OSAAP® Online Services

Privacy Policy

Version: 2.0
Effective Date: January 24, 2026
Last Updated: January 24, 2026

Table of Contents

1. Introduction
2. Definitions
3. Personal Data We Collect
4. How We Use Your Data
5. Legal Basis for Processing
6. Data Sharing and Disclosure
7. Data Retention
8. International Data Transfers
9. Data Security
10. Your Privacy Rights
11. Cookies and Tracking
12. Children's Privacy
13. Regional Privacy Rights
14. Third-Party Services
15. Changes to This Policy
16. Contact Us

1. Introduction

OSAAP Technologies, a division of OSAAP America LLC ("OSAAP," "we," "us," or "our"), is committed to protecting your privacy and ensuring the security of your personal information. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you use our services.

Our Commitment: We believe in transparency and giving you control over your personal data. This policy is designed to comply with global privacy regulations including the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA/CPRA), Lei Geral de Protecao de Dados (LGPD), Personal Information Protection and Electronic Documents Act (PIPEDA), UK GDPR, and Australian Privacy Act.

1.1 Covered Services

This Privacy Policy applies to all OSAAP Online Services, including:

- **BlueID®** - Identity and access management platform (osaapblueid.net)
- **BlueMobile®** - Mobile applications for iOS and Android
- **OSAAP Project Portals** - Web-based project management (osaaponline.net)
- **OSAAP Converter Accounts** - Data conversion services (osaaptechnologies.net)
- **Shadowboard Online Tools** - Tool database services (shadowboard.tools)
- **BlueSupportDesk** - Customer support portal (osaaptechnologies.net)

1.2 Data Controller Information

For the purposes of applicable data protection laws, the data controller is:

OSAAP Technologies
Division of OSAAP America LLC
10 Kidder Rd, Unit 4
Chelmsford, MA 01824
United States

2. Definitions

The following terms have specific meanings throughout this Privacy Policy:

Personal Data	Any information relating to an identified or identifiable natural person, including name, email address, IP address, device identifiers, and location data.
Processing	Any operation performed on personal data, including collection, storage, use, disclosure, modification, or deletion.
Data Subject	The individual to whom personal data relates (i.e., you, the user).
Service Provider	A third party that processes personal data on our behalf to provide services.
Consent	Freely given, specific, informed, and unambiguous indication of your agreement to the processing of your personal data.
Account	A unique account created for you to access our services.
Cookies	Small data files stored on your device that help us provide and improve our services.
Device	Any device that can access our services, including computers, smartphones, and tablets.

3. Personal Data We Collect

3.1 Information You Provide Directly

We collect information you voluntarily provide when using our services:

- **Account Information:** Name, email address, phone number, postal address, username, and password
- **Profile Information:** Job title, company name, profile picture, and preferences
- **Payment Information:** Billing address, payment card details (processed securely by payment processors)
- **Communications:** Support requests, feedback, survey responses, and correspondence
- **Content:** Data you upload, create, or share through our services

3.2 Information Collected Automatically

When you access our services, we automatically collect certain information:

- **Device Information:** Device type, operating system, browser type, unique device identifiers
- **Usage Data:** Pages visited, features used, time spent, click patterns, and navigation paths
- **Network Information:** IP address, internet service provider, connection type
- **Location Data:** General geographic location based on IP address (precise location only with consent)
- **Log Data:** Access times, error logs, referring URLs, and system activity

3.3 Information from Third Parties

We may receive information from third-party sources:

- **Authentication Providers:** When you sign in using third-party services (e.g., Microsoft, Google)
- **Business Partners:** Information from partners who refer you to our services
- **Public Sources:** Publicly available information to supplement our records

Sensitive Data: We do not intentionally collect sensitive personal data such as racial or ethnic origin, political opinions, religious beliefs, health information, or biometric data unless specifically required for the service and with your explicit consent.

4. How We Use Your Data

We use your personal data for the following purposes:

4.1 Service Delivery

- Providing, maintaining, and improving our services
- Processing transactions and managing your account
- Authenticating your identity and managing access
- Delivering features and functionality you request

4.2 Communication

- Sending service-related notifications and updates
- Responding to your inquiries and support requests
- Providing security alerts and important notices
- Sending marketing communications (with your consent)

4.3 Improvement and Analytics

- Analyzing usage patterns to improve our services
- Conducting research and development
- Personalizing your experience
- Testing new features and functionality

4.4 Security and Compliance

- Detecting and preventing fraud, abuse, and security incidents
- Protecting the rights and safety of our users
- Complying with legal obligations and regulatory requirements
- Enforcing our terms of service and policies

5. Legal Basis for Processing

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

Contract Performance	Processing necessary to fulfill our contractual obligations to you	Account creation, service delivery, transaction processing
Consent	Processing based on your explicit consent	Marketing communications, optional features, cookies
Legitimate Interests	Processing necessary for our legitimate business interests	Service improvement, security, fraud prevention, analytics
Legal Obligation	Processing required to comply with applicable laws	Tax reporting, regulatory compliance, legal requests
Vital Interests	Processing necessary to protect someone's life or safety	Emergency situations, safety alerts

Withdrawing Consent: Where we rely on consent, you may withdraw it at any time by contacting us or using the opt-out mechanisms provided. Withdrawal does not affect the lawfulness of processing before withdrawal.

6. Data Sharing and Disclosure

We may share your personal data in the following circumstances:

6.1 Service Providers

We engage trusted third parties to perform services on our behalf, including:

- Cloud hosting and infrastructure providers
- Payment processors and billing services
- Email and communication services
- Analytics and performance monitoring
- Customer support platforms

All service providers are contractually bound to protect your data and use it only for specified purposes.

6.2 Business Transfers

In the event of a merger, acquisition, reorganization, or sale of assets, your personal data may be transferred. We will notify you before your data becomes subject to a different privacy policy.

6.3 Legal Requirements

We may disclose your data when required by law or to:

- Comply with legal process, court orders, or government requests
- Protect our rights, property, or safety
- Investigate potential violations of our terms
- Preventing fraud or security threats

6.4 With Your Consent

We may share your data with third parties when you have been given explicit consent for specific purposes.

Data Sales: We do not sell your personal data to third parties for monetary consideration. For CCPA purposes, certain data sharing for targeted advertising may be considered a "sale" - see Section 13 for opt-out rights.

7. Data Retention

We retain your personal data only for as long as necessary to fulfill the purposes for which it was collected:

Account Information	Duration of account + 3 years	Service delivery and legal compliance
Transaction Records	7 years from transaction	Financial and tax regulations
Usage Data	2 years	Service improvement and analytics
Support Communications	3 years from resolution	Quality assurance and dispute resolution
Marketing Preferences	Until consent withdrawn	Consent management
Security Logs	1 year	Security monitoring and incident response

After the retention period expires, data is securely deleted or anonymized for statistical purposes.

8. International Data Transfers

As a global service provider based in the United States, we may transfer your personal data to countries outside your country of residence.

8.1 Transfer Safeguards

When transferring data internationally, we implement appropriate safeguards:

- **Standard Contractual Clauses (SCCs):** EU-approved contractual terms ensuring data protection
- **Data Processing Agreements:** Binding agreements with all service providers
- **Adequacy Decisions:** Transfers to countries with adequate data protection recognized by relevant authorities
- **Technical Safeguards:** Encryption, access controls, and security measures

8.2 EU-U.S. and UK-U.S. Transfers

For transfers from the European Economic Area (EEA), United Kingdom, or Switzerland to the United States, we rely on Standard Contractual Clauses and supplementary measures to ensure adequate protection of your data.

Your Rights: You have the right to obtain a copy of the safeguards we use for international transfers by contacting us at the address provided in Section 16.

9. Data Security

We implement comprehensive security measures to protect your personal data:

9.1 Technical Measures

- **Encryption:** TLS/SSL encryption for data in transit; AES-256 encryption for data at rest
- **Access Controls:** Role-based access, multi-factor authentication, and least privilege principles
- **Network Security:** Firewalls, intrusion detection, and continuous monitoring
- **Secure Development:** Security testing, code reviews, and vulnerability assessments

9.2 Organizational Measures

- **Security Training:** Regular training for all employees handling personal data
- **Policies and Procedures:** Comprehensive information security policies
- **Vendor Management:** Security assessments of all service providers
- **Incident Response:** Documented procedures for security incident handling

9.3 Data Breach Notification

In the event of a data breach affecting your personal data, we will:

- Notify relevant supervisory authorities within required timeframes (72 hours for GDPR)
- Notify affected individuals when the breach poses high risk to their rights
- Document of the breach and remediation measures taken

Your Role: While we implement robust security measures, you also play a role in protecting your data. Please use strong passwords, enable two-factor authentication, and report any suspicious activity immediately.

10. Your Privacy Rights

You have fundamental rights regarding your personal data. These rights may vary based on your location and applicable laws.

Right to Access

Request a copy of the personal data we hold about you and information about how it is processed.

Right to Rectification

Request correction of inaccurate or incomplete personal data.

Right to Erasure

Request deletion of your personal data in certain circumstances ("right to be forgotten").

Right to Restrict Processing

Request limitation of how we use your data while concerns are addressed.

Right to Data Portability

Receive your data in a structured, machine-readable format and transfer it to another provider.

Right to Object

Object to processing based on legitimate interests, including profiling and direct marketing.

Right to Withdraw Consent

Withdraw consent at any time where processing is based on consent.

Right to Complain

Lodge a complaint with supervisory authority if you believe your rights have been violated.

10.1 Exercising Your Rights

To exercise any of these rights:

- **Account Settings:** Many rights can be exercised directly through your account settings
- **Email:** Contact us at privacy@osaaptechnologies.com
- **Mail:** Write to our Privacy Team at the address in Section 16

We will respond to verifiable requests within 30 days (or as required by applicable law). We may need to verify your identity before processing your request.

No Discrimination: We will not discriminate against you for exercising your privacy rights. You will receive equal service and pricing regardless of your privacy choices.

11. Cookies and Tracking Technologies

We use cookies and similar technologies to enhance your experience, analyze usage, and deliver targeted content.

11.1 Types of Cookies

Essential Cookies	Required for basic functionality, authentication, and security	Session or persistent
Functional Cookies	Remember your preferences and settings	Up to 1 year
Analytics Cookies	Measure and analyze how you use our services	Up to 2 years
Marketing Cookies	Delivering relevant advertisements and measuring campaign effectiveness	Up to 1 year

11.2 Managing Cookies

You can control cookies through:

- **Cookie Banner:** When first visiting our site, you can select your cookie preferences
- **Browser Settings:** Most browsers allow you to block or delete cookies
- **Opt-Out Tools:** Industry opt-out platforms for advertising cookies

11.3 Other Tracking Technologies

- **Web Beacons:** Small images that track email opens and page visits
- **Local Storage:** Browser storage for application data
- **Device Fingerprinting:** Limited use for fraud prevention only

11.4 Do Not Track

Our services do not currently respond to "Do Not Track" browser signals. However, you can use the cookie controls described above to manage tracking.

12. Children's Privacy

We take the protection of children's privacy seriously.

12.1 Age Restrictions

Our services are not intended for children under the age of:

- **16 years** in the European Economic Area (unless lower age specified by member state)
- **13 years** in the United States (COPPA compliance)
- **The applicable age of consent** in your jurisdiction

12.2 Parental Consent

Where our services are available to minors, we obtain verifiable parental consent before collecting personal information from children. Parents have the right to:

- Review their child's personal information
- Request deletion of their child's data
- Refuse further collection or use

12.3 Inadvertent Collection

If we become aware that we have collected personal data from a child without proper consent, we will take immediate steps to delete that information. Please contact us if you believe a child has provided personal data without authorization.

13. Regional Privacy Rights

Depending on your location, you may have additional privacy rights under local laws.

European Economic Area, United Kingdom, and Switzerland (GDPR/UK GDPR)

If you are in the EEA, UK, or Switzerland, you have the following additional rights:

- **Supervisory Authority:** Right to lodge a complaint with your local data protection authority
- **Automated Decision-Making:** Right not to be subject to decisions based solely on automated processing
- **Data Protection Officer:** You may contact our DPO at dpo@osaaptechnologies.com

EU Representative: For inquiries from the EU, please contact our designated representative (details available upon request).

California, USA (CCPA/CPRA)

California residents have additional rights under the California Consumer Privacy Act and California Privacy Rights Act:

- **Right to Know:** Categories and specific pieces of personal information collected
- **Right to Delete:** Request deletion of personal information
- **Right to Opt-Out:** Opt-out of the "sale" or "sharing" of personal information
- **Right to Correct:** Request correction of inaccurate personal information
- **Right to Limit Use:** Limit use of sensitive personal information
- **Non-Discrimination:** Not be discriminated against for exercising rights

Categories of Information: In the past 12 months, we have collected identifiers, commercial information, internet activity, and professional information. We may share certain categories with service providers and business partners.

To opt-out of sales/sharing: Contact us at privacy@osaaptechnologies.com with subject "Do Not Sell My Personal Information"

Brazil (LGPD)

If you are in Brazil, the Lei Geral de Protecao de Dados provides you with rights including:

- Confirmation of the existence of processing
- Access to your data
- Correction of incomplete, inaccurate, or outdated data
- Anonymization, blocking, or deleting unnecessary data
- Data portability
- Information about sharing with third parties
- Revocation of consent

Canada (PIPEDA)

Canadian residents have rights under the Personal Information Protection and Electronic Documents Act:

- Access to personal information held about you
- Challenge the accuracy and completeness of information
- Withdraw consent to collection, use, or disclosure
- Complain to the Privacy Commissioner of Canada

Australia (Privacy Act)

Australian residents have rights under the Privacy Act 1988 and Australian Privacy Principles:

- Access to personal information we hold about you
- Correction of personal information
- Complain about privacy breaches to the Office of the Australian Information Commissioner
- Opt-out of direct marketing communications

Australian users may contact us if they believe their data has been transferred overseas without appropriate protections.

Other U.S. State Privacy Laws

Residents of Virginia, Colorado, Connecticut, Utah, and other states with comprehensive privacy laws have rights like California residents, including access, deletion, correction, portability, and opt-out rights. Contact us to exercise your rights under applicable state law.

14. Third-Party Services

Our services may integrate with or link to third-party services.

14.1 Third-Party Links

Our services may contain links to websites, applications, or services not operated by us. We are not responsible for the privacy practices of these third parties. We encourage you to review their privacy policies.

14.2 Third-Party Integrations

We use the following categories of third-party services:

- **Analytics:** Google Analytics, Microsoft Application Insights
- **Email Services:** Mailchimp for marketing communications
- **Payment Processing:** Secure payment processors for transactions
- **Advertising:** Google Ads for remarketing (with consent)
- **Cloud Infrastructure:** Microsoft Azure for hosting and storage

14.3 Social Media

If you interact with social media features on our services, those platforms may collect information about your visit. Refer to each platform's privacy policy for details.

15. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or for other operational reasons.

15.1 Notification of Changes

When we make material changes, we will:

- Update the "Last Updated" date at the top of this policy
- Post a prominent notice on our services
- Send email notification to registered users (for significant changes)
- Obtain consent where required by law

15.2 Review

We encourage you to review this policy periodically. Your continued use of our services after changes take effect constitutes acceptance of the revised policy.

16. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us:

privacy@osaaptechnologies.com

support@osaaptechnologies.com

We aim to respond to all privacy-related inquiries within 30 days. For complex requests, we may need additional time but will keep you informed of progress.

OSAAP® Online Services Privacy Policy

Version 2.0 | Effective January 24, 2026

© 2026 OSAAP America LLC. All rights reserved.

Trademark Notice: OSAAP®, BlueID®, and BlueMobile® are registered trademarks of OSAAP America LLC in the United States and other countries. All other trademarks are the property of their respective owners.