Privacy Policy - Oxygen AI Positron Service

Introduction

Last Updated: January 26, 2026

Welcome to Oxygen AI Positron. This Privacy Policy explains how Syncro Soft SRL ("Syncro Soft," "we," "us," or "our") collects, uses, processes, and protects your personal information when you use the Oxygen AI Positron Service (the "Service").

We are committed to protecting your privacy and being transparent about our data practices. This Privacy Policy applies to all users of the AI Positron Service, whether you are an individual user or part of an Organization.

Understanding Our Service Architecture: The Oxygen AI Positron Service is an API-based infrastructure that enables Client Applications (such as Oxygen XML Editor plugins) to access Large Language Model (LLM) providers. Understanding this architecture is essential to understanding our data practices:

- We operate an API gateway: We authenticate requests, validate credits, and route queries to LLM Providers you select
- We do NOT provide a direct user interface for AI interactions: You interact with AI through Client Applications
- We process two fundamentally different categories of data: Account and Billing Data (which we store) and API Request Data (which we transmit without storing)

Key Privacy Principles:

- Minimal Data Collection: We collect only the data necessary to provide the Service
- No Storage of API Request Content: We do not store, log, or retain the content of your AI queries or responses
- Transparency: We clearly explain what data we process and why
- User Control: You have meaningful control over your data and can exercise your rights
- Security: We implement robust security measures to protect data we store

Important Documents: This Privacy Policy should be read together with:

- Our Terms of Service (governing your use of the Service)
- Our Data Processing Agreement (governing personal data processing for business customers in applicable jurisdictions)
- Our Organization Owner Supplemental Terms (if you create an Organization)

In case of any conflict, the Data Processing Agreement takes precedence for data protection matters.

This Privacy Policy does NOT cover:

- How client applications (such as Oxygen AI Positron plugin) process your data locally
- What data client applications choose to include in API requests
- Whether client applications store queries or responses locally

Each client application that integrates with AI Positron Service has its own privacy policy covering its data practices. You should review the client application's Privacy Policy for how that application processes your data and uses AI Positron Service. Where Syncro Soft provides both AI Positron Service and the client application (such as an Oxygen AI Positron plugin), we publish separate privacy policies for each plugin because they process data in different ways and for different purposes.

By using the Service, you consent to the data practices described in this Privacy Policy. If you do not agree with this Privacy Policy, please do not use the Service.

2. Information We Collect

We collect different types of information depending on how you interact with the Service. It's critical to understand the distinction between data we store and data that merely passes through our infrastructure.

2.1 Account Information

When you create an account with AI Positron, you authenticate using either your Google account or your GitHub account. Through this OAuth authentication process, we collect:

- Full name/username as provided in your account
- Email address associated with your account
- Google/Github account unique identifier
- Account Metadata (Account creation date, status, user identifier)

We do not have access to your Google or GitHub passwords. Authentication is handled securely by Google or GitHub, and we receive only the information listed above after you authorize the connection.

2.2 Organization and Team Information (if applicable)

If you create or join an Organization (also called a "Team" in the Service interface) or are invited to join one, we additionally collect and store:

- For Organization Owners:
    - Organization name and settings
    - Names and email addresses of confirmed Organization Members
    - Information about individuals who have accessed invitation links but have not yet been confirmed (name, email, request timestamp)
    - Generic invitation links you generate and their status
- For Organization Members:
    - Organization Membership Status (which Organizations you belong to)

    - Membership Dates (when you joined and (if applicable) when you were removed)
    - Your role within the Organization (currently just "Member," but may expand)

2.3 API Credentials and Authentication

- API Keys and Tokens: Authentication credentials that Client Applications use to make API requests on your behalf
- Session Information: Information about your active sessions in the account portal
- Authentication Logs: Records of login attempts, successful logins, and logout events (retained for 90 days for security purposes)

2.4 API Usage Metadata

We collect and store metadata about your API usage for billing, service monitoring, and support purposes:

- Request Count: Number of API requests made during each period
- Timestamp: When each request occurred
- User Identifier: Which account made the request
- Organization Identifier: Which Organization the request was associated with (if applicable)
- LLM Provider Selected: Which LLM Provider you selected for each request
- Client Application Identifier: Which Client Application made the request
- Request Size in Bytes: Size of the request payload (NOT the content)
- Response Size in Bytes: Size of the response payload (NOT the content)
- Latency: How long the request took to process
- Status Code: Whether the request succeeded or failed
- Error Codes: If the request failed, what type of error occurred
- Credits Consumed: How many credits were consumed by the request

Important: This metadata does not include or reveal the actual content of your API requests or responses. We collect sizes and counts, not content.API Request Metadata is retained for 90 days for billing verification and troubleshooting, after which detailed metadata is deleted. We retain only aggregated, anonymized statistics after 90 days.

2.5 Information We Receive About Client Applications

When a client application connects to AI Positron Service on your behalf, we receive:

- Application name and version (e.g., "Oxygen XML Editor 26.0 with AI Positron Plugin 1.2")
- Operating system and basic device information (for compatibility and troubleshooting)
- Your account authentication tokens (to verify you have an active account and sufficient credits) -
- Your default LLM provider selection (if configured)

2.5 Billing and Payment Information

For paid subscriptions, we collect:

- Payment method information
- Billing address
- Transaction history and invoice information
- Tax identification numbers (if required by applicable tax laws)

Payment processing is handled by third-party payment processors who act as data processors on our behalf. We do not directly store credit card numbers on our servers. Our payment processors store this information securely and in compliance with PCI-DSS standards.

2.6 Technical and Usage Information

Like most online services, we automatically collect certain technical information when you use the Service: IP address, date and time of access, session duration. This information is collected through server logs, cookies, and similar technologies.

2.6 Communications

If you contact us through email, support tickets, or other communication channels, we collect:

- Your email address and name
- Content of your communications with us
- Any attachments or additional information you provide
- Records of our responses to you

2.7 Information We Do NOT Collect

To be absolutely clear about our data practices, we do NOT collect, store, or process:

- Query Content: The text, prompts, questions, or other content you submit to AI language models
- LLM Responses: The outputs, answers, or content generated by AI language models in response to your queries
- Personal Data from Queries: Any personal data that may appear in your queries or in LLM responses
- Precise Geolocation: We do not track your physical location beyond general location derived from IP address
- Special Categories of Personal Data: We do not intentionally collect sensitive personal data such as racial or ethnic origin, political opinions, religious beliefs, health data, sexual orientation, genetic data, or biometric data

3. How We Use Your Information

3.1 Account Information

We use your account information (name and email from OAuth) to:

- Create and maintain your user account

- Authenticate you when you log in to the Service
- Display your name within the Service interface
- Communicate with you about your account
- Provide customer support
- Comply with legal obligations

Legal Basis (for EEA/UK/Swiss users): Performance of contract (providing the Service to you) and legitimate interests (maintaining security and providing support).

3.2 Organization Information

We use Organization information to:

- Enable Organization Owners to create and manage Organizations
- Process invitation requests and manage Organization membership
- Facilitate centralized billing for Organization subscriptions
- Display Organization membership information to Organization Owners and Members
- Notify Organization Owners and Members of membership changes

Legal Basis (for EEA/UK/Swiss users): Performance of contract (providing Organization features) and legitimate interests (managing customer relationships).

3.3 Billing Information

We use billing and payment information to:

- Process subscription payments
- Generate invoices and receipts
- Manage subscription renewals and cancellations
- Prevent fraud and unauthorized transactions
- Comply with tax and accounting obligations

Legal Basis (for EEA/UK/Swiss users): Performance of contract (processing payments), legal obligations (tax and accounting requirements), and legitimate interests (fraud prevention).

3.4 API Request Metadata

We use query metadata (not query content) to:

- Calculate and charge credits based on usage
- Monitor Service performance and availability
- Identify and troubleshoot technical issues
- Generate aggregate usage statistics for Service improvement
- Prevent abuse and enforce usage limits

Legal Basis (for EEA/UK/Swiss users): Performance of contract (providing and billing for the Service) and legitimate interests (maintaining Service quality and preventing abuse).

3.5 Technical and Usage Information

We use technical and usage information to:

- Maintain and improve the Service
- Diagnose technical problems
- Analyze usage patterns to enhance user experience
- Monitor Service security and detect potential threats
- Generate aggregate analytics about Service usage

Legal Basis (for EEA/UK/Swiss users): Legitimate interests (maintaining and improving the Service, ensuring security).

3.6 Communications

We use communications data to:

- Respond to your inquiries and requests
- Provide customer support
- Investigate and resolve complaints
- Maintain records of our interactions with you

Legal Basis (for EEA/UK/Swiss users): Legitimate interests (providing customer support) and legal obligations (record-keeping requirements).

3.7 Purposes We Do NOT Use Your Information For

We do NOT use your information for:

- Training AI Models: We do not use your queries, LLM responses, or any other user content to train AI models, whether our own or third parties'
- Marketing to Third Parties: We do not sell or rent your personal information to third parties for their marketing purposes
- Profiling or Targeted Advertising: We do not create detailed profiles about you or serve targeted advertisements based on your Service usage
- Secondary Analysis: We do not analyze query content or LLM responses for any purpose beyond transmitting them between you and the LLM provider
- Cross-Context Behavioral Advertising: We do not track your behavior across different websites or services for advertising purposes

4. How We Share Your Information

4.1 Third-Party Service Providers (Data Processors)

We share your information with third-party service providers who process data on our behalf to help us operate the Service. A complete list of data processors is available in our Data Processing Agreement, which can be requested by contacting privacy@oxygenxml.com.

4.2 Third-Party LLM Providers (Independent Controllers)

The API Request Flow. When you use AI features in a client application:

- Client Application → AI Positron Service API: The client application sends an API request containing:
    - Your authentication token
    - The query content (generated by the application based on your actions)
    - Selected LLM provider
    - Request parameters
- AI Positron Service → LLM Provider: AI Positron Service validates your authentication and credits, then forwards the query to the selected LLM Provider's API
- LLM Provider → AI Positron Service: The LLM Provider processes the query and returns a response
- AI Positron Service → Client Application: AI Positron Service forwards the response back to the client application
- Client Application → You: The client application displays the response in its interface

At no point in this flow does AI Positron Service store query content or responses. We act purely as an authenticated routing layer.

LLM Providers Are Independent Controllers. The LLM providers are independent data controllers who process your queries according to their own privacy policies and terms of service. When a client application sends a query through AI Positron Service to an LLM Provider:

- The LLM Provider receives the query content
- The LLM Provider processes the query using its AI models
- The LLM Provider may store, log, or use the query according to its own policies
- AI Positron Service does NOT control, cannot verify, and is NOT responsible for how LLM Providers process your data

Your Responsibility: You are responsible for:

- Reviewing each LLM provider's privacy policy before using that provider
- Understanding how each provider processes your queries
- Ensuring you have legal authority to send any personal data to the LLM provider
- Complying with applicable data protection laws when using LLM providers

Our Role: We act only as a technical intermediary. We:

- Do NOT control how LLM providers process your queries
- Are NOT responsible for LLM provider data practices
- Do NOT store your queries or their responses

4.3 Organization Owners

If you are a member of an Organization, the Organization Owner can see:

- Your name and email address
- Your membership status in the Organization
- The date you joined the Organization
- Basic usage metadata (such as whether you are actively using the Service)

Organization Owners cannot see:

- The content of your queries to LLM providers
- The responses you receive from LLM providers
- Detailed usage information beyond aggregate statistics

4.4 Legal Requirements and Protection of Rights

We may disclose your information if required to do so by law or if we believe in good faith that such disclosure is necessary to:

- Comply with legal obligations, court orders, or legal processes
- Respond to lawful requests from government authorities
- Enforce our Terms of Service or other agreements
- Protect the rights, property, or safety of Syncro Soft, our users, or the public
- Detect, prevent, or address fraud, security, or technical issues
- Protect against legal liability

When we disclose information for legal reasons, we will:

- Limit disclosure to what is legally required
- Notify affected users when permitted by law
- Challenge overly broad or inappropriate requests when possible

4.5 Business Transfers

If Syncro Soft is involved in a merger, acquisition, asset sale, bankruptcy, or other business transaction, your information may be transferred to the acquiring entity. We will:

- Notify you via email and/or prominent notice on our website before your information is transferred
- Ensure the acquiring entity agrees to protect your information according to this Privacy Policy or provide you with the option to delete your account before transfer

5. Data Retention

5.1 Account Information We retain your account information (name, email, avatar image, OAuth identifiers) for as long as your account is active or as needed to provide you with the Service. If you delete your account, we will delete your account information within 30 days, except as described in Section 5.5 below.

5.2 Organization Information For Organization Owners, we retain Organization information for as long as the Organization exists. When an Organization is deleted, we delete Organization information within 30 days, except as described in Section 5.5 below. For Organization Members who are removed from an Organization or who request deletion of their data, we delete their Organization membership information within 30 days.

5.3 Billing Information We retain billing and payment information for as long as required by law, typically 7 years for tax and accounting purposes. This includes: transaction records,

invoices, payment method information and billing addresses. After the legally required retention period, we securely delete billing information.

5.4 API Request Metadata We retain API request metadata (timestamps, selected providers, usage statistics) for 90 days for billing verification and technical troubleshooting purposes. After 90 days, we delete detailed metadata and retain only aggregated, anonymized statistics.

5.5 Legal and Compliance Requirements We may retain information beyond the periods described above if:

- Required by applicable law or regulation
- Necessary to resolve disputes or enforce our agreements
- Necessary to establish, exercise, or defend legal claims
- Necessary to protect the rights, property, or safety of Syncro Soft or others

In these cases, we retain only the specific information necessary for the stated purpose and delete it once the purpose is fulfilled.

5.6 Backup Systems. Account and billing information deleted from our active systems may persist in backup systems for up to 90 days. Backups are encrypted and are not accessible for normal operations. After 90 days, information is permanently deleted from all backups.

5.7 What We Do NOT Retain We do NOT retain:

- Query content: Queries you send to LLM providers are transmitted in real-time and are not stored in any system, including backups
- LLM responses: Responses from LLM providers are transmitted to you in real-time and are not stored
- Detailed logs of queries: System logs that might capture transient data are automatically deleted after 7 days maximum

6. Data Security

6.1 Technical Security Measures

We implement industry-standard security measures to protect your information, including:

Encryption:

- All data transmitted between your device and our servers is encrypted using TLS 1.2 or higher
- All data transmitted between our servers and LLM providers is encrypted using TLS 1.2 or higher
- Account and billing information stored in databases is encrypted at rest using AES-256 encryption
- Encryption keys are stored separately from encrypted data and are managed through secure key management systems

Access Controls:

- Role-based access control (RBAC) limits employee access to personal data based on job function
- Multi-factor authentication required for all administrative access to production systems
- Automatic session timeout for inactive sessions
- Regular review and audit of access permissions

Network Security:

- Firewalls and intrusion detection/prevention systems protect our infrastructure
- Network segmentation isolates production systems from development and corporate networks
- Regular security patching and updates
- DDoS protection and rate limiting

Application Security:

- Regular security code reviews
- Automated security scanning of code and dependencies
- Penetration testing by independent security firms
- Secure software development lifecycle practices

6.2 Organizational Security Measures

Employee Training and Policies:

- All employees with access to personal data receive data protection and security training
- Confidentiality agreements signed by all employees and contractors
- Clear security policies and procedures
- Background checks conducted on employees with access to personal data (where permitted by law)

Incident Response:

- 24/7 security monitoring for critical systems
- Documented incident response plan
- Procedures for containing and remediating security incidents
- Notification procedures for affected users and authorities as required by law

Vendor Management:

- Security assessments of third-party service providers before engagement
- Contractual requirements for vendors to implement appropriate security measures
- Regular review of vendor security practices

6.3 Limitations of Security

While we implement strong security measures, no system is 100% secure. We cannot guarantee absolute security of your information. You are responsible for:

- Keeping your OAuth credentials (Google or GitHub login) secure
- Not sharing your account access with others
- Using strong passwords for your OAuth accounts
- Promptly notifying us if you suspect unauthorized access to your account

If you become aware of any security breach or unauthorized access, please immediately contact us at security@oxygenxml.com.

7. Your Rights and Choices

7.1 Rights Under GDPR (EEA/UK Users) If you are located in the European Economic Area or United Kingdom, you have the following rights under GDPR and UK DPA:

- Right of Access: You have the right to request a copy of the personal data we hold about you. We will provide this information within 30 days of your request.
- Right to Rectification: If your personal data is inaccurate or incomplete, you have the right to request that we correct or complete it. You can update most of your account information directly through the Service interface.
- Right to Erasure ("Right to be Forgotten"): You have the right to request deletion of your personal data in certain circumstances, including the data is no longer necessary for the purposes for which it was collected, you object to processing based on legitimate interests and there are no overriding legitimate grounds, the data has been unlawfully processed, deletion is required to comply with legal obligations.
- Right to Restriction of Processing: You have the right to request that we restrict processing of your personal data in certain circumstances, such as when you contest the accuracy of the data or object to processing.
- Right to Data Portability: You have the right to receive your personal data in a structured, commonly used, and machine-readable format (such as JSON or XML) and to transmit that data to another service provider.
- Right to Object: You have the right to object to processing of your personal data based on legitimate interests. If you object, we will stop processing unless we can demonstrate compelling legitimate grounds that override your interests.
- Right Not to Be Subject to Automated Decision-Making: We do not use automated decision-making or profiling that produces legal effects or similarly significantly affects you.
- Right to Withdraw Consent: Where processing is based on consent, you have the right to withdraw consent at any time. This will not affect the lawfulness of processing based on consent before withdrawal.
- Right to Lodge a Complaint: You have the right to lodge a complaint with a supervisory authority if you believe our processing of your personal data violates data protection law.

7.2 Rights Under CCPA (California Users) If you are a California resident, you have the following rights under the California Consumer Privacy Act (CCPA):

- Right to Know: You have the right to request that we disclose:
    - Categories of personal information we collected about you
    - Categories of sources from which the personal information was collected
    - Business or commercial purpose for collecting or selling personal information

    - Categories of third parties with whom we share personal information
    - Specific pieces of personal information we collected about you
- Right to Delete: You have the right to request deletion of personal information we collected from you, subject to certain exceptions.
- Right to Correct: You have the right to request correction of inaccurate personal information we maintain about you.
- Right to Opt-Out of Sale or Sharing: We do not sell or share your personal information as defined by CCPA. If our practices change, we will update this Privacy Policy and provide you with the right to opt out.
- Right to Limit Use of Sensitive Personal Information: We do not use sensitive personal information in ways that would trigger this right under CCPA.
- Right to Non-Discrimination: We will not discriminate against you for exercising any of your CCPA rights.

7.3 Rights Under Other U.S. State Privacy Laws If you are a resident of Virginia, Colorado, Connecticut, or Utah, you have similar rights under your state's privacy law, including rights to access, correct, delete, and obtain a copy of your personal data, and to opt out of certain processing activities.

7.4 How to Exercise Your Rights

To exercise any of the rights described above, you can:

- Email us: privacy@oxygenxml.com
- Use account settings: Many rights can be exercised directly through your account settings in the Service interface (such as updating your information or deleting your account)
- Contact support: support@oxygenxml.com

When you submit a request, we will:

- Verify your identity to protect your privacy and security
- Respond within the legally required timeframe (typically 30 days for GDPR, 45 days for CCPA)
- Provide the requested information or action free of charge (in most cases)
- Explain if we cannot comply with your request and the reasons why

Verification Process: To verify your identity, we may request:

- Confirmation of your email address through a verification link
- Information matching what we have on file for your account
- Additional information if needed for security purposes

Authorized Agents: For California residents, you may designate an authorized agent to make requests on your behalf. We require written authorization from you confirming the agent's authority.

7.5 Account Deletion

You can delete your account at any time by:

- Emailing support@oxygenxml.com from your registered email address
- Using the account deletion feature in the Service interface (if available)

When you delete your account:

- Your account information will be deleted within 30 days
- If you are an Organization Owner, your Organization will also be deleted, and all Organization Members will be removed
- If you are an Organization Member, you will be removed from any Organizations you belong to
- Billing information will be retained for the legally required period (typically 7 years)
- Backups containing your information will be deleted within 90 days

8. International Data Transfers

8.1 Data Transfer Mechanisms

Syncro Soft is located in Romania (European Economic Area). However, some of our service providers and the LLM providers you choose to use are located outside the EEA, including in the United States.

When we transfer personal data from the EEA, UK, or Switzerland to countries outside these jurisdictions, we ensure appropriate safeguards are in place:

- For transfers to the United States:
  - EU-U.S. Data Privacy Framework: For service providers certified under the EU-U.S. Data Privacy Framework, we rely on their certification as an adequacy mechanism
  - Standard Contractual Clauses (SCCs): For other U.S.-based service providers, we use Standard Contractual Clauses approved by the European Commission
  - UK Addendum: For transfers subject to UK law, we use the UK Addendum to the Standard Contractual Clauses
- For transfers to other countries:
  - We rely on adequacy decisions from the European Commission where available
  - Where no adequacy decision exists, we use Standard Contractual Clauses

8.2 Your Choices Regarding LLM Provider Transfers

When you select an LLM provider through our Service, your query data will be transmitted to that provider's infrastructure, which may be located in various countries including the United States. By selecting a specific LLM provider and submitting a query, you are explicitly instructing us to transmit your data to that provider's jurisdiction.

We provide information about each LLM provider's location and data protection certifications within the Service interface and in our Data Processing Agreement. You are responsible for:

- Reviewing this information before using each LLM provider

- Ensuring that such transfers comply with applicable laws in your jurisdiction
- Selecting LLM providers whose data processing locations are acceptable for your use case

8.3 Safeguards for International Transfers

In addition to legal transfer mechanisms, we implement supplementary technical and organizational measures for international transfers:

- End-to-end encryption during data transmission
- Encryption at rest for data stored outside the EEA
- Strict access controls limiting who can access transferred data
- Regular assessments of the legal framework in destination countries

9. Children's Privacy

The Oxygen AI Positron Service is not intended for children under the age of 18. We do not knowingly collect personal information from children under 18. By using the Service, you represent that you are at least 18 years old, or if you are under 18, that you have the permission and supervision of a parent or legal guardian.

If we become aware that we have inadvertently collected personal information from a child under 18 without proper parental consent, we will take steps to delete that information as quickly as possible.

If you believe we may have collected information from a child under 18, please contact us immediately at privacy@oxygenxml.com.

10. Cookies and Tracking Technologies

10.1 Types of Cookies We Use

We use cookies and similar tracking technologies to provide and improve the Service. A cookie is a small text file that is stored on your device when you visit our website.

Essential Cookies (Required):

- Authentication cookies that remember you are logged in
- Session cookies that maintain your session state
- Security cookies that help protect against fraud and abuse

These cookies are necessary for the Service to function and cannot be disabled.

Analytics Cookies (Optional):

- Usage analytics to understand how users interact with the Service
- Performance monitoring to identify technical issues
- Aggregate statistics about Service usage

These cookies help us improve the Service but are not essential for basic functionality.

10.2 Cookie Management

You can control cookies through your browser settings. Most browsers allow you to:

- View and delete cookies
- Block cookies from specific websites
- Block all cookies
- Receive warnings before cookies are set

10.3 Do Not Track Signals

Some browsers transmit "Do Not Track" (DNT) signals. Currently, there is no industry consensus on how to respond to DNT signals. We do not currently respond to DNT signals, but we do not engage in cross-site tracking or targeted advertising that DNT is intended to prevent.

11. Third-Party Links and Services

The Service may contain links to third-party websites, services, or resources that are not operated by us. This Privacy Policy does not apply to third-party websites or services.

When you click on a third-party link or use a third-party service (including LLM providers), you leave our Service and are subject to the third party's privacy policy and terms of service. We encourage you to read the privacy policies of any third-party services you use.

We are not responsible for:

- The privacy practices of third-party websites or services
- The content or functionality of third-party services
- Data breaches or security incidents at third-party services
- Any harm or damages resulting from your use of third-party services

12. Data Controllers and Processors

12.1 Syncro Soft as Data Controller For personal data we collect directly from you (such as account information obtained through OAuth), Syncro Soft SRL acts as the data controller. We determine the purposes and means of processing this data.

12.2 Syncro Soft as Data Processor. For Organization accounts, the Organization (through the Organization Owner) acts as the data controller for Organization Member personal data, and Syncro Soft acts as a data processor. We process Organization Member data only according to the Organization Owner's instructions and as described in our Data Processing Agreement.

12.3 LLM Providers as Independent Controllers LLM providers (such as OpenAI, Anthropic, and Google) are independent data controllers for query data you send to them

through our Service. We do not control and are not responsible for how they process your queries. Each LLM provider processes queries according to its own privacy policy.

12.4 Representative in the EU As Syncro Soft SRL is established in Romania (an EU member state), we do not need to appoint an EU representative under Article 27 of the GDPR.

13. 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 other factors. When we make material changes, we will notify you by:

- Posting the updated policy on our website with a new "Last Updated" date
- Sending an email notification to the email address associated with your account
- Displaying a prominent notice on the Service

Material changes may include:

- Changes to the types of personal information we collect
- Changes to how we use or share personal information
- Changes to your rights or how to exercise them
- Changes to our data retention practices
- Changes to our legal basis for processing

We encourage you to review this Privacy Policy periodically. Your continued use of the Platform after changes become effective constitutes your acceptance of the revised Privacy Policy.

14. Contact Us

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

- **Email**:
  - General privacy inquiries: privacy@oxygenxml.com
  - Security concerns: security@oxygenxml.com
  - General support: support@oxygenxml.com
- **Mail**:

  Syncro Soft SRL

  Attention: Data Protection / Privacy

  Remus 5A, Craiova, 200082, Romania

- **Response Time**: We aim to respond to all privacy inquiries within 5 business days. For data subject rights requests under GDPR or CCPA, we will respond within the legally required timeframe (typically 30-45 days).

- **Supervisory Authority (for EEA users)**: If you are not satisfied with our response to your privacy concerns, you have the right to lodge a complaint with your local supervisory authority.