OSEVRA Limited - Privacy Policy

Effective Date: February 2026 **Last Updated:** February 2026 **Website:** www.osevra.com
Service Region: Asia-Pacific (APAC)

---

1. Introduction

OSEVRA Limited ("we," "us," "our," or "OSEVRA") is committed to protecting your privacy and ensuring you have a positive experience on our website and when using our services. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you visit our website www.osevra.com and use our services.

Please read this Privacy Policy carefully. If you do not agree with our policies and practices, please do not use our website or services. By accessing and using www.osevra.com, you acknowledge that you have read, understood, and agree to be bound by all the provisions of this Privacy Policy.

---

2. Applicable Privacy Laws

This Privacy Policy complies with privacy and data protection laws across the APAC region:

Australia:

- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- Spam Act 2003 (Cth)

New Zealand:

- Privacy Act 2020
- Health Information Privacy Code 2020

Singapore:

- Personal Data Protection Act (PDPA)
- Singapore Standards on Data Protection

Hong Kong:

- Personal Data (Privacy) Ordinance (PDPO)
- Code of Practice on Information Security

Japan:

- Act on the Protection of Personal Information (APPI)
- My Number Act

South Korea:

- Personal Information Protection Act (PIPA)
- Telecommunications Business Act

Malaysia:

- Personal Data Protection Act 2010 (PDPA)
- Malaysia Standards on Data Protection

Thailand:

- Personal Data Protection Act (PDPA) B.E. 2562 (2019)

Indonesia:

- Law No. 27 of 2022 on Personal Data Protection

Philippines:

- Data Privacy Act of 2012 (Republic Act No. 10173)
- National Privacy Commission Guidelines

Vietnam:

- Law on Information Security 2015
- Decree 13/2023/ND-CP on Data Protection

---

3. Information We Collect

3.1 Information You Provide Directly

Contact Forms and Inquiries: When you fill out contact forms, request information, or inquire about our services, we collect:

- Full name
- Email address
- Phone number
- Company name and position

- Message content
- Country and region

Account Registration: If you create an account on our website, we collect:

- Username and password
- Email address
- Full name
- Company information
- Billing address
- Payment information (processed securely through third-party providers)

Service Requests: When you request our services, we collect:

- Infrastructure requirements and specifications
- Technical information about your current systems
- Project details and timelines
- Budget information
- Compliance and security requirements

Customer Support: When you contact our support team, we collect:

- Communication records (emails, chat transcripts, call recordings)
- Issue descriptions and technical details
- Troubleshooting information
- Feedback and suggestions

Feedback and Surveys: When you participate in surveys or provide feedback, we collect:

- Survey responses
- Ratings and reviews
- Suggestions and comments
- Usage patterns and preferences

3.2 Information Collected Automatically

Website Usage Data: When you visit our website, we automatically collect:

- IP address and device identifier
- Browser type and version
- Operating system
- Pages visited and time spent on each page
- Referring website
- Search queries
- Click patterns and interactions
- Device type (desktop, mobile, tablet)

Cookies and Tracking Technologies: We use cookies, web beacons, pixels, and similar technologies to:

- Remember your preferences
- Track website usage
- Analyze visitor behavior
- Improve website functionality
- Deliver targeted content
- Prevent fraud

Analytics Data: Through analytics services (Google Analytics, Mixpanel, etc.), we collect:

- User journey and navigation patterns
- Conversion data
- Traffic sources
- Geographic location (country/region level)
- Device and browser information
- Session duration and bounce rates

Log Files: Our servers automatically create log files containing:

- Access timestamps
- IP addresses
- Requested resources
- HTTP status codes
- Referrer information
- User agent information

3.3 Information from Third Parties

Business Partners: We may receive information from:

- Resellers and channel partners
- Referral sources
- Marketing partners
- Technology partners

Social Media: If you interact with us on social media platforms, we may collect:

- Public profile information
- Comments and messages
- Engagement data
- Follower information

Publicly Available Sources: We may collect information from:

- Public business registries

- Industry directories
- News sources
- Government records
- Public databases

Third-Party Services: We may receive information from:

- Payment processors
- Email service providers
- CRM platforms
- Marketing automation tools
- Analytics providers

---

4. How We Use Your Information

4.1 Service Delivery

We use your information to:

- Provide and deliver our services
- Process service requests and orders
- Manage your account and subscriptions
- Deliver technical support
- Send service-related notifications
- Fulfill contractual obligations
- Maintain service quality and reliability

4.2 Communication

We use your information to:

- Respond to inquiries and requests
- Send transactional emails (confirmations, receipts, updates)
- Provide customer support
- Send newsletters and updates (with your consent)
- Notify you of changes to our services
- Send security alerts and notifications

4.3 Marketing and Promotion

With your consent, we use your information to:

- Send promotional emails and offers
- Notify you about new services and features
- Invite you to events and webinars
- Conduct marketing campaigns
- Personalize marketing communications
- Analyze marketing effectiveness

4.4 Business Operations

We use your information to:

- Improve our website and services
- Conduct research and analytics
- Develop new products and services
- Manage business operations
- Prevent fraud and abuse
- Comply with legal obligations
- Enforce our terms and policies

4.5 Legal and Compliance

We use your information to:

- Comply with legal requirements
- Respond to legal requests and court orders
- Protect our legal rights
- Investigate complaints and disputes
- Maintain audit trails
- Meet regulatory requirements

4.6 Data Analytics

We use your information to:

- Analyze usage patterns and trends
- Identify areas for improvement
- Understand customer needs
- Optimize website performance
- Personalize user experience
- Generate business intelligence

---

5. Legal Basis for Processing

We process your personal information based on the following legal grounds:

Contractual Necessity: Processing necessary to provide services you have requested or to perform a contract with you.

Legitimate Interests: Processing necessary for legitimate business interests including service improvement, fraud prevention, and business operations.

Consent: Processing based on your explicit consent for specific purposes such as marketing communications.

Legal Obligation: Processing required to comply with applicable laws, regulations, and legal requests.

Vital Interests: Processing necessary to protect your vital interests or the vital interests of others.

Public Task: Processing necessary to perform a task in the public interest or official authority.

---

6. Information Sharing and Disclosure

6.1 Service Providers

We share information with third-party service providers who assist us in operating our website and providing services, including:

- Cloud hosting providers
- Payment processors
- Email service providers
- Analytics providers
- CRM platforms
- Customer support tools
- Marketing automation services

These service providers are contractually obligated to maintain confidentiality and use information only for the purposes we specify.

6.2 Business Partners

We may share information with:

- Resellers and channel partners
- Technology partners
- Integration partners
- Co-marketing partners

Business partners are required to maintain confidentiality and comply with applicable privacy laws.

6.3 Legal Requirements

We may disclose information when required by law or when we believe in good faith that disclosure is necessary to:

- Comply with legal obligations
- Respond to lawful government requests
- Enforce our terms and policies
- Protect our rights, privacy, safety, or property
- Protect against fraud or security threats
- Protect the rights, privacy, safety, or property of others

6.4 Business Transfers

If OSEVRA is involved in a merger, acquisition, bankruptcy, dissolution, reorganization, or similar transaction or proceeding, your information may be transferred as part of that transaction. We will provide notice before your information becomes subject to a different privacy policy.

6.5 Consent-Based Sharing

With your explicit consent, we may share information with:

- Third-party marketers
- Research organizations
- Industry partners
- Other entities for specific purposes

You can withdraw consent at any time by contacting us.

6.6 Aggregated and De-Identified Information

We may share aggregated or de-identified information that cannot reasonably be used to identify you with:

- Business partners
- Research organizations
- Industry analysts
- Marketing partners
- Public audiences

---

7. Data Retention

7.1 Retention Periods

We retain personal information for as long as necessary to:

- Provide services you have requested
- Fulfill contractual obligations
- Comply with legal requirements
- Resolve disputes
- Enforce our agreements
- Pursue legitimate business interests

Specific Retention Periods:

- **Account Information**: Retained while account is active, plus 3 years after account closure
- **Transaction Records**: Retained for 7 years (required by financial regulations)
- **Customer Support Records**: Retained for 3 years
- **Marketing Communications**: Retained until you unsubscribe
- **Website Analytics**: Retained for 26 months
- **Log Files**: Retained for 90 days
- **Cookies**: Retained according to cookie type (session to 2 years)

7.2 Deletion and Destruction

When information is no longer needed, we securely delete or destroy it using:

- Secure deletion methods
- Data destruction services
- Physical destruction of storage media
- Anonymization and de-identification

---

8. Data Security

8.1 Security Measures

We implement comprehensive security measures to protect your information:

Technical Safeguards:

- Encryption of data in transit (TLS 1.2+) and at rest (AES-256)
- Secure authentication mechanisms (multi-factor authentication)
- Firewalls and intrusion detection systems
- Regular security updates and patches
- Vulnerability scanning and penetration testing
- Secure backup and recovery procedures

Administrative Safeguards:

- Access controls and role-based permissions
- Employee training on data protection
- Confidentiality agreements with staff
- Incident response procedures
- Data protection policies and procedures
- Regular security audits

Physical Safeguards:

- Secure data centers with controlled access
- Video surveillance and monitoring
- Locked storage for physical records
- Environmental controls
- Disaster recovery procedures

8.2 Data Breach Notification

In the event of a data breach, we will:

- Notify affected individuals without unreasonable delay
- Provide details of the breach and information affected
- Explain steps we are taking to address the breach
- Offer resources to help protect your information
- Comply with notification requirements in applicable laws

---

9. Your Privacy Rights

9.1 Access and Portability

You have the right to:

- Access your personal information
- Receive a copy of your information in a portable format
- Understand what information we hold about you
- Request information about how your data is used

How to Request: Contact office@osevra.com with "Access Request" in the subject line. We will respond within 30 days.

9.2 Correction and Update

You have the right to:

- Correct inaccurate information
- Update outdated information
- Complete incomplete information
- Request correction of errors

How to Request: Contact office@osevra.com with details of the corrections needed. We will update your information and confirm the changes.

9.3 Deletion and Erasure

You have the right to request deletion of your information in certain circumstances:

- When information is no longer necessary
- When you withdraw consent
- When you object to processing
- When processing is unlawful
- When required by law

Limitations: We may retain information when necessary for:

- Legal compliance
- Contractual obligations
- Fraud prevention
- Dispute resolution
- Legitimate business interests

How to Request: Contact office@osevra.com with "Deletion Request" in the subject line. We will respond within 30 days.

9.4 Objection and Restriction

You have the right to:

- Object to processing of your information
- Request restriction of processing
- Opt-out of marketing communications
- Withdraw consent at any time

How to Request: Contact office@osevra.com with details of your objection or restriction request.

9.5 Marketing Preferences

You can control marketing communications by:

- Clicking "Unsubscribe" in marketing emails
- Updating preferences in your account settings
- Contacting office@osevra.com
- Using opt-out mechanisms in your device settings

9.6 Cookie Preferences

You can control cookies by:

- Using cookie preference tools on our website
- Adjusting browser settings
- Using browser extensions to block cookies
- Opting out of analytics tracking

---

10. International Data Transfers

10.1 Cross-Border Transfers

As an APAC mainline service, we may transfer your information across APAC countries to:

- Provide services
- Maintain backup systems
- Optimize infrastructure
- Support business operations

10.2 Transfer Mechanisms

We use appropriate safeguards for international transfers:

- Standard Contractual Clauses (SCCs)
- Binding Corporate Rules (BCRs)
- Adequacy Decisions
- Your explicit consent
- Contractual protections

10.3 Data Localization

For certain jurisdictions with data localization requirements, we:

- Store data within the required country
- Comply with local data residency laws
- Maintain separate data centers where required
- Implement geographic restrictions

---

11. Children's Privacy

Our website and services are not directed to children under 13 years of age. We do not knowingly collect personal information from children under 13. If we become aware that we have collected information from a child under 13, we will delete such information and terminate the child's account.

For children 13-18 years old, we provide additional privacy protections and may require parental consent for certain processing activities.

---

12. Third-Party Links and Services

Our website may contain links to third-party websites and services that are not operated by OSEVRA. This Privacy Policy does not apply to third-party websites, and we are not responsible for their privacy practices.

We encourage you to review the privacy policies of any third-party websites before providing personal information or using their services.

---

13. Cookies and Tracking Technologies

13.1 Cookie Types

Essential Cookies: Required for website functionality, security, and user authentication. Cannot be disabled.

Performance Cookies: Used to analyze website usage and improve performance. You can disable these.

Functional Cookies: Used to remember your preferences and provide personalized features. You can disable these.

Marketing Cookies: Used for targeted advertising and marketing. You can disable these.

13.2 Cookie Management

You can manage cookies by:

- Using our cookie preference tool
- Adjusting browser settings
- Using browser extensions
- Opting out of specific cookie types

13.3 Do Not Track

Some browsers include a "Do Not Track" feature. We currently do not respond to Do Not Track signals, but you can use browser settings to disable tracking.

---

14. California Consumer Privacy Act (CCPA) Compliance

While OSEVRA is primarily an APAC service, if you are a California resident, you have the following rights under the CCPA:

- **Right to Know**: Request what personal information is collected, used, and shared
- **Right to Delete**: Request deletion of personal information
- **Right to Opt-Out**: Opt-out of sale or sharing of personal information
- **Right to Correct**: Request correction of inaccurate information

- **Right to Limit Use**: Limit use of sensitive personal information

How to Exercise Rights: Contact office@osevra.com with your request. We will respond within 45 days.

---

15. European Union GDPR Compliance

While OSEVRA is primarily an APAC service, if you are an EU resident, you have rights under the GDPR including:

- **Right of Access**: Access your personal information
- **Right to Rectification**: Correct inaccurate information
- **Right to Erasure**: Request deletion of your information
- **Right to Restrict Processing**: Limit how we process your information
- **Right to Data Portability**: Receive your information in a portable format
- **Right to Object**: Object to processing of your information
- **Right to Lodge a Complaint**: File a complaint with your data protection authority

How to Exercise Rights: Contact office@osevra.com with your request. We will respond within 30 days.

---

16. Contact Information

16.1 Privacy Officer

For privacy-related inquiries, requests, or complaints:

Email: office@osevra.com **Response Time:** 30 days (or as required by applicable law)

16.2 Data Protection Authorities

If you have concerns about our privacy practices, you can contact the relevant data protection authority in your country:

Australia:

- Office of the Australian Information Commissioner (OAIC)

- Website: https://www.oaic.gov.au/
- Email: enquiries@oaic.gov.au

New Zealand:

- Privacy Commissioner
- Website: https://www.privacy.org.nz/
- Phone: 0800 803 202

Singapore:

- Personal Data Protection Commission (PDPC)
- Website: https://www.pdpc.gov.sg/
- Email: pdpc@pdpc.gov.sg

Hong Kong:

- Office of the Privacy Commissioner for Personal Data (PCPD)
- Website: https://www.pcpd.org.hk/
- Phone: 2827 8601

Japan:

- Personal Information Protection Commission (PPC)
- Website: https://www.ppc.go.jp/

South Korea:

- Personal Information Protection Commission (PIPC)
- Website: https://www.pipc.go.kr/

Malaysia:

- Personal Data Protection Commissioner (PDPC)
- Website: https://www.pdp.gov.my/

Thailand:

- Personal Data Protection Committee (PDPC)
- Website: https://www.pdpc.mict.go.th/

Indonesia:

- Ministry of Communication and Informatics
- Website: https://www.kominfo.go.id/

Philippines:

- National Privacy Commission (NPC)
- Website: https://www.privacy.gov.ph/

Vietnam:

- Ministry of Public Security
- Website: https://www.mps.gov.vn/

---

17. Policy Updates

17.1 Changes to This Policy

We may update this Privacy Policy periodically to reflect changes in our practices, technology, legal requirements, or other factors. We will notify you of material changes by:

- Posting the updated policy on our website
- Sending you an email notification
- Requesting your consent if required by law

Effective Date of Changes: Changes become effective when posted to our website unless otherwise specified.

17.2 Your Continued Use

Your continued use of our website and services following notification of changes constitutes your acceptance of the updated Privacy Policy.

---

18. Additional Information

18.1 Sensitive Information

We do not intentionally collect sensitive personal information including:

- Health or medical information
- Biometric data
- Genetic information
- Religious or philosophical beliefs
- Political opinions
- Trade union membership
- Racial or ethnic origin
- Sexual orientation or gender identity

If you provide sensitive information, we will use it only for the purposes you specify and with appropriate safeguards.

18.2 Automated Decision-Making

We do not use automated decision-making or profiling that produces legal or similarly significant effects on you without your knowledge and consent.

18.3 Accountability

OSEVRA maintains:

- Data protection policies and procedures
- Employee training programs
- Regular privacy audits
- Incident response procedures
- Documentation of processing activities
- Records of consent and legitimate interests

---

19. Definitions

Personal Information/Personal Data: Any information relating to an identified or identifiable natural person.

Processing: Any operation performed on personal information including collection, use, storage, disclosure, or deletion.

Data Controller: The entity that determines the purposes and means of processing personal information.

Data Processor: The entity that processes personal information on behalf of the controller.

Data Subject: The individual to whom personal information relates.

Consent: Freely given, specific, informed, and unambiguous indication of agreement to processing.

Legitimate Interests: Interests pursued by the controller or third party that are necessary and proportionate to the processing.

20. Acknowledgment

By using www.osevra.com, you acknowledge that you have read, understood, and agree to this Privacy Policy. If you do not agree with any part of this policy, please do not use our website or services.

Document Version: 1.0 **Last Updated:** February 2026 **Next Review Date:** August 2026

OSEVRA Limited APAC Mainline Service Provider www.osevra.com

End of Privacy Policy