

- Encryption at rest and transit
- Multi-factor authentication
- Role-based access
- Monitoring and incident response.

Absolute security cannot be guaranteed.

15. Data Subject Rights

Individuals may:

- Access data
- Request correction
- Request deletion
- Restrict processing
- Request portability
- Object to processing.

Requests are processed within statutory timelines by contacting : contact@primal.com.

16. U.S. Privacy Rights

Where applicable, individuals may request:

- Access
- Deletion
- Correction
- Opt-out of certain processing.

17. Data Breach Response

In case of breach:

- Investigation initiated immediately
- Supervisory authorities notified within 72 hours where required
- Affected individuals informed where risk is high.

18. Children's Data

Services are not directed to children.

19. Third-Party Websites

We are not responsible for external websites linked from our platform.

20. Advanced Legal Governance

Primalt applies GDPR in alignment with:

- EDPB guidance
- CJEU jurisprudence including Schemes I & II
- European enforcement precedents.

21. Client Responsibility and Indemnification

Clients acting as Controllers warrant lawful data sourcing and agree to indemnify Primalt against claims arising from unlawful instructions or datasets.

22. Limitation of Liability

To the maximum extent permitted:

Primalt is not liable for:

- Indirect damages
- Regulatory penalties caused by client misuse
- AI decision outcomes.

Liability is limited to fees paid unless mandatory law requires otherwise.

23. Third-Party Infrastructure Disclaimer

Primalt is not responsible for outages or incidents caused by external providers beyond reasonable control.

24. No Guarantee of Regulatory Compliance

Use of Primalt services does not constitute legal or regulatory compliance guarantees.

Primalt

25. Automated Decision Reliance Disclaimer

Clients must review automated outputs before critical decisions.

26. International Transfer Risk Acknowledgement

Users acknowledge inherent risks in cross-border processing despite safeguards.

27. Regulatory Cooperation

Primalt cooperates with supervisory authorities including Malta IDPC.

28. Updates

Policy may be updated periodically with notice 30 days before the update.

29. Enterprise Risk Allocation Framework

To ensure legal clarity:

- Primalt provides technological infrastructure and development services.
- Clients remain responsible for:
    - Business logic decisions
    - Regulatory compliance strategy
    - Data governance policies
    - Legal risk assessments.

Primalt does not assume regulatory responsibility unless explicitly agreed in writing.

30. Advanced Controller vs Processor Liability Allocation

Where Primalt acts as Processor:

- Client defines purposes and lawful basis.
- Client confirms data subject transparency obligations fulfilled.

Primalt:

- Processes only documented instructions.
- Is not responsible for unlawful instructions or datasets.

Client agrees to indemnify Primalt against:

- GDPR claims arising from controller decisions
- unlawful data sources
- improper consent mechanisms.

31. AI Governance and Algorithmic Responsibility

Primalt develops AI-enabled systems but does not control:

- Client deployment context
- End-user decisions
- Operational outcomes.

Therefore:

- AI outputs are informational tools only.
- Clients must perform human validation before critical use.

Primalt disclaims liability for:

- Bias arising from client datasets
- Incorrect decisions based on AI outputs
- Misinterpretation of predictive models.

32. Model Training Data Liability Shield

Clients warrant that all datasets used for:

- Training
- Testing
- Fine-tuning

are:

- Lawfully obtained
- Free of IP infringement
- GDPR compliant.

Primalt does not independently verify all datasets unless contracted for data auditing services.

33. Cross-Border Data Transfer Enterprise Clause

Transfers outside EEA rely on:

- Standard Contractual Clauses
- Transfer Impact Assessments
- Technical safeguards (encryption, access minimization).

Users acknowledge:

Absolute equivalence of legal protections cannot be guaranteed across jurisdictions.

Primalt

34. Security Standard of Care

Primalt implements industry-standard security measures aligned with:

- ISO 27001 principles
- OWASP guidelines
- Zero Trust access models.

However: No digital system can guarantee absolute security. Residual risk is acknowledged by users.

35. Platform Misuse Protection Clause

Primalt shall not be liable where:

- Client configures systems insecurely
- Client ignores security recommendations
- Third-party integrations introduce vulnerabilities.

36. Service Dependency & Infrastructure Disclaimer

Primalt relies on third-party infrastructure providers. Primalt is not liable for:

- Cloud outages
- Vendor downtime
- Infrastructure-level breaches outside Primalt's direct control.

37. Regulatory Compliance Non-Warranty

Unless explicitly stated in writing, Primalt does not guarantee:

- GDPR compliance
- AI Act compliance
- Cybersecurity certification.

Services provide tools enabling compliance but do not replace legal assessment.

38. Advanced Limitation of Liability Structure

To maximum legal extent, Primalt shall not be liable for:

- Indirect damages
- Loss of data or profits
- Reputational damage
- Regulatory fines imposed on clients.

Primalt

Total liability capped at fees paid during previous 12 months unless mandatory law applies.

39. Data Governance Charter

Primalt commits to:

- Data minimization by design
- Privacy-first architecture
- Ethical AI principles
- Transparent data processing.

40. EU AI Act Alignment Statement

Primalt aligns with risk-based AI governance including:

- Human oversight
- Documentation
- Risk assessment procedures.

41. Vendor and Sub Processor Governance

All vendors must:

- Sign GDPR-compliant agreements
- Maintain adequate security safeguards.

42. Legal Enforcement and Case Awareness

Compliance model informed by:

- Schemes I & II (CJEU)
- Meta Ireland enforcement (cross-border transfers)
- Google CNIL transparency decision
- Amazon Luxembourg consent case.

43. Governing Law and Jurisdiction Shield

Data disputes governed by: Maltese Legislation.

Primary jurisdiction: Malta.

Effective Date: *19 February 2026*