DATA PROCESSING ADDENDUM - Oxygen AI Positron Service

Effective Date: February 9, 2026

This Data Processing Addendum ("DPA") forms part of the Service Agreement (the "Agreement") between:

CUSTOMER (the "Data Controller" or "Controller" or "Customer")

and

SYNCRO SOFT SRL, a company registered in Romania with registration number RO10639959 having its registered office at Remus 5A, Craiova, 20082, Romania (the "Data Processor" or "Processor" or "Syncro Soft")

(each a "Party" and together the "Parties")

WHEREAS:

- A. Customer acts as a Data Controller and has engaged Syncro Soft to provide the Oxygen AI Positron Service ("Service") pursuant to the Agreement;
- B. The Service is an API-based backend service that enables client applications (primarily Oxygen family dedicated plugins) to access multiple Large Language Model providers through an authenticated interface;
- C. In the course of providing the Service, Syncro Soft will Process certain Personal Data on behalf of and in accordance with Customer's documented instructions;
- D. The Service also transmits query data from client applications to third-party LLM Providers selected by users, acting as a technical intermediary without storing or retaining query content;
- E. The parties wish to ensure such Processing is conducted in accordance with applicable Data Protection Laws, in particular the General Data Protection Regulation (EU) 2016/679 ("GDPR");
- F. This DPA sets forth the terms and conditions that govern such Processing and the parties' respective obligations.

NOW, THEREFORE, in consideration of the mutual covenants and agreements herein contained, the parties agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions

Unless otherwise defined in this DPA, capitalized terms have the meanings assigned to them in the Service Agreement. The following additional definitions apply:

- "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party, where "control" means ownership of at least 50% of the voting rights or equity interests.
- "Client Application" means any software application that integrates with the Service via API to provide AI functionality to end users, including but not limited to Oxygen AI Positron for Desktop plugin, Oxygen AI Positron for Content Fusion plugin, and other authorized Oxygen AI Positron family plugins.
- "Controller" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- "Data Protection Laws" means all applicable laws and regulations relating to privacy, data protection, and data security, including but not limited to: Regulation (EU) 2016/679 (General Data Protection Regulation or "GDPR"); EU GDPR as saved into UK law by virtue of section 3 of the UK's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 (together, "UK Data Protection Law"); Swiss Federal Data Protection Act of 25 September 2020 and its corresponding ordinances; California Consumer Privacy Act of 2018 California Civil Code § 1798.100 et seq., as amended by the California Privacy Rights Act of 2020, including any implementing regulations ("CCPA"); the ePrivacy Directive (2002/58/EC) as amended; any successor or replacement legislation; and any other applicable national or international privacy or data protection laws.
- "U.S. Privacy Laws" means the subset of Data Protection Laws applicable to residents of the United States, including without limitation the CCPA.
- "Data Privacy Frameworks" or "DPF" means (as applicable) the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and Swiss-U.S. Data Privacy Framework self-certification programs operated by the U.S. Department of Commerce and any respective successors.
- "UK Addendum" means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioner's Office under s. 119A(1) of the UK Data Protection Act 2018, as it is revised under s. 18 therein, as may be amended or superseded from time to time.
- "Data Subject" means an identified or identifiable natural person whose Personal Data is processed. For purposes of this DPA, Data Subjects include Service users, Organization Owners, Organization Members, and any other individuals whose Personal Data may appear in API Request Data.

- "EEA" means the European Economic Area, comprising the EU member states plus Iceland, Liechtenstein, and Norway.
- "International Transfer" means a transfer of Personal Data from the EEA to a country outside the EEA that has not received an adequacy decision from the European Commission.
- "LLM Provider" means a third-party provider of Large Language Model services that users can access through the Service, including but not limited to providers such as OpenAI, Anthropic, Google, and others as listed in Annex III.
- "OAuth Provider" means third-party authentication service providers (currently Google and GitHub) that facilitate user authentication and from which initial user account data is obtained.
- "Organization" or "Team" means a billing entity created by a user (the Organization Owner) that allows grouping of multiple users under a single payment relationship, where the Organization Owner pays for API usage credits consumed by all confirmed members. This structure does not involve content sharing or document collaboration between members but exists exclusively for centralized billing administration.
- "Organization Owner" or "Administrator" means the user who creates an Organization and has administrative rights to invite members, confirm membership requests, and manage billing for all Organization members.
- "Organization Member" or "Team Member" means a user invited by an Organization Owner to join an Organization through a generic invitation link, whose membership becomes active only after explicit confirmation by the Organization Owner. Members benefit from API usage credits paid for by the Organization Owner but operate independently without shared workspaces or content.
- "Pending Membership Request" means a request to join an Organization generated when a person accesses a generic invitation link, which remains pending until the Organization Owner either confirms or rejects the request.
- "Personal Data" means any information relating to an identified or identifiable natural person, as defined in Article 4(1) of the GDPR. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.
- "Personal Information" has the meaning assigned to it in the CCPA and applies solely where Customer qualifies as a "Business" and Syncro Soft processes such information as a "Service Provider" under the CCPA. For clarity, Personal Information may include categories of information that are not considered Personal Data under the GDPR, and obligations under this Agreement apply to each term only within the scope of its respective legislation.

- "Account and Billing Data" means Personal Data that Syncro Soft stores persistently in connection with the Service, including user account information (full name and email address obtained through OAuth authentication), Organization membership information, API access credentials, billing and payment data, and user roles within Organizations.
- "API Request Data" means the data transmitted in API requests from Client Applications to the Service and then to selected LLM Providers, which may incidentally contain Personal Data. API Request Data is transmitted in real-time and is not stored, logged, cached, or retained by Syncro Soft beyond transient processing in server memory during the routing operation.
- "API Request Metadata" means non-content information about API requests that Syncro Soft collects for billing, service monitoring, and technical support, including timestamps, user identifiers, selected LLM Provider, request and response sizes in bytes (but not content), status codes, credits consumed, and Client Application identifiers. API Request Metadata does not include or reveal the content of API requests or responses.
- "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed, as defined in Article 4(12) of the GDPR.
- "Processor" means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller. For purposes of Account and Billing Data processed under this DPA, Syncro Soft is the Processor.
- "Processing" or "Process" means any operation or set of operations performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction, as defined in Article 4(2) of the GDPR.
- "Security Incident" means any actual or reasonably suspected Personal Data Breach or any other actual or reasonably suspected breach of Syncro Soft's security obligations under this DPA.
- "Standard Contractual Clauses" or "SCCs" means the standard data protection clauses for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection, as approved by the European Commission pursuant to Decision 2021/914 dated 4 June 2021, or any subsequent version thereof.
- "Sub-processor" means any entity engaged by Syncro Soft to process Account and Billing Data on behalf of Customer in connection with the Service. This term specifically refers to entities that process the Personal Data that Syncro Soft stores and controls, and does not include LLM Providers (which are independent controllers for API Request Data) or

Client Application providers (which are independent controllers for processing within their applications).

- "Supervisory Authority" means an independent public authority established by an EU member state pursuant to GDPR Article 51, or any equivalent authority under other applicable Data Protection Laws.

1.2 Interpretation

In this DPA, unless the context otherwise requires: references to "including" shall mean "including without limitation"; references to "Section" or "Annex" are references to sections of or annexes to this DPA; references to "writing" or "written" include email and other electronic communications; words in the singular shall include the plural and vice versa; headings are for convenience only and shall not affect the interpretation of this DPA; the terms "herein," "hereof," and "hereunder" refer to this DPA as a whole.

The annexes form an integral part of this DPA.

2. ROLES AND SCOPE OF PROCESSING

2.1 Service Architecture and Access Model

2.1.1 Nature of the Service

The Oxygen AI Positron Service is an API-based backend service designed to enable Client Applications to access multiple LLM Providers through a unified, authenticated interface. The Service architecture consists of:

- Account Management Portal: A web interface at https://aipositron.oxygenxml.com/ where users create accounts via OAuth, manage subscriptions, purchase credit packages, configure preferences, and view API usage statistics.
- API Backend Infrastructure: Server infrastructure that authenticates API requests from Client Applications, validates user credentials and credit availability, routes API requests to selected LLM Providers, receives responses from LLM Providers, and returns responses to requesting Client Applications.
- No Direct End-User Interface for Queries: The Service does NOT provide a direct chat interface or query submission interface for end users. Users interact with AI functionality exclusively through Client Applications that integrate with the Service via API.

2.1.2 Access Through Client Applications Only

The functional AI capabilities provided by the Service are accessed exclusively through Client Applications, including:

- Oxygen AI Positron for Desktop Plugin: Provides AI-powered content generation, improvement suggestions, and other AI features directly within the XML editing environment.
- Oxygen AI Positron for Content Fusion Plugin: Integrates AI capabilities into the collaborative document review and authoring workflow.
- Other Authorized Oxygen Family Products: Additional applications that integrate AI Positron Service through dedicated plugins.

These Client Applications provide the user interface, determine what data to include in API requests based on user actions and document content, manage the display of responses, and may store queries or responses locally within the application environment.

2.1.3 API Request Flow

When a user utilizes AI features through a Client Application:

- User Action in Client Application: User performs an action that triggers AI functionality (e.g., types in a chat interface, selects text in editor interface and clicks "improve," or triggers an automated AI feature)
- Client Application Generates API Request: The Client Application constructs an API request containing the query data (which may include user input, selected document content, or application-generated prompts)
- API Request to Service: Client Application sends authenticated API request to AI Positron Service
- Authentication and Routing: Service validates user authentication, checks credit availability, and routes the request to the user-selected LLM Provider
- LLM Processing: LLM Provider processes the query and generates a response
- Response Return: Service receives response from LLM Provider and returns it to the requesting Client Application
- Display to User: Client Application displays the response in its interface

At no point in this flow does the Service store the content of API requests or responses beyond transient processing in server memory during the routing operation.

2.2 Two Distinct Categories of Data Processing

This DPA applies to two fundamentally different categories of Personal Data processing by Syncro Soft in connection with the Service. These categories have different characteristics, legal bases, and data protection obligations.

2.2.1 Category 1: Persistent Processing of Account and Billing Data

Syncro Soft processes and stores Personal Data necessary for account management, authentication, Organization administration, billing, and API access control. This processing includes:

- *Account Creation and Authentication:* Syncro Soft processes Personal Data of users obtained through OAuth authentication for the purpose of creating and managing user accounts. Users authenticate to the Service using their existing OAuthcredentials, and Syncro Soft receives and stores the user's name,email address and avatar picture from the selected OAuth Provider.
- *Organization and Team Management:* When a user creates an Organization and invites members, Syncro Soft processes Personal Data of invited members (name and email address) for the purpose of managing Organization membership and facilitating centralized billing. The Organization Owner is responsible for payment of API usage credits consumed by all confirmed members of their Organization.
- *Invitation and Membership Confirmation Process:* Organization Owners can generate generic invitation links to invite users to join their Organization. When a person accesses

such an invitation link, a Pending Membership Request is created containing that person's account information (or prompting them to create an account if they do not have one). The person does not become an Organization Member until the Organization Owner explicitly confirms the membership request. Syncro Soft stores information about Pending Membership Requests until they are either confirmed or rejected by the Organization Owner.

- *API Access Credentials:* Syncro Soft generates and manages API authentication tokens and credentials that Client Applications use to authenticate API requests on behalf of users.
- *Billing and Payment Processing:* Syncro Soft processes billing and payment information necessary to charge users and Organization Owners for credit packages, process payments, track credit consumption through API usage, and generate invoices.
- *Service Communications:* Syncro Soft uses stored email addresses to send service-related notifications, including account confirmations, password resets, credit balance alerts, billing notifications, security alerts, and administrative communications.

For this Category 1 processing, Customer is the Controller and Syncro Soft is the Processor. Customer determines the purposes and means of processing this data (by choosing to create an account, create an Organization, invite members, etc.), and Syncro Soft processes it on Customer's behalf according to Customer's instructions as documented in this DPA and the Service Agreement.

2.2.2 Category 2: Real-Time API Transmission of Request Data (No Storage)

Client Applications send API requests containing query data through the Service to selected LLM Providers. This transmission process involves:

Nature of Transmission: The Service acts as an authenticated API gateway. When a Client Application sends an API request:

- Service receives the encrypted API request from the Client Application
- Service validates the user's authentication credentials
- Service checks the user's available credit balance
- Service routes the API request to the selected LLM Provider's API endpoint
- Service receives the response from the LLM Provider
- Service returns the response to the requesting Client Application

Stateless Architecture: The Service is architected to process API requests statelessly, meaning:

- No session data is maintained between requests
- API request content passes through server memory only during the routing operation
- No application-level caching or buffering of request content occurs
- Server memory is cleared after each request is completed

No Storage or Retention of Request Content: The Service does NOT:

- Store the content of API requests sent by Client Applications
- Store the content of responses received from LLM Providers
- Log request or response content in application logs
- Cache request or response content for any purpose
- Retain request or response content in backup systems
- Have any persistent storage mechanism for request or response content

Metadata Collection Only: The Service collects and logs API Request Metadata for billing verification, service performance monitoring, and technical troubleshooting:

- Timestamp of API request
- User account identifier (internal ID, not name or email in logs)
- Organization identifier (if user is part of an Organization)
- Selected LLM Provider
- Client Application identifier and version
- Request payload size in bytes (but NOT the actual content)
- Response payload size in bytes (but NOT the actual content)
- API response time and latency measurements
- HTTP status codes and error codes
- Number of credits consumed

Client Application's Role: The Client Application, not the Service, determines:

- What content to include in API requests (user inputs, document content, application-generated prompts)
- When to send API requests (immediate, batched, scheduled, or background)
- How to present responses to users in the application interface
- Whether to store API requests or responses locally within the Client Application's environment

The Service has no visibility into, control over, or responsibility for these Client Application decisions.

For this Category 2 processing, Syncro Soft does not act as a Processor within the meaning of GDPR Article 28 because the Service does not "process" the data in a meaningful sense, it merely transmits it through its infrastructure as a technical conduit. The processing relationships for API Request Data exist directly between:

- Customer and the Client Application provider (the application processes user documents and actions to generate API requests)
- Customer and the LLM Provider (the provider processes API requests according to its own terms and privacy policy)

The Service is a technical intermediary in this data flow, providing authenticated routing infrastructure, but is not a processor of the request content itself.

2.3 Data Controllers and Processors for Each Category

2.3.1 For Account and Billing Data (Category 1):

Customer as Controller: Customer is the Controller of all Account and Billing Data. Customer determines the purposes and means of processing by deciding to create an account, create an Organization, invite members, and use the Service. Customer is responsible for ensuring that processing of Account and Billing Data has a lawful basis under Data Protection Laws.

Syncro Soft as Processor: Syncro Soft is the Processor of Account and Billing Data. Syncro Soft processes this data only on behalf of and according to Customer's instructions as documented in this DPA, the Service Agreement, and through Customer's use of the Service.

CCPA Roles: To the extent Processing of Account and Billing Data is subject to the CCPA, the parties agree that Customer is the "Business" and Syncro Soft is the "Service Provider" as those terms are defined by the CCPA.

2.3.2 For API Request Data (Category 2):

Customer Retains Control: Customer retains complete control over API Request Data, including what information to include in requests (through configuration of the Client Application) and which LLM Provider to use for processing.

Syncro Soft as Technical Intermediary: Syncro Soft does not determine the purposes or means of processing API Request Data and therefore does not act as a Processor under GDPR Article 28 for this data. The Service provides only technical infrastructure for authenticated API request routing.

LLM Providers as Independent Controllers: LLM Providers are independent data controllers (or processors, depending on their specific terms of service) for API Request Data they receive through the Service. Each LLM Provider processes requests according to its own privacy policy and terms of service. Syncro Soft does not control and is not responsible for how LLM Providers process API Request Data.

Client Application Providers as Controllers: Client Application providers are independent controllers for processing that occurs within their applications, including decisions about what data to include in API requests, whether to store requests or responses locally, and how to present information to users. Where Syncro Soft provides both the Service and the Client Application (such as Oxygen XML AI Positron plugins), Syncro Soft acts in two separate capacities with distinct processing operations governed by separate privacy policies.

2.4 Customer's Instructions

2.4.1 Documented Instructions for Account and Billing Data. Customer's instructions for the processing of Account and Billing Data are documented in:

- This DPA and its Annexes
- The Service Agreement
- Customer's use and configuration of the Service through the account portal (including creating an account, creating Organizations, inviting and confirming members, purchasing credits, and configuring settings)
- Any other written instructions provided by Customer that Syncro Soft acknowledges in writing

2.4.2 Compliance with Instructions Syncro Soft shall process Account and Billing Data only in accordance with Customer's documented instructions unless required to do so by applicable law, in which case Syncro Soft shall inform Customer of that legal requirement before processing (unless prohibited by law from doing so).

2.4.3 Unlawful Instructions. If Syncro Soft believes that any instruction from Customer violates Data Protection Laws, Syncro Soft will promptly inform Customer and may suspend performance of the instruction until Customer confirms or modifies the instruction. Syncro Soft will not be liable for any failure to process Personal Data to the extent that such failure results from Customer's unlawful instructions.

2.4.4 Additional Instructions. Customer may issue additional written instructions regarding the processing of Account and Billing Data that are consistent with the terms of this DPA and the Service Agreement. Syncro Soft will evaluate such instructions and may charge reasonable fees if complying with the instructions requires work beyond the scope of the Service or this DPA. If Syncro Soft cannot reasonably comply with an instruction, the Parties will work together in good faith to find an alternative solution.

2.4.5 No Instructions for API Request Data. Customer acknowledges that Syncro Soft does not process API Request Data according to Customer's instructions in the sense contemplated by GDPR Article 28 because Syncro Soft does not process the content of such data—it only routes it. Customer's selection of an LLM Provider and submission of an API request through a Client Application constitutes Customer's instruction to transmit the request to that specific LLM Provider, but this is a transmission instruction rather than a data processing instruction in the GDPR sense.

3. DETAILS OF PROCESSING

The details of the processing of Personal Data by Syncro Soft on behalf of Customer are set forth in Annex I (Details of Processing) to this DPA, including: subject matter of processing; duration of processing; nature and purpose of processing; types of Personal Data processed; and categories of Data Subjects.

Customer acknowledges that the details in Annex I provide a general description of the processing activities and that actual processing may vary based on Customer's specific use of the Service and the Client Applications through which Customer accesses the Service.

4. CUSTOMER'S OBLIGATIONS

4.1 Lawfulness of Processing Account and Billing Data

Customer warrants and represents that:

1. Lawful Basis: Customer has a lawful basis under Data Protection Laws for the processing of Account and Billing Data through the Service, including any necessary consents, contractual necessity, legal obligations, legitimate interests, or other lawful basis.
2. Data Subject Rights and Transparency: Customer has provided or will provide Data Subjects with appropriate information about the processing of their Personal Data (including information required by Articles 13 and 14 of the GDPR) and has obtained any necessary consents or authorizations.
3. Organization Owner Responsibilities: If Customer acts as an Organization Owner, Customer warrants that:
    - Customer has the authority to invite individuals to join the Organization and to commit to paying for their API usage
    - Customer has informed or will inform invited members about the processing of their Personal Data by Syncro Soft as described in this DPA and Syncro Soft's Privacy Policy
    - Customer will exercise reasonable care in distributing invitation links to ensure they reach only intended recipients
    - Customer will promptly review and act upon Pending Membership Requests to avoid prolonged storage of data for individuals who accessed invitation links unintentionally
4. Lawful Transfer: If Customer transfers Personal Data to Syncro Soft from jurisdictions outside the EEA, Customer has ensured that such transfers comply with applicable Data Protection Laws in the originating jurisdiction.
5. Special Categories of Personal Data: Customer will not process Special Categories of Personal Data (as defined in Article 9 of the GDPR) through the Service without first notifying Syncro Soft in writing and obtaining Syncro Soft's prior written consent. If such processing is authorized, the Parties will implement additional safeguards as required by Data Protection Laws.
6. U.S. Privacy Laws Compliance: To the extent U.S. Privacy Laws apply, Customer agrees to not take any action that would render the provision of Personal Information to Syncro Soft a "sale" under U.S. Privacy Laws or a "share" under the CCPA, or render Syncro Soft not a "service provider" under the CCPA.

4.2 Accuracy and Minimization

Customer is responsible for: ensuring that Account and Billing Data processed through the Service is accurate, adequate, relevant, and limited to what is necessary for the purposes of

processing; providing only accurate information when creating accounts and Organizations; keeping account information up to date; ensuring that invitations are sent only to individuals who should legitimately be part of the Organization; and maintaining the quality and integrity of Personal Data processed through the Service.

4.3 Organization Member Management

Customer acting as an Organization Owner is responsible for: ensuring that all individuals invited to join an Organization are legitimately intended to be members; exercising reasonable diligence in distributing generic invitation links to minimize the risk of unintended recipients accessing the links; promptly reviewing Pending Membership Requests and confirming or rejecting them in a timely manner; understanding that confirmed members' API usage will be charged to the Organization Owner; informing Organization Members about their rights regarding their Personal Data and how they can exercise those rights; and responding appropriately if a Member wishes to leave the Organization or requests deletion of their Personal Data.

4.4 Responsibility for API Request Data

Because the Service does not process the content of API Request Data and has no visibility into what Personal Data (if any) is included in such requests, Customer bears sole responsibility for:

1. Understanding Client Application Behavior: Customer must understand how each Client Application used to access the Service generates API requests, including:
    - What data the Client Application may include in requests (user inputs, document content, metadata)
    - When the Client Application sends requests (user-initiated, automatic, background)
    - What controls the Client Application provides to manage data inclusion
    - Whether the Client Application stores requests or responses locally
2. Lawful Basis for Data in API Requests: Customer must ensure that there is a lawful basis under Data Protection Laws for any Personal Data that may be included in API requests sent through the Service to LLM Providers. This includes obtaining necessary consents, ensuring contractual necessity, or establishing another appropriate lawful basis.
3. Transparency to Data Subjects: If Personal Data of individuals other than Customer is included in API requests (such as when Customer uses AI features on documents containing others' content), Customer must inform those individuals that:
    - Their data may be processed by AI systems
    - Their data will be transmitted to third-party LLM Providers
    - Each LLM Provider processes data according to its own privacy policy
    - They have rights under Data Protection Law regarding their data

4. Reviewing LLM Provider Policies: Customer is responsible for reviewing and understanding the privacy policy and data processing practices of each LLM Provider that Customer chooses to use through the Service. Customer should:
    - Understand whether each LLM Provider uses query data for AI model training
    - Understand each provider's data retention practices
    - Understand the jurisdictional location of each provider's data processing
    - Assess whether each provider's practices are appropriate for the types of data Customer intends to send
5. Sensitive and Confidential Data: Customer must exercise appropriate caution when using AI features through Client Applications on content containing:
    - Trade secrets or confidential business information
    - Personal Data of customers, employees, or third parties
    - Content subject to confidentiality agreements, non-disclosure obligations, or attorney-client privilege
    - Unpublished or proprietary content
    - Health information, financial data, or other sensitive personal information
    - Special Categories of Personal Data as defined in GDPR Article 9

    Customer acknowledges that when AI features are used on such content through a Client Application, the Client Application may include that content in API requests sent to LLM Providers through the Service. Customer should not use AI features on content if transmitting that content to LLM Providers would violate applicable laws, contractual obligations, or ethical duties.
6. Configuring Client Applications: Customer is responsible for properly configuring any Client Applications used to access the Service, including:
    - Reviewing and adjusting privacy settings within the Client Application
    - Disabling automatic or background API request generation if it does not align with Customer's data protection requirements
    - Setting up content filters or exclusions to prevent sensitive data from being included in requests
    - Training users on appropriate use of AI features within Client Applications
7. Third-Party Content: If Customer uses AI features on content created by collaborators, clients, partners, or other third parties (such as in collaborative editing environments like Oxygen Content Fusion), Customer must:
    - Determine whether Customer has the right to send such content to LLM Providers
    - Obtain necessary consents or authorizations from content creators

- Inform content creators that their content may be processed by AI systems through the Service
- Ensure such processing complies with any agreements with content creators

8. Monitoring and Oversight: Customer should implement appropriate oversight of how AI features accessed through the Service are used within Customer's organization, particularly for:
    - Client Applications that may generate API requests automatically based on user actions
    - Background or scheduled API requests that may occur without explicit user initiation for each request
    - Processing of documents or content containing Personal Data of multiple individuals

4.5 Client Application Provider Relationships

Customer acknowledges and understands that:

1. Separate Privacy Policies Apply: Each Client Application that integrates with the Service is governed by its own privacy policy that is separate from this DPA and the Service's Privacy Policy. Customer should review:
    - This DPA and the Service Privacy Policy (for how the Service processes data)
    - The Client Application's privacy policy (for how the application processes data)
2. Client Application as Controller: The Client Application provider acts as an independent data controller for processing that occurs within the Client Application, including:
    - Decisions about what data to include in API requests
    - Local storage of queries or responses within the application
    - Analytics or telemetry about how users interact with AI features
    - Any other processing of user data within the application environment
3. Syncro Soft's Dual Roles: Where Syncro Soft provides both the Service and a Client Application (such as Oxygen AI Positron plugins), Customer acknowledges that Syncro Soft acts in two separate capacities:
    - As Processor for Account and Billing Data under this DPA
    - As independent Controller for data processing within the Client Application, governed by that application's separate privacy policy

    These are distinct processing operations with separate purposes, legal bases, and data protection obligations.

5. PROCESSOR'S OBLIGATIONS

5.1 Confidentiality

- Confidentiality Obligations: Syncro Soft shall ensure that persons authorized to process Account and Billing Data (including employees, contractors, and Sub-processors) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- Access Limitation: Syncro Soft shall ensure that access to Account and Billing Data is limited to those personnel who need access to perform their duties in connection with the Service and that such personnel are appropriately trained in data protection.
- Non-Disclosure: Syncro Soft shall not disclose Account and Billing Data to any third party except: to Sub-processors as permitted under Section 6; as required by applicable law (with notice to Customer where permitted); or as instructed by Customer.
- API Request Data: Syncro Soft's systems are architecturally designed such that Syncro Soft personnel do not have access to the content of API requests or responses during transmission. There are no mechanisms by which request content can be intercepted, viewed, logged, or recorded by Syncro Soft personnel.

5.2 Security Measures

1. Technical and Organizational Measures: Syncro Soft shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.
2. Security Measures for Account and Billing Data (Stored Data):For Account and Billing Data that is stored persistently, such measures shall include, as appropriate:
    - Encryption of Personal Data at rest using industry-standard encryption algorithms (AES-256 or equivalent)
    - Encrypted backups with secure key management
    - Ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident
    - Regular testing, assessing, and evaluating the effectiveness of technical and organizational measures
    - Access controls ensuring that Account and Billing Data is accessible only to authorized personnel based on role-based access control principles
    - Secure authentication mechanisms including support for multi-factor authentication for administrative accounts

- Regular security assessments, vulnerability scanning, and penetration testing
- Secure data disposal and deletion procedures

3. Security Measures for API Request Data Transmission: For API Request Data that is transmitted through the Service to LLM Providers, security measures are fundamentally different and focus on protecting data during transmission without storage:
    - Transmission exclusively via TLS 1.2 or higher encryption between Client Applications and the Service
    - Transmission exclusively via TLS 1.2 or higher encryption between the Service and LLM Provider APIs
    - Stateless request processing architecture where servers do not retain any data between requests
    - Absence of application-level logging of request or response content
    - No caching, buffering, or temporary persistent storage of request or response content
    - Secure API authentication using encrypted credentials
    - Rate limiting and abuse prevention mechanisms that operate on metadata only without inspecting request content
    - Monitoring systems that track only metadata (request counts, response times, error rates) without accessing request content
4. OAuth Security: For authentication via OAuth Providers, security measures include validation of OAuth tokens according to industry best practices; protection against CSRF and injection attacks; rate limiting for authentication attempts; secure storage of OAuth refresh tokens (if applicable) with encryption; and immediate revocation capabilities if an account is compromised.
5. Security Documentation: A more detailed description of Syncro Soft's current security measures is set forth in Annex II (Technical and Organizational Security Measures) to this DPA. Customer acknowledges that these measures are subject to technical progress and development, and Syncro Soft may update or modify them from time to time, provided that such updates or modifications do not result in a material degradation of the security of the Service.
6. Industry Standards: Syncro Soft shall maintain certifications, attestations, or compliance with recognized industry security standards (such as ISO 27001) to the extent commercially reasonable and appropriate for the Service. Syncro Soft will make information about current certifications available to Customer upon request.

5.3 Assistance with Data Subject Rights See Section 11 (Data Subject Rights Assistance) for detailed provisions regarding Syncro Soft's assistance with Customer's obligations to respond to Data Subject requests.

5.4 Assistance with Compliance Obligations

- Security Breach Notification: Syncro Soft shall assist Customer in ensuring compliance with Customer's obligations under Articles 32 to 36 of the GDPR (security of processing, notification of Personal Data Breaches, communication to Data Subjects, Data Protection Impact Assessments, and prior consultation with Supervisory Authorities), taking into account the nature of processing and the information available to Syncro Soft. See Section 8 (Personal Data Breaches).
- Prior Consultation: If required under Article 36 of the GDPR, Syncro Soft will provide reasonable assistance to Customer in consulting with Supervisory Authorities.
- Information Provision: Syncro Soft will make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR, limited to processing activities for which Syncro Soft acts as Processor (i.e., Account and Billing Data).
- Audits: Syncro Soft shall allow for and contribute to audits, including inspections, conducted by Customer or an auditor mandated by Customer, subject to the audit provisions in Section 9 of this DPA.
- U.S. Privacy Laws Compliance: To the extent U.S. Privacy Laws apply, Syncro Soft certifies that it understands and will comply with its obligations as a "Service Provider" under the CCPA and provide Customer with all assistance required to address Customer's obligations under the CCPA.

6. SUB-PROCESSORS

6.1 Authorized Sub-processors

Customer provides general authorization for Syncro Soft to engage Sub-processors to process Account and Billing Data on Customer's behalf, provided that Syncro Soft complies with the requirements of this Section 6.

For clarity, "Sub-processors" as used in this Section refers only to entities that process Account and Billing Data that Syncro Soft stores and controls. LLM Providers are not Sub-processors under this DPA because they are independent Controllers for API Request Data, and Syncro Soft does not control their processing activities. LLM Providers are addressed separately in Section 7.

A current list of Sub-processors for Account and Billing Data is set forth in Annex III (Sub-processors and LLM Providers)

6.2 Sub-processor Requirements

When engaging a Sub-processor for processing Personal Data, Syncro Soft shall:

- Enter into a written contract with each Sub-processor imposing data protection obligations that are substantially similar to those imposed on Syncro Soft under this DPA, and, to the extent applicable, including the restrictions required under U.S. Privacy Laws such as prohibitions on selling, sharing, or retaining, using, or disclosing Personal Information beyond what is permitted under the Agreement.
- Remain fully liable to Customer for the performance of the Sub-processor's obligations.
- Monitor Sub-processor compliance with data protection obligations. Take reasonable steps to ensure Sub-processors comply with Data Protection Laws.

6.3 Changes to Sub-processors

- Notification. Syncro Soft shall notify Customer of any intended changes concerning the addition or replacement of Sub-processors at least 30 days before authorizing any new Sub-processor to process Personal Data. Notice will be provided via: i) email to Customer's account email address; and (ii) update to the Sub-processor list at https://www.oxygenxml.com/aipositron/subprocessors-list.html
- Objection. Customer may object to Syncro Soft's appointment of a new Sub-processor for Account and Billing Data or material change to an existing Sub-processor on reasonable data protection grounds by notifying Syncro Soft in writing within 30 days of receiving notice of the intended change.
- Resolution. If Customer objects, the Parties shall work together in good faith to find a commercially reasonable solution to address Customer's concerns, which may include: Syncro Soft providing additional safeguards or commitments regarding the Sub-processor; Syncro Soft not using the Sub-processor for Customer's Account and Billing Data; Syncro

Soft using an alternative Sub-processor; or Customer adjusting its use of affected Service features to avoid the Sub-processor (if technically feasible).

- Termination Right. If the parties cannot reach a resolution within 30 days and Customer has reasonable grounds for its objection, Customer may terminate the affected Services by providing written notice to Syncro Soft, with termination effective at the end of Customer's then-current billing period, or immediately with a pro-rata refund of prepaid fees for the terminated Services for the period after termination. This termination right is Customer's sole and exclusive remedy if Customer objects to a new Sub-processor.
- Deemed Acceptance. Customer's failure to object within 30 days of notification shall constitute consent to the use of the new Sub-processor.

6.4 No Objection to Current Sub-processors. By entering into this DPA, Customer agrees to the engagement of the Sub-processors listed in Annex III as of the Effective Date of this DPA.

7. LLM PROVIDERS AND API REQUEST DATA TRANSMISSION

7.1 Nature of LLM Provider Relationship

The Service enables users to access multiple Large Language Model services through Client Applications that integrate with the Service's API. When a user selects an LLM Provider and a Client Application sends an API request, the Service transmits that request to the selected LLM Provider and returns the response. This section clarifies the data protection relationship between Customer, Syncro Soft, LLM Providers, and Client Application providers.

7.2 LLM Providers as Independent Controllers

LLM Providers are independent data controllers (or processors, depending on their specific terms of service) for API Request Data they receive through the Service. Syncro Soft does not control and is not responsible for how LLM Providers process API Request Data. Each LLM Provider processes requests according to its own privacy policy, terms of service, and data processing practices.

7.3 Customer's Responsibilities Regarding LLM Providers

Customer acknowledges and agrees that:

- Review of LLM Provider Policies: Customer is responsible for reviewing and understanding the privacy policies, terms of service, and data processing practices of each LLM Provider that Customer chooses to use. The Service provides links to these policies within the account portal and in Annex III, but Customer remains responsible for staying informed about any updates or changes to LLM Provider policies.
- Consent and Lawful Basis: Customer is responsible for ensuring that it has a lawful basis under Data Protection Laws for transmitting any Personal Data to LLM Providers, including obtaining any necessary consents from Data Subjects or ensuring that another lawful basis applies.
- Transparency to Data Subjects: If Customer includes Personal Data about individuals in API requests sent to LLM Providers (either directly or through documents processed by Client Applications), Customer is responsible for informing those Data Subjects that their Personal Data will be processed by third-party LLM Providers and for providing appropriate transparency information as required by Data Protection Laws.
- Jurisdictional Awareness: Customer is responsible for understanding the jurisdictional implications of sending data to LLM Providers located in various countries. Syncro Soft provides information about each LLM Provider's location in the account portal and in Annex III, but Customer must assess whether these locations are appropriate for the types of data Customer intends to process.

- Selection of Appropriate LLM Providers: Customer has complete control over which LLM Providers to use and can choose to use only LLM Providers whose data processing practices Customer finds acceptable. If Customer has concerns about a particular LLM Provider's privacy practices, Customer should not configure Client Applications to use that provider.

7.4 Information About LLM Providers

Syncro Soft maintains current information about available LLM Providers in Annex III (Sub-processors and LLM Providers), in the account portal at https://aipositron.oxygenxml.com/. For each LLM Provider, Syncro Soft provides: the provider's name and parent company; the provider's primary jurisdiction and data processing locations (if publicly disclosed); links to the provider's privacy policy and terms of service; and information about any relevant certifications or compliance frameworks (such as Data Privacy Framework certification, ISO certifications, SOC 2 compliance).

Syncro Soft will use commercially reasonable efforts to keep this information current, but Customer should independently verify information about LLM Providers, particularly before using a provider for processing sensitive data.

7.5 Changes to Available LLM Providers

- Addition of New LLM Providers: Syncro Soft may add new LLM Providers to the Service at any time to provide Customer with more options and improved functionality. The addition of a new LLM Provider does not require prior notice to Customer because Customer has complete discretion over whether to configure Client Applications to use any particular LLM Provider. Customer is not obligated to use any LLM Provider and can choose to use only those providers whose privacy practices Customer finds acceptable.
- When a new LLM Provider is added to the Service, Syncro Soft will: update Annex III to include the new provider; provide information about the new provider within the account portal; and send a notification to users announcing the availability of the new provider (this notification is for informational purposes and does not trigger any objection rights under this DPA).
- Removal of LLM Providers: If Syncro Soft intends to remove an LLM Provider that is currently available in the Service, Syncro Soft will provide at least 30 days' advance notice to users who have recently configured Client Applications to use that provider. This notice period allows users to adjust their configurations if they have been relying on the provider being removed.
- No Objection Rights for LLM Provider Changes: Because LLM Providers are not Sub-processors under this DPA and because Customer has complete discretion over which LLM Providers to use (through Client Application configuration), the objection and termination rights set forth in Section 6.3 do not apply to changes in the list of available LLM Providers.

If Syncro Soft adds an LLM Provider whose privacy practices Customer finds unacceptable, Customer can simply choose not to configure Client Applications to use that provider while continuing to use other available providers.

7.6 Syncro Soft's Limited Role in API Request Processing

Syncro Soft's role with respect to API Request Data is strictly limited to providing the technical infrastructure for authenticated transmission. Specifically:

- No Control Over Request Content: Syncro Soft does not and cannot control what information Customer (through Client Applications) includes in API requests. Syncro Soft has no way of knowing whether any particular API request contains Personal Data, and if so, what type of Personal Data or whose Personal Data it is.
- No Storage or Inspection: Syncro Soft does not store, log, cache, or retain API Request Data. The Service architecture is designed to transmit API requests through Syncro Soft's servers without any persistent storage. Syncro Soft does not inspect the content of API requests for any purpose, including analytics, quality assurance, or security monitoring (except for scanning for malicious payloads or abuse patterns using automated systems that do not retain content).
- Technical Transmission Only: Syncro Soft's systems receive an encrypted API request from the Client Application, validate the user's authentication credentials and credit balance, add appropriate authentication headers to communicate with the selected LLM Provider, transmit the request via HTTPS to the LLM Provider, receive the response from the LLM Provider, and transmit the response back to the requesting Client Application. This entire process occurs in real-time without any intermediate persistent storage.
- Metadata Only: Syncro Soft may collect and log API Request Metadata for billing, service availability monitoring, and technical troubleshooting purposes. This metadata includes timestamp, user identifier, selected LLM Provider, request and response sizes in bytes, latency, status codes, and credits consumed. This metadata does not include or reveal the content of API requests or responses.

7.7 Security of API Request Transmission

While Syncro Soft does not process API Request Data content, Syncro Soft implements appropriate security measures to ensure the confidentiality and integrity of API Request Data during transmission:

- Encryption in Transit: All API request transmissions between Client Applications and the Service, and between the Service and LLM Providers, are encrypted using TLS 1.2 or higher. API requests are never transmitted in plaintext over any network.
- Secure API Authentication: Syncro Soft securely manages API credentials for authenticating with LLM Providers. These credentials are encrypted at rest and are never exposed to users or logged in any system logs.
- Network Isolation: Each user's API requests are isolated at the network level to prevent any possibility of requests from different users being commingled or misdirected.
- Stateless Processing: The Service uses stateless HTTP connections without any persistent session data that could leak request information between API calls.

7.8 Client Application as Intermediary

Customer acknowledges that Client Applications act as an additional layer between the user and the Service. The Client Application:

- Receives user inputs or processes document content to generate API request data
- Sends authenticated API requests to the Service
- Receives responses from the Service and displays them to users
- May store API requests or responses locally within the Client Application environment

The Client Application provider (which may be Syncro Soft for Oxygen family products, or may be a third party) is responsible for the data processing that occurs within the Client Application. This processing is governed by the Client Application's own privacy policy, not by this DPA.

8. INTERNATIONAL TRANSFERS

8.1 Transfers of Account and Billing Data Outside EEA

Customer acknowledges and agrees that Syncro Soft may transfer Account and Billing Data to countries outside the European Economic Area ("EEA"), including to the United States and other jurisdictions where Sub-processors are located, for the purposes of providing the Service.

Syncro Soft shall ensure that any such transfer of Account and Billing Data to a country outside the EEA is subject to appropriate safeguards as required by Data Protection Law. Depending on the destination, Syncro Soft may rely on one or more of the following mechanisms:

- Adequacy Decisions. Where the European Commission has adopted an adequacy decision recognizing that a third country provides an adequate level of data protection, Syncro Soft may rely on such adequacy decision for transfers of Account and Billing Data to that country.
- EU-U.S. Data Privacy Framework (DPF). For transfers to Sub-processors located in the United States that are certified under the EU-U.S. Data Privacy Framework (or any successor framework), Syncro Soft may rely on such certification as an adequacy mechanism under Article 45 GDPR.
- Standard Contractual Clauses (SCCs). For transfers to countries without an adequacy decision from the European Commission, Syncro Soft will implement the Standard Contractual Clauses approved by the European Commission pursuant to Decision 2021/914 (Module Two: Controller to Processor) or any subsequent version approved by the European Commission.

8.2 Transfers of API Request Data to LLM Providers

Customer acknowledges and explicitly understands that when Customer (through a Client Application) selects an LLM Provider and sends an API request, API Request Data (which may contain Personal Data) will be transmitted to that LLM Provider's systems, which may be located in jurisdictions outside the EEA.

8.2.1 Customer's Responsibility for API Request Data Transfers: Because Syncro Soft does not control the processing of API Request Data by LLM Providers, and because Customer directly selects (through Client Application configuration) which LLM Provider to use for each request, Customer is responsible for ensuring that transfers of API Request Data to LLM Providers comply with applicable Data Protection Laws.

Customer's selection of a particular LLM Provider and submission of an API request to that provider (through a Client Application) constitutes Customer's explicit instruction to transmit the request data to that provider's jurisdiction. The Service merely executes this instruction by transmitting the data to the selected provider.

8.2.2 Information to Support Customer's Assessment: To assist Customer in assessing the legality of transfers to LLM Providers, Syncro Soft provides information about each LLM Provider's location and data processing practices in Annex III, in the account portal. This information includes: the LLM Provider's primary jurisdiction; known data processing locations (if the provider has disclosed this information); links to the provider's privacy policy and data transfer disclosures; information about the provider's participation in adequacy frameworks (such as EU-U.S. Data Privacy Framework certification); and information about the provider's use of Standard Contractual Clauses or other transfer mechanisms (if publicly disclosed).

8.2.3 Customer's Due Diligence: Customer should conduct its own due diligence regarding each LLM Provider's data transfer practices before configuring Client Applications to use that provider for API requests containing Personal Data. If Customer is subject to specific regulatory requirements or restrictions regarding international data transfers, Customer should: review each LLM Provider's privacy policy and data transfer disclosures; assess whether the LLM Provider's transfer mechanisms are adequate for Customer's compliance obligations; consider implementing additional safeguards or contractual protections directly with LLM Providers if necessary; and choose to configure Client Applications to use only LLM Providers whose transfer practices meet Customer's compliance requirements.

8.2.4 Syncro Soft's Lack of Control: Syncro Soft cannot guarantee or warrant that any particular LLM Provider's data transfer practices will meet Customer's specific compliance requirements. Syncro Soft's role is limited to providing the technical means to transmit API requests to providers selected by Customer. The adequacy of transfer mechanisms is a matter between Customer and the LLM Provider.

8.3 Standard Contractual Clauses for Account and Billing Data

The Standard Contractual Clauses are incorporated into and form part of this DPA with respect to transfers of Account and Billing Data outside the EEA to jurisdictions without an adequacy decision. Where there is any conflict between the provisions of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

The parties agree to the following specific terms regarding the Standard Contractual Clauses:

- Module: The parties agree that Module Two (Controller to Processor) of the Standard Contractual Clauses applies to the processing activities for Account and Billing Data under this DPA.
- Clause 7 (Docking Clause): The parties agree that the docking clause applies, allowing entities that are not party to this DPA to accede to the Standard Contractual Clauses.
- Clause 9 (Use of Sub-processors): The parties agree to Option 2 (General Written Authorization), whereby Controller provides general authorization for Processor to engage

Sub-processors for Account and Billing Data, subject to the notification and objection procedures set forth in Section 6 of this DPA.

- Clause 11 (Redress): The parties agree that the optional language regarding the independent dispute resolution body shall not apply.
- Clause 17 (Governing Law): The Standard Contractual Clauses shall be governed by the law of Romania.
- Clause 18 (Choice of Forum and Jurisdiction): Any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of Bucharest, Romania.
- Annexes to SCCs: The information required for Annexes I, II, and III of the Standard Contractual Clauses is set forth in the Annexes to this DPA.

UK Data Protection Law: To the extent the Account and Billing Data is subject to UK Data Protection Law, Syncro Soft agrees to Process such Personal Data in compliance with the SCCs, with the following modifications: The SCCs shall be deemed amended as specified by Part 2 of the UK Addendum, Tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed respectively with the information set out in Annexes 1-3 of this DPA (as applicable); and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party."

8.4 Additional Safeguards for Transfers

In addition to implementing the Standard Contractual Clauses for Account and Billing Data, Syncro Soft shall implement supplementary measures: encryption at rest (AES-256) and in transit (TLS 1.2+); access controls limiting access to authorized personnel only; confidentiality commitments from all personnel with access; contractual measures requiring Sub-processors to implement equivalent safeguards; and regular review and assessment of measure effectiveness.

8.5 Government Access Requests

Syncro Soft shall implement policies and procedures to handle government or law enforcement requests for access to Account and Billing Data transferred outside the EEA: assess legality, scope, and proportionality before complying; challenge unlawful, overbroad, or disproportionate requests; notify Customer unless prohibited by law; disclose only minimum data necessary if required to comply; and document all requests and make documentation available to Customer to extent permitted by law.

8.5.1 API Request Data: For API Request Data, Syncro Soft cannot respond to government requests because Syncro Soft does not possess API Request Data. Any government requests for API Request Data would need to be directed to the relevant LLM Provider(s).

8.6 Suspension of Transfers

If Standard Contractual Clauses are invalidated, Syncro Soft is unable to implement appropriate supplementary measures, Syncro Soft becomes aware that local laws prevent fulfilling DPA obligations, or a supervisory authority orders suspension, then Syncro Soft shall immediately

notify Customer and shall suspend transfers of Account and Billing Data outside the EEA until an alternative legal mechanism is identified and implemented. If transfers cannot be resumed within 60 days, either party may terminate the affected portion of the Service upon written notice.

9. PERSONAL DATA BREACHES

9.1 Notification to Customer

Syncro Soft will notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Account and Billing Data, and in any event within 72 hours of becoming aware of the breach, unless a longer period is permitted by applicable law.

Personal Data Breach notifications shall be sent via email to Customer's account email address. Notifications may also be sent via the account portal interface.

9.2 Content of Notification

To the extent the information is available to Syncro Soft at the time of notification, Syncro Soft will include in the notification: description of the nature of the breach, including categories and approximate number of Data Subjects and records concerned; name and contact details of Syncro Soft's data protection contact; description of the likely consequences; and description of measures taken or proposed to address the breach and mitigate effects.

If not all information is available at the time of initial notification, Syncro Soft will provide the information in phases without undue further delay as it becomes available.

9.3 Investigation and Remediation

Upon becoming aware of a Personal Data Breach affecting Account and Billing Data, Syncro Soft will: promptly investigate to determine cause, scope, and impact; take reasonable steps to mitigate effects; preserve evidence; cooperate with Customer's reasonable requests for information and assistance; provide reasonable assistance in notifying Data Subjects or Supervisory Authorities if required; and implement measures to prevent similar breaches.

9.4 Customer's Responsibilities

Customer is responsible for: determining whether notification to Data Subjects or Supervisory Authorities is required; complying with any notification obligations; and taking any additional measures required by Data Protection Laws in response to the breach.

Syncro Soft will provide reasonable cooperation and assistance to Customer in fulfilling these responsibilities.

9.5 Breaches at LLM Providers or Client Applications

9.5.1 LLM Provider Breaches: If an LLM Provider experiences a data breach that affects API Request Data sent by Customer, this would not constitute a Personal Data Breach under this DPA because Syncro Soft does not control or possess that data. Customer should monitor breach notifications from LLM Providers directly and should respond to any such breaches according to Customer's own incident response procedures and legal obligations.

Syncro Soft will inform Customer if Syncro Soft becomes aware of a data breach at an LLM Provider that may affect Customer's API Request Data, but Syncro Soft's knowledge of such breaches will be limited to public announcements or direct notifications from the LLM Provider.

9.5.2 Client Application Breaches: If a Client Application experiences a data breach affecting data stored locally within the application (such as stored conversation history or cached responses), this is the responsibility of the Client Application provider, not Syncro Soft (unless Syncro Soft is also the Client Application provider, in which case separate notification procedures under that application's privacy policy would apply).

9.6 No Acknowledgment of Fault

Syncro Soft's notification of or response to a Personal Data Breach under this Section 9 will not be construed as an acknowledgment by Syncro Soft of any fault or liability with respect to the breach. Syncro Soft's liability for Personal Data Breaches is subject to the limitations and exclusions set forth in the Service Agreement.

9.7 Security Incidents vs. Personal Data Breaches

For clarity, not every security incident constitutes a Personal Data Breach. Events such as unsuccessful login attempts, scanning, pings, port scans, denial of service attacks, or other events that do not result in unauthorized access to or loss of Account and Billing Data are not Personal Data Breaches and will not trigger the notification obligations under this Section 9. However, Syncro Soft may notify Customer of such security incidents as part of its general security practices.

10. AUDIT RIGHTS

10.1 Customer's Right to Audit

Customer has the right to audit Syncro Soft's compliance with this DPA and Data Protection Law with respect to processing of Account and Billing Data, subject to the procedures and limitations set forth in this Section 10.

Audits may be conducted for purposes of verifying compliance with this DPA, assessing adequacy of security measures for Account and Billing Data, investigating suspected data breaches or security incidents, or complying with Customer's own legal or regulatory obligations.

10.1.1 Scope Limitation for API Request Data: Audits cannot extend to API Request Data content because Syncro Soft does not process API Request Data content in a manner that would be subject to audit—API Request Data passes through Syncro Soft's systems without storage or inspection. Audits may verify the architectural and security measures that prevent API Request Data from being stored or accessed, but cannot access API Request Data itself because no such data exists in Syncro Soft's systems.

10.2 Audit Procedures

Audits shall be conducted in accordance with the following procedures: at least 60 days advance notice (unless urgent circumstances require shorter notice); specification of scope, objectives, timing, auditor identity, and areas of concern; scheduling at mutually convenient times during business hours with minimal disruption; use of qualified, independent auditors who are not competitors and have executed confidentiality agreements; execution of Syncro Soft's confidentiality agreement by Customer and auditors; and treatment of audit information as confidential except as necessary for Data Protection Law compliance demonstrations to supervisory authorities.

Syncro Soft shall provide reasonable cooperation and assistance during the audit, including providing access to relevant documentation, personnel, and systems, subject to security and confidentiality restrictions.

10.3 Limitations on Audit Rights

Audit rights are subject to the following limitations: frequency limited to once per 12 months (unless data breach or supervisory authority requires audit); scope limited to aspects relevant to processing Customer's Account and Billing Data; auditors must comply with Syncro Soft's security policies; Customer responsible for all audit costs (Syncro Soft may charge reasonable fees for audits requiring more than 16 hours of personnel time); and audits must not disrupt operations or compromise security.

10.4 Alternative Compliance Verification

In lieu of on-site audits, Customer may request alternative evidence of compliance: certifications and audit reports (ISO 27001, SOC 2); completed security questionnaires or DPIAs; standard audit reports covering data protection practices; remote assessments via video conference; or documentation of Sub-processor compliance.

Syncro Soft may require Customer to accept alternative compliance verification in lieu of on-site audits where on-site audits would be excessively disruptive or costly, Syncro Soft has recently undergone independent audits, or multiple customers are requesting audits within a short time.

If Customer is not satisfied with alternative verification and reasonably requires an on-site audit for legitimate compliance purposes, the parties shall work together in good faith to arrange an audit that meets Customer's needs while respecting Syncro Soft's operational constraints.

10.5 Audit Reports and Findings

Following audit completion: Customer or auditors shall provide Syncro Soft with a draft audit report and opportunity to respond; Syncro Soft shall have 15 business days to provide written responses including corrections, context, and remediation plans; Customer shall provide final audit report within 15 business days of receiving Syncro Soft's response; if audit identifies material non-compliance, Syncro Soft shall promptly develop and implement a remediation plan and provide updates on progress; and audit reports shall be treated as confidential except when disclosure is required to supervisory authorities, legal counsel, auditors (subject to confidentiality), or as required to establish Data Protection Law compliance.

10.6 Supervisory Authority Audits

If a supervisory authority requests or requires an audit of Syncro Soft's data processing activities in connection with Customer's Account and Billing Data, Syncro Soft shall: fully cooperate and provide requested information, documentation, and access; notify Customer of the audit request (except where prohibited); share with Customer any findings or recommendations relating to Customer's data (to extent permitted); and implement required corrective actions in a timely manner and inform Customer of remediation measures taken.

11. DELETION AND RETURN OF PERSONAL DATA

11.1 Return or Deletion Upon Termination

Upon termination or expiration of the Service Agreement, Syncro Soft shall, at Customer's choice: return a complete copy of all Account and Billing Data in a commonly used, machine-readable format (such as JSON or XML); or securely delete or destroy all Account and Billing Data, including all copies, backups, and archived data.

Prior to deletion, Syncro Soft will make Account and Billing Data available for Customer to retrieve for a period of 30 days following termination. Customer is responsible for retrieving data during this Retrieval Period.

Customer shall notify Syncro Soft of its choice in writing within 30 days of termination. If Customer does not provide such instruction, Syncro Soft shall delete all Account and Billing Data in accordance with Section 11.2 below.

11.1.1 API Request Data: API Request Data does not require return or deletion procedures because Syncro Soft does not store API Request Data. Any API Request Data that may have been retained by LLM Providers or stored locally by Client Applications is subject to those providers' and applications' own data retention and deletion practices. Customer should contact LLM Providers or Client Application providers directly if Customer requires deletion of data from those systems.

11.2 Deletion Procedures and Timeline

If Customer instructs Syncro Soft to delete Account and Billing Data, or if Customer does not provide instructions within 30 days of termination, Syncro Soft shall:

- Immediate Deletion from Active Systems: Delete Account and Billing Data from all active production systems within 7 days of the end of the data retrieval period (typically 30 days after termination).
- Deletion from Backups: Delete Account and Billing Data from backup systems, archives, and disaster recovery systems within 90 days of deletion from active systems.
- Secure Deletion Methods: Use industry-standard secure deletion methods including cryptographic erasure of encryption keys, multi-pass overwriting of data on magnetic media, and secure deletion commands for solid-state storage.
- Certificate of Deletion: Upon Customer's written request made within 60 days of termination, Syncro Soft will provide written certification signed by an authorized representative confirming that Account and Billing Data has been deleted in accordance with this Section 11, except to extent retention is required by law as described in Section 11.3.

11.3 Exceptions to Deletion

Notwithstanding deletion obligations in Sections 11.1 and 11.2, Syncro Soft may retain Account and Billing Data to the extent and for the period required by: applicable laws, regulations, or legal process (Syncro Soft shall limit retention to minimum required by law); legitimate business needs such as retaining billing records for accounting and tax purposes (typically 7 years), records necessary to defend against legal claims, or aggregated anonymized data that cannot be linked back to Customer or any individual; or archival systems (archived logs, system snapshots, disaster recovery systems not readily accessible, deleted within 90-180 days).

Syncro Soft shall maintain records of any Account and Billing Data retained under these exceptions and shall make such records available to Customer upon reasonable request.

11.4 Aggregated and Anonymized Data

Syncro Soft may retain aggregated, anonymized, or de-identified data derived from Account and Billing Data or API Request Metadata that can no longer be attributed to Customer or to any identified or identifiable individual. Such data is not considered Personal Data under Data Protection Law and is not subject to the return or deletion obligations in this Section 11.

Anonymization shall be performed using recognized techniques: removal of all direct identifiers; aggregation to sufficiently large groups; and assessment of re-identification risks.

11.5 Sub-processor, LLM Provider, and Client Application Deletion

Syncro Soft shall ensure that all Sub-processors are contractually obligated to return or delete Account and Billing Data in accordance with this Section 11. Syncro Soft shall take reasonable steps to verify Sub-processor compliance, including obtaining certificates of deletion where appropriate.

For LLM Providers, Syncro Soft cannot ensure deletion of API Request Data because Syncro Soft does not control LLM Provider data retention practices.

For Client Applications, if applications have stored API requests or responses locally, deletion of such locally stored data is the responsibility of the Client Application provider. Customer should contact Client Application providers directly regarding deletion of locally stored data.

11.6 Pending Membership Requests

Upon deletion of an Organization's data or upon termination of the Service Agreement, Syncro Soft shall also delete all Pending Membership Requests associated with that Organization, including email addresses or account information of individuals who accessed invitation links but were never confirmed as members.

12. DATA SUBJECT RIGHTS ASSISTANCE

12.1 Customer's Responsibility for Data Subject Requests

Customer is responsible for responding to requests from Data Subjects seeking to exercise their rights under Data Protection Laws, including: right of access (GDPR Article 15); right to rectification (Article 16); right to erasure/"right to be forgotten" (Article 17); right to restriction of processing (Article 18); right to data portability (Article 20); right to object (Article 21); and rights related to automated decision-making (Article 22).

To the extent U.S. Privacy Laws apply, Syncro Soft shall assist Customer in responding to verifiable consumer requests under the CCPA: right to know/access Personal Information; right to delete Personal Information; right to correct inaccurate Personal Information; and right to opt-out of sale or sharing of Personal Information.

If Syncro Soft receives a Data Subject request directly from a Data Subject regarding Account and Billing Data, Syncro Soft will promptly redirect the Data Subject to Customer and will not respond directly unless required by applicable law or unless Customer has authorized Syncro Soft to respond. Syncro Soft will inform Customer of any such direct requests within 5 business days.

12.2 Syncro Soft's Assistance for Account and Billing Data

Taking into account the nature of the processing, Syncro Soft shall provide reasonable assistance to Customer to enable Customer to respond to Data Subject Requests regarding Account and Billing Data:

- Redirecting Requests: If a Data Subject submits a request directly to Syncro Soft, Syncro Soft will promptly inform Customer within 5 business days, not respond directly except to inform them to contact Customer (unless required by law), and forward the request to Customer.
- Providing Access: Upon Customer's request, Syncro Soft will provide Customer with access to relevant Account and Billing Data. In most cases, Customer can access this data directly through the account portal. For Organization Owners, this includes viewing member lists and Pending Membership Requests.
- Facilitating Rectification: Customer can rectify inaccurate Account and Billing Data directly through the account portal by updating account settings. Syncro Soft will provide technical support if Customer encounters difficulties.
- Facilitating Erasure: Customer can request deletion of Account and Billing Data through the account portal or by contacting Syncro Soft support. Upon request, Syncro Soft will confirm deletion from active systems, confirm deletion from backups (typically within 90 days), and provide written confirmation upon request. For Organization Members, if a member requests

deletion of their data, Syncro Soft will notify the Organization Owner that the member has been removed from the Organization, as this affects the billing relationship.

- Facilitating Data Portability: Syncro Soft provides data export functionality within the account portal enabling Customer to download Account and Billing Data in machine-readable formats (JSON or XML). Upon request, Syncro Soft will provide reasonable assistance if standard export functionality is insufficient.
- Facilitating Restriction: If Customer requests that Syncro Soft restrict processing of specific Account and Billing Data pending resolution of a Data Subject Request, Syncro Soft will work with Customer to implement appropriate restrictions (such as temporarily suspending access to an account). Syncro Soft will only process restricted data as permitted by GDPR Article 18(2).
- Providing Information: Upon Customer's request, Syncro Soft will provide information about processing activities, Sub-processors, security measures, and other details necessary for Customer to respond to Data Subject Requests regarding processing performed by Syncro Soft.

12.3 Severe Limitations for API Request Data

Syncro Soft cannot provide assistance with Data Subject Requests that relate to Personal Data that may have appeared in API Request Data sent to LLM Providers through Client Applications. Because Syncro Soft does not store, log, or retain API Request Data, Syncro Soft:

- Cannot identify whether a particular Data Subject's personal data was included in API requests
- Cannot determine which API requests contained what personal data
- Cannot retrieve or provide copies of API requests that may have contained a Data Subject's personal data
- Cannot delete specific API requests (as API requests are not stored)
- Cannot confirm whether a Data Subject's data was or was not transmitted through the Service

Syncro Soft can only assist with requests related to Account and Billing Data as described in Section 12.2.

Customer's Responsibility for API Request Data: If Client Applications store API requests or responses locally (independent of the Service), Customer is responsible for responding to Data Subject Requests regarding that locally stored data. This is separate from Syncro Soft's obligations under this DPA.

12.4 General Limitations on Assistance

Syncro Soft's assistance obligations under this Section 12 are subject to the following limitations:

- Technical Limitations: Syncro Soft's assistance is limited by the technical capabilities of the Service. Syncro Soft is not obligated to develop new features or functionality to facilitate Data Subject Requests.
- Reasonable Efforts: Syncro Soft will provide assistance using commercially reasonable efforts, but cannot guarantee that all Data Subject Requests can be fully satisfied, particularly for complex or unusual requests.
- Self-Service Tools: In most cases, Customer can respond to Data Subject Requests using self-service tools available in the account portal without requiring Syncro Soft's assistance.
- Time and Resources: For requests requiring significant manual effort or custom development beyond standard Service functionality, Syncro Soft may charge reasonable fees for assistance provided. Syncro Soft will notify Customer of any anticipated fees before performing chargeable work.

13. LIABILITY AND INDEMNIFICATION

13.1 Syncro Soft's Liability to Customer

Syncro Soft's liability to Customer for any breach of this DPA with respect to Account and Billing Data, including unauthorized or unlawful processing, data breaches, failure to implement appropriate security measures, or failure to comply with Customer's lawful instructions, shall be governed by the limitation of liability provisions set forth in the Service Agreement.

Notwithstanding any limitations of liability in the Service Agreement, Syncro Soft shall be liable for damages arising from: Syncro Soft's failure to comply with obligations under Data Protection Law that are specifically directed at processors (such as security requirements under GDPR Article 32); Syncro Soft acting outside or contrary to Customer's lawful instructions regarding Account and Billing Data; or gross negligence or willful misconduct in processing Account and Billing Data.

Limitation for API Request Data and LLM Providers: Syncro Soft's liability does not extend to the processing of API Request Data by LLM Providers or Client Applications, as Syncro Soft does not control such processing. Any claims related to LLM Provider or Client Application processing of API Request Data must be directed to the relevant LLM Provider or Client Application provider.

To the extent that Data Protection Law provides for direct liability of processors to Data Subjects (such as under GDPR Article 82), nothing in this DPA or the Service Agreement shall limit such liability with respect to Account and Billing Data.

13.2 Allocation of Liability Between Parties

Where both Customer and Syncro Soft are liable to Data Subjects for the same damage under Data Protection Law (such as under GDPR Article 82) related to Account and Billing Data:

- Joint and Several Liability: Customer and Syncro Soft shall be jointly and severally liable to the Data Subject for the full amount of the damage.
- Internal Allocation: As between Customer and Syncro Soft, liability shall be allocated: Customer shall be solely liable for damages arising from Customer's own breach or from Customer providing unlawful instructions; Syncro Soft shall be solely liable for damages arising from Syncro Soft's breach or processing outside/contrary to Customer's lawful instructions; and where damage results from acts or omissions of both parties, liability shall be allocated in proportion to each party's degree of fault.
- Right of Recovery: If either party pays more than its proportionate share of damages to a Data Subject, that party shall have a right of recovery against the other party for the excess amount paid.

13.3 Customer's Indemnification of Syncro Soft

Customer shall indemnify, defend, and hold harmless Syncro Soft and its officers, directors, employees, and agents from and against any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising from or relating to:

- Unlawful Instructions: Customer's instructions to Syncro Soft that violate Data Protection Law or the rights of Data Subjects.
- Customer's Data Protection Violations: Customer's own violations of Data Protection Law regarding Account and Billing Data, including processing without lawful basis, failure to obtain necessary consents, failure to comply with transparency obligations, failure to respond appropriately to Data Subject requests, or violation of data minimization or purpose limitation principles.
- API Request Data Violations: Customer's inclusion of Personal Data in API Request Data sent to LLM Providers without a lawful basis or without complying with applicable transparency and consent requirements. Syncro Soft is not responsible for Customer's decisions about what information to include in API requests or which LLM Providers to use.
- Organization Management Violations: For Organization Owners, violations arising from inviting individuals without proper authority or legal basis, or distributing invitation links in a manner that violates Data Protection Law.
- Third-Party Claims: Third-party claims (including claims by Data Subjects) arising from Customer's processing of Personal Data or Customer's use of the Service in violation of Data Protection Law.

This indemnification is subject to Customer receiving prompt written notice, having sole control of defense and settlement (provided Customer may not settle in a manner that admits liability on Syncro Soft's behalf or imposes obligations on Syncro Soft without Syncro Soft's consent), and receiving reasonable cooperation from Syncro Soft (at Customer's expense).

13.4 Syncro Soft's Indemnification of Customer

Syncro Soft shall indemnify, defend, and hold harmless Customer and its officers, directors, employees, and agents from and against any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising from or relating to:

- Syncro Soft's Data Protection Violations: Syncro Soft's breach of this DPA or Data Protection Law with respect to Account and Billing Data, including failure to implement appropriate security measures, unauthorized or unlawful processing, processing outside or contrary to Customer's lawful instructions, failure to assist Customer with Data Subject requests, or unauthorized disclosure.
- Data Breaches: Data breaches affecting Account and Billing Data resulting from Syncro Soft's failure to implement appropriate security measures or from Syncro Soft's gross negligence or willful misconduct.

- Sub-processor Violations: Violations of Data Protection Law by Sub-processors engaged by Syncro Soft for processing Account and Billing Data, except where caused by Customer's instructions or actions.
- Limitation for API Request Data, LLM Providers, and Client Applications: This indemnification does not extend to claims arising from LLM Provider or Client Application processing of API Request Data, as Syncro Soft does not control such processing. Customer assumes responsibility for selecting appropriate LLM Providers and Client Applications and for the consequences of transmitting API Request Data to such providers.

This indemnification is subject to Syncro Soft receiving prompt written notice, having sole control of defense and settlement (provided Syncro Soft may not settle in a manner that admits liability on Customer's behalf or imposes obligations on Customer without Customer's consent), and receiving reasonable cooperation from Customer (at Syncro Soft's expense).

13.5 Limitations on Indemnification

The indemnification obligations in Sections 13.3 and 13.4 do not apply to the extent that the claim arises from: the indemnified party's own breach; the indemnified party's gross negligence or willful misconduct; the indemnified party's failure to mitigate damages; modifications to the Service made by the indemnified party without consent; or combination of the Service with third-party products or services not provided or approved by the indemnifying party, where the claim would not have arisen but for such combination.

13.6 Notification of Regulatory Actions

Each party shall promptly notify the other party of any regulatory investigation, enforcement action, or proceeding by a supervisory authority that relates to the processing of Account and Billing Data under this DPA.

The parties shall cooperate with each other in responding to any such regulatory action: sharing relevant information and documentation (subject to legal and confidentiality restrictions); coordinating responses to supervisory authority inquiries; and jointly developing remediation plans where appropriate.

Neither party shall make any admission of liability or agree to any settlement or consent order with a supervisory authority that would adversely affect the other party without that party's prior written consent (not to be unreasonably withheld).

14. TERM AND TERMINATION

14.1 Term

This DPA shall commence on the Effective Date of the Service Agreement and shall remain in effect for as long as Syncro Soft processes Account and Billing Data on behalf of Customer under the Service Agreement.

14.2 Effect of Agreement Termination

Upon termination or expiration of the Service Agreement, this DPA shall automatically terminate, except that certain provisions shall survive: Section 11 (Return and Deletion of Personal Data) for time necessary to complete return or deletion; Section 13 (Liability and Indemnification) for any claims arising before or as a result of termination; Section 8 (International Data Transfers) for any Account and Billing Data not yet returned or deleted; Section 5.1 (Confidentiality) indefinitely or until Account and Billing Data is returned or deleted; and Section 15 (General Provisions) to extent necessary to give effect to surviving provisions.

Final Processing Activities: Syncro Soft may continue to process Account and Billing Data to extent necessary to: provide Customer with access to retrieve data during retrieval period; complete return of data to Customer if requested; comply with legal obligations requiring retention of data; or establish, exercise, or defend legal claims.

14.3 Termination for Breach of DPA

Either party may terminate this DPA and the Service Agreement immediately upon written notice if the other party materially breaches this DPA and: fails to cure the breach within 30 days of receiving written notice; the breach cannot be cured (such as unauthorized disclosure of Account and Billing Data); or the breach exposes the non-breaching party to material risk of regulatory penalties or liability.

Customer's Right to Terminate: Customer may terminate if Syncro Soft breaches security obligations resulting in a data breach or significant risk regarding Account and Billing Data, processes Account and Billing Data outside or contrary to Customer's instructions, fails to provide assistance required under Section 12, or engages a Sub-processor for Account and Billing Data without proper authorization or notification.

Syncro Soft's Right to Terminate: Syncro Soft may terminate if Customer provides instructions that violate Data Protection Law and refuses to modify such instructions after notice, materially breaches payment obligations, or continuing to process Account and Billing Data would expose Syncro Soft to material legal or regulatory risk.

14.4 Effect of DPA Termination

Upon termination of this DPA: Syncro Soft shall immediately cease all processing of Account and Billing Data except as permitted under Section 11.3; Syncro Soft shall return or delete Account and Billing Data in accordance with Section 11, unless Customer has already retrieved all data during the retrieval period; Syncro Soft shall provide Customer with written certification of deletion as specified in Section 11.2; Syncro Soft shall not make any further use of Account and Billing Data; and Syncro Soft shall instruct all Sub-processors to immediately cease processing and to return or delete Account and Billing Data.

14.5 No Prejudice to Other Rights

Termination of this DPA shall be without prejudice to any other rights or remedies either party may have under the Service Agreement, Data Protection Law, or applicable law, including: right to seek damages for breaches occurring before termination; right to seek injunctive relief to prevent ongoing breaches; obligation to pay outstanding fees or charges; or right of Data Subjects to seek compensation for damages.

15. AMENDMENTS AND UPDATES

15.1 Changes to Data Protection Law

If changes to Data Protection Law require amendments to this DPA to maintain compliance, Syncro Soft may update this DPA by: providing Customer with at least 30 days' advance written notice of the proposed changes; making the updated DPA available at the Service website and in the account portal; and continuing to process Account and Billing Data under the existing DPA during the notice period.

Customer may object to changes by providing written notice within 30 days. If Customer objects on reasonable data protection grounds, the parties shall work together in good faith to reach an agreeable solution. If no solution can be reached, Customer may terminate the Service Agreement in accordance with Section 14.3.

If Customer does not object within 30 days, the updated DPA shall take effect automatically at the end of the notice period.

15.2 Changes Required by Supervisory Authorities

If a supervisory authority requires changes to this DPA as a condition of approving the processing or in response to an investigation or enforcement action, Syncro Soft shall notify Customer and implement the required changes. Such changes shall take effect immediately upon implementation, and Customer's continued use of the Service constitutes acceptance of the changes.

15.3 Updates to Sub-processor and LLM Provider Lists

Updates to the list of Sub-processors for Account and Billing Data shall be made in accordance with Section 6. Updates to the list of available LLM Providers shall be made in accordance with Section 7.

15.4 Administrative Updates

Syncro Soft may make administrative updates to this DPA without prior notice: corrections of typographical errors or formatting; updates to contact information or addresses; clarifications that do not materially change the parties' rights or obligations; or updates to cross-references or defined terms. Such administrative updates shall be posted at the Service website and shall take effect immediately.

16. GENERAL PROVISIONS

16.1 Relationship to Service Agreement

This DPA is incorporated into and forms part of the Service Agreement. In the event of any conflict between the provisions of this DPA and the Service Agreement with respect to the processing of Personal Data, the provisions of this DPA shall control.

16.2 Order of Precedence

In the event of any conflict or inconsistency between the documents that form the Agreement, the following order of precedence shall apply (from highest to lowest): Standard Contractual Clauses (if applicable); this Data Processing Agreement; Service Agreement; other appendices or exhibits; and Privacy Policy and other policies referenced in the agreements.

16.3 Entire Agreement on Data Processing

This DPA, together with the Service Agreement and the Standard Contractual Clauses (if applicable), constitutes the entire agreement between the parties regarding the processing of Personal Data and supersedes all prior agreements, understandings, negotiations, and discussions, whether oral or written, regarding this subject matter.

16.4 Severability

If any provision of this DPA is held to be invalid, illegal, or unenforceable, such provision shall be modified to the minimum extent necessary to make it valid and enforceable while preserving its intent, or if such modification is not possible, such provision shall be severed from this DPA. The remaining provisions shall remain in full force and effect unless such severance would materially alter the balance of rights and obligations.

16.5 No Waiver

No failure or delay by either party in exercising any right or remedy shall constitute a waiver of that right or remedy. Any waiver must be in writing and signed by an authorized representative of the party granting the waiver. A waiver of any breach shall not constitute a waiver of any subsequent breach.

16.6 Third-Party Beneficiaries

Data Subjects as Third-Party Beneficiaries: Data Subjects are third-party beneficiaries of this DPA to the extent necessary to enforce their rights under Data Protection Law with respect to Account and Billing Data, including: right to enforce certain provisions against Syncro Soft (such as security obligations and return/deletion of data); right to enforce Standard Contractual Clauses (if applicable); and right to seek compensation for damages.

No Other Third-Party Rights: Except as provided above for Data Subjects, this DPA does not confer any rights upon any person or entity other than the parties and their permitted successors and assigns.

16.7 Assignment

Neither party may assign, transfer, or delegate this DPA or any rights or obligations without the prior written consent of the other party, except that: Syncro Soft may assign without Customer's consent to an affiliate/subsidiary or in connection with a merger, acquisition, corporate reorganization, or sale of assets (provided assignee agrees in writing to be bound); Customer may assign without Syncro Soft's consent in connection with a merger, acquisition, or corporate reorganization (provided assignee agrees in writing to be bound).

Any attempted assignment in violation of this Section shall be void.

16.8 Notices

All notices, requests, consents, and other communications under this DPA shall be in writing and shall be deemed given when: sent by confirmed email; or sent by registered or certified mail, return receipt requested.

- Notices to Syncro Soft: Syncro Soft SRL, Attention: Data Protection Officer/Legal Department, Email: privacy@oxygenxml.com, Address: Remus 5A, Craiova, 200082, Romania.
- Notices to Customer: To the email address provided by Customer in the Service Account or as subsequently updated in account settings.
- Routine Communications: Routine communications may be provided by email to Customer's account email address, in-Service notifications within the account portal, or posting on Syncro Soft's website or customer portal.

16.9 Governing Law and Jurisdiction

This DPA shall be governed by and construed in accordance with the laws of Romania, without regard to its conflict of law principles, except where the Standard Contractual Clauses (if applicable) specify a different governing law.

Subject to the provisions of the Standard Contractual Clauses (if applicable), any dispute arising out of or relating to this DPA shall be subject to the exclusive jurisdiction of the courts of Bucharest, Romania.

Supervisory Authority: For purposes of Data Protection Law, the competent supervisory authority shall be: for Syncro Soft, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), the Romanian Data Protection Authority; and for Customer, the supervisory authority in Customer's jurisdiction.

16.10 Language

This DPA is executed in English. If this DPA is translated into any other language, the English version shall prevail in the event of any conflict or ambiguity.

16.11 Counterparts and Electronic Signatures

This DPA may be executed in any number of counterparts, each of which shall be deemed an original. This DPA may be executed by electronic signature, which shall be considered as an original signature for all purposes. Electronic acceptance through the Service interface (such as clicking "I Accept" during account setup) shall constitute valid execution of this DPA.

16.12 Survival

The provisions of this DPA that by their nature should survive termination or expiration shall survive, including: Section 5.1 (Confidentiality); Section 11 (Return and Deletion of Personal Data); Section 13 (Liability and Indemnification); and Section 16 (General Provisions).

16.13 Force Majeure

Neither party shall be liable for any failure or delay in performing its obligations under this DPA (except for payment obligations) to the extent such failure or delay is caused by circumstances beyond its reasonable control.

The party affected by a force majeure event shall: notify the other party promptly; use reasonable efforts to mitigate the effects; and resume performance as soon as reasonably practicable.

If a force majeure event continues for more than 60 days, either party may terminate this DPA and the Service Agreement upon written notice.

16.14 Compliance with Laws

Each party shall comply with all applicable laws and regulations in performing its obligations under this DPA.

17. CONTACT INFORMATION

For all matters relating to this DPA, including Data Subject requests, data breaches, audits, and general data protection inquiries, please contact:

Syncro Soft SRL - Data Protection Team

- General Email (Audit Requests, DPA Questions): privacy@oxygenxml.com
- Data Breach Notifications: security@oxygenxml.com
- Postal Address: Syncro Soft SRL, Attention: Data Protection/Privacy, Remus 5A, Craiova, 200082, Romania

ANNEXES TO DPA

The following annexes form part of this Data Processing Agreement and provide the information required by the Standard Contractual Clauses:

- **ANNEX I:** DETAILS OF PROCESSING
- **ANNEX II:** TECHNICAL AND ORGANIZATIONAL MEASURES
- **ANNEX III:** LIST OF SUBPROCESSORS AND LLM PROVIDERS

ANNEX I: DETAILS OF PROCESSING

This Annex I forms part of the Data Processing Agreement, corresponds to Annex I of the **Standard Contractual Clauses** and provides details about the parties, the nature and purpose of the processing, and the categories of Personal Data and Data Subjects.

A. LIST OF PARTIES

Data Exporter (Customer):

- Name: Customer's entity name as identified in the Agreement
- Address: Customer's address as specified in the Agreement
- Contact person: Customer's contact details as specified in the Agreement
- Email: Customer's email as identified in the Agreement
- Signature and date: These Clauses shall be deemed executed and entered into by Customer as of the DPA Effective Date.
- Role: Data Controller

Data Importer (Processor):

- Name: Syncro Soft SRL
- Address: Remus 5A, Craiova, 200082, Romania
- Contact person: Data Protection Officer / Privacy Team
- Email:privacy@oxygenxml.com
- Signature and date: These Clauses shall be deemed executed and entered into by Syncro Soft as of the DPA Effective Date.
- Role: Data Processor

B. DESCRIPTION OF TRANSFER

1. Subject Matter of Processing

The subject matter of processing is the provision of the Oxygen AI Positron Service, which is an API-based backend service that enables Client Applications (primarily Oxygen family products through dedicated plugins) to access multiple Large Language Model providers through a unified, authenticated interface with centralized account management and billing.

The Service provides users with the ability to authenticate once through OAuth providers and then access multiple LLM providers through various Client Applications without establishing separate commercial relationships with each LLM provider. For organizations, the Service

enables centralized billing where an Organization Owner pays for API usage credits consumed by all confirmed members of the organization.

2. Duration of Processing

Processing of Account and Billing Data will continue for the duration of the Service Agreement between Syncro Soft and Customer, plus any retention period required by law or as necessary to complete return or deletion obligations following termination.

API Request Data is transmitted in real-time through the Service infrastructure to selected LLM Providers without any storage or retention.

3. Nature and Purpose of Processing

The nature and purpose of processing is divided into two fundamentally distinct categories that reflect the Service's architecture and data flows:

1. **Persistent Processing of Account and Billing Data**

   Nature of Processing: Storage, organization, retrieval, and management of user account information, Organization membership data, API access credentials, and billing information.

   Purposes of Processing:

   - User authentication is performed via OAuth integration , allowing users to create accounts without establishing separate passwords specifically for the Service.
   - Account management encompasses maintaining user profile information, tracking account status (active, suspended, terminated), managing user preferences and settings configured through the account portal, and providing users with access to view and modify their account information.
   - Organization and team management for centralized billing involves enabling users to create Organizations, generate generic invitation links that can be distributed to intended members, processing Pending Membership Requests when individuals access invitation links, allowing Organization Owners to confirm or reject membership requests, maintaining records of Organization membership (which users belong to which Organizations and in what role), and facilitating the billing relationship where Organization Owners pay for credits consumed by all confirmed members.
   - API access control and authentication includes generating and managing API authentication tokens that Client Applications use to make authenticated requests to the Service, validating authentication credentials on each API request to ensure only authorized users can access LLM providers through the Service, tracking API usage and enforcing rate limits and usage quotas based on subscription tiers.

- Billing and payment processing encompasses subscription payments, tracking credit consumption through API usage (based on metadata about API requests such as which LLM provider was used and request/response sizes)
- Service communications involve sending account-related emails including account creation confirmations and welcome messages, password reset links (for users who establish passwords in addition to OAuth), notification emails when credit balance is low, billing notifications including payment confirmations and failed payment alerts, security alerts if suspicious activity is detected, and administrative communications about service updates or policy changes.
- Technical support and troubleshooting includes maintaining support ticket history, processing support requests related to account issues or billing questions, and providing users with information about their API usage patterns to help optimize their use of the Service.
- Compliance with legal obligations encompasses retaining records as required by applicable laws (such as financial records for tax purposes), responding to valid legal process (such as subpoenas or court orders), and cooperating with law enforcement when legally required.
- Fraud prevention and security monitoring involves detecting and preventing unauthorized account access, and maintaining audit logs of administrative actions for security investigations.

2. **Real-Time Transmission of API Request Data (No Storage)**

   Nature of Processing: Stateless routing and transmission of encrypted API requests from authenticated Client Applications to selected LLM Provider APIs, with responses returned to the requesting Client Application.

   Purpose of Processing:

   - The sole purpose is to provide technical infrastructure that enables Client Applications to send authenticated API requests to multiple LLM providers without requiring users to establish separate accounts, or handle separate billing relationships with each LLM provider. The Service acts as an authenticated gateway that validates the user has an active account with sufficient credits, routes the request to the appropriate LLM provider, and returns the response to the requesting Client Application.
   - The Service performs authentication validation by checking that the API authentication token included in the request corresponds to an active user account, credit availability validation by confirming the user has sufficient credits to cover the anticipated cost of the API request based on the selected LLM provider's pricing, request routing by forwarding the authenticated request to the selected

LLM provider's API endpoint using Syncro Soft's established API integration with that provider, and response return by receiving the LLM provider's response and transmitting it back to the Client Application that made the original request.

Crucially, throughout this entire process, the Service does not inspect, analyze, log, or store the content of API requests or responses. The Service infrastructure is architecturally designed to be stateless, meaning servers process requests without maintaining any session state or data between requests.

4. Types of Personal Data Processed

The types of Personal Data processed are strictly limited and clearly defined based on the two categories of processing:

1. **Account and Billing Data (Stored Persistently)**
    - User identification information includes full name of user as provided by their OAuth provider, email address and avatar picture of user as provided by their OAuth provider, and OAuth provider identifier which is a unique identifier assigned by Google or GitHub to the user's account that allows Syncro Soft to associate the OAuth authentication with the user's account in the Service.
    - Account metadata includes account creation date and IP recording when the user first created their account, last login date tracking when the user most recently authenticated to the Service, account status indicating whether the account is active, suspended, or terminated, and subscription tier information showing which plan the user has subscribed to.
    - Organization and membership information includes Organization name chosen by the Organization Owner when creating the Organization, Organization creation date, Organization membership records showing which users belong to which Organizations, user roles within Organizations indicating whether each user is the Organization Owner or a regular Member, Pending Membership Request data containing email addresses and account information for individuals who have accessed invitation links but have not yet been confirmed as members by the Organization Owner, and invitation link metadata tracking when invitation links were generated and which links have been accessed.
    - Billing and payment information includes payment method details stored securely by payment processors in compliance with PCI-DSS standards
    - API access credentials include API authentication tokens generated by the Service that Client Applications use to authenticate requests, token expiration dates and refresh policies, and API key identifiers that allow tracking of which Client Application made which requests for troubleshooting purposes.

- Service usage preferences include default LLM provider selection if the user has configured a preferred provider, API request preferences such as timeout settings or response format preferences, and notification preferences indicating which types of email notifications the user wishes to receive.
- Support and communication records include support ticket content and history when users contact customer support, email communication history of service-related emails sent to and received from users, and notes or records created by support staff during the resolution of support issues.

2. **API Request Metadata (Collected but Not Including Content)**

   While the Service does not collect, store, or retain the content of API requests or responses, the Service does collect metadata about API requests for billing verification, service performance monitoring, and technical troubleshooting. This metadata includes timestamp of when the API request was received by the Service, user account identifier which is an internal database ID (not the user's name or email) that allows associating the request with the correct account for billing purposes, Organization identifier if the user is part of an Organization to enable proper billing to the Organization Owner, selected LLM provider indicating which LLM provider the request was routed to, Client Application identifier and version information showing which Client Application and which version of that application made the request, request payload size in bytes (but absolutely not the actual content of the request), response payload size in bytes (but absolutely not the actual content of the response), API response time and latency measurements for performance monitoring, HTTP status codes indicating whether the request succeeded or failed, error codes and error types if the request failed (for example timeout errors, authentication errors, or LLM provider errors), and number of credits consumed calculated based on the LLM provider's pricing model and the request and response sizes.

5 Categories of Data Subjects

The categories of Data Subjects whose Personal Data is processed through the Service include several distinct groups, each with different relationships to the Service and different types of data processed:

- **Individual Users of the Service.** Individual users are persons who create accounts at the Oxygen AI Positron Service These users access AI functionality through Client Applications such as Oxygen AI Positron plugins that integrate with the Service via API. Individual users pay for their own API usage through subscriptions and are not part of any Organization.
- **Organization Owners and Administrators.** Organization Owners are individual users who have created Organizations for the purpose of centralized billing. In addition to having individual user accounts, Organization Owners have administrative capabilities including the ability to generate invitation links, review and confirm or reject Pending Membership

Requests, view the list of confirmed Organization Members, and manage billing for all members of their Organization.

- **Organization Members.** Organization Members are individual users who have been invited to and confirmed as members of an Organization. Organization Members access the Service through Client Applications just like individual users, but their API usage is billed to the Organization Owner rather than to themselves personally.
- **Individuals with Pending Membership Requests.** These are persons who have accessed a generic Organization invitation link and have either created a new account or logged into an existing account, thereby generating a Pending Membership Request that awaits confirmation by the Organization Owner. These individuals are not yet Organization Members and do not have access to the benefits of Organization membership.
- **Individuals Whose Personal Data May Appear in API Requests.** When users of the Service use AI features through Client Applications to process documents or content, that content may contain Personal Data about individuals other than the user themselves. Syncro Soft has no way of knowing whose Personal Data may appear in API requests because the Service does not store or inspect the content of API requests. These individuals are Data Subjects only in the sense that their Personal Data may be transmitted through the Service to LLM Providers, but Syncro Soft has no direct relationship with these individuals and processes their data only as a technical conduit. The primary data protection obligations toward these individuals rest with the Customer (who decides what content to include in API requests) and with the LLM Providers (who actually process the content).

6. Special Categories of Data

Customer shall not include Special Categories of Personal Data as defined in GDPR Article 9 in Account and Billing Data without prior written notice to and consent from Syncro Soft. The standard use of the Service for account creation and billing purposes should not involve Special Categories of Personal Data.

For API Request Data, Syncro Soft has no knowledge of or control over whether users include Special Categories of Personal Data in their API requests to LLM Providers. Customer is solely responsible for ensuring compliance with applicable laws if Customer includes Special Categories of Personal Data in API requests sent through Client Applications to LLM Providers.

7 Processing Operations

The specific processing operations performed by Syncro Soft vary depending on which category of data is being processed:

1. **For Account and Billing Data (Persistent Processing):** collection of data from OAuth Providers during authentication; storage in secure databases with encryption at rest; organization and structuring for account management and billing purposes; retrieval and

consultation to provide Service functionality; transmission to Sub-processors for specific purposes such as payment processing; regular backup and disaster recovery operations; deletion upon termination or at Customer's request; and aggregation and anonymization for service improvement analytics.

2. **For API Request Data (Real-Time Transmission Without Storage)**: Processing Flow:
    - Reception & Authentication: HTTPS requests are received, authenticated, and validated against the user's active account.
    - Credit Check: The request's estimated cost is calculated and temporarily reserved to ensure sufficient user credits.
    - Routing & Transmission: The request is forwarded to the selected LLM provider via encrypted HTTPS connections.
    - Response & Return: The LLM's response is received, actual cost is deducted from the user's balance, metadata is logged, and the response is returned to the client.

    Throughout this entire process, the content of requests and responses is never written to disk, stored in databases, logged, or cached. Data exists only transiently in server memory during active processing and is immediately purged upon request completion.

C. COMPETENT SUPERVISORY AUTHORITY

For Customer: The supervisory authority in Customer's jurisdiction as determined by GDPR Article 55 (establishment) or Article 56 (lead supervisory authority).

For Processor: Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) - the Romanian Data Protection Authority.

ANNEX II: TECHNICAL AND ORGANIZATIONAL MEASURES

This Annex II forms part of the Data Processing Agreement, corresponds to Annex II of the **Standard Contractual Clauses** and describes the technical and organizational security measures implemented by Syncro Soft to protect Personal Data processed under this DPA.

Customer acknowledges that these measures are subject to technical progress and development, and Syncro Soft may update or modify them from time to time, provided that such updates or modifications do not result in a material degradation of the overall security of the Service.

A. Security Measures for Account and Billing Data (Stored Data)

These measures apply to Personal Data that Syncro Soft stores persistently, including user account information, Organization membership data, and billing information.

- **Measures of Pseudonymization and Encryption**
  - Encryption at rest using AES-256 or equivalent encryption algorithms for all Personal Data stored in databases.
  - Encrypted backups with separate key management, ensuring backup data is protected with the same level of encryption as production data.
  - Database-level encryption with keys managed through a secure key management system with role-based access controls.
  - Encryption of sensitive fields within databases, including OAuth tokens if stored.
  - Hashing of passwords and sensitive credentials using industry-standard algorithms such as bcrypt or Argon2.
  - Transport layer encryption using TLS 1.2 or higher for all data in transit between systems and Sub-processors.
- **Measures for Ensuring Ongoing Confidentiality, Integrity, Availability, and Resilience**
  - Role-based access control (RBAC) limiting access to Account and Billing Data based on job function and need-to-know principles.
  - Multi-factor authentication required for all administrative access to production systems.
  - Regular review and audit of access permissions, with automated alerts for unusual access patterns.
  - Segregation of duties ensuring no single individual has complete control over critical security functions.
  - Redundant systems and infrastructure to ensure high availability and resilience against hardware failures.
  - Geographic distribution of data centers to protect against localized disasters.

- Regular security patching and updates of all systems, with critical security patches applied within 30 days of release.
- Intrusion detection and prevention systems (IDS/IPS) monitoring for malicious activity.
- Network segmentation isolating production systems from development and corporate networks.
- Anti-malware and anti-virus protection on all servers and workstations.

- **Measures for Ensuring the Ability to Restore Availability and Access to Personal Data**
  - Automated daily backups of all Account and Billing Data with retention for at least 30 days.
  - Encrypted backup storage in geographically separate locations from primary data centers.
  - Regular testing of backup restoration procedures, with documented recovery time objectives (RTO) and recovery point objectives (RPO).
  - Disaster recovery plan with defined procedures for recovering from various types of incidents.
  - Redundant infrastructure allowing for failover to backup systems with minimal downtime.
  - Point-in-time recovery capabilities allowing restoration of data to specific timestamps if needed.
- **Processes for Regularly Testing, Assessing, and Evaluating Effectiveness**
  - Annual third-party security assessments and penetration testing by qualified security firms.
  - Regular vulnerability scanning of all internet-facing systems and critical internal systems.
  - Security audits of access logs and system configurations on a quarterly basis.
  - Incident response drills and tabletop exercises to test security incident procedures.
  - Annual review of this DPA and security documentation to ensure continued compliance with Data Protection Laws.
  - Compliance certifications such as ISO 27001 maintained and renewed regularly (where applicable).
- **Measures for User Identification and Authorization**
  - OAuth 2.0 authentication through trusted providers (Google and GitHub) with secure token validation.
  - Session management with secure session tokens, automatic timeout after periods of inactivity, and secure session termination procedures.
  - Audit logging of all authentication events and privileged operations.

    - Separation of user data ensuring users can only access their own account information and Organizations they belong to.
    - Organization Owner privileges validated before allowing access to member information or billing controls.
- **Measures for the Protection of Data During Transmission**
    - All data transmitted over public networks encrypted using TLS 1.3 or higher.
    - Certificate pinning or validation to prevent man-in-the-middle attacks.
    - Secure API authentication using encrypted API keys or OAuth tokens.
    - VPN or other secure channels used for administrative access to systems.
- **Measures for the Protection of Data During Storage**
    - Secure data centers with physical security controls including access badges, surveillance cameras, and security personnel.
    - Environmental controls (temperature, humidity, fire suppression) to protect hardware.
    - Secure disposal procedures for hardware, including physical destruction or cryptographic erasure of storage media before decommissioning.
- **Measures for Ensuring Physical Security**
    - Data centers certified to industry standards such as ISO 27001 or SOC 2.
    - 24/7 monitoring and security personnel at data center facilities.
    - Biometric or multi-factor access controls for entry to server rooms.
    - Video surveillance with recorded footage retained for security review.
    - Visitor logs and escort requirements for non-employees entering secure areas.
- **Measures for Ensuring Incident Management**
    - Security incident response plan defining roles, responsibilities, and procedures for responding to security incidents.
    - 24/7 security monitoring and incident response capability for critical security incidents.
    - Incident classification system prioritizing incidents based on severity and impact.
    - Documented procedures for notification to affected customers and supervisory authorities as required by Data Protection Laws.
    - Post-incident review and lessons learned process to improve security measures.
    - Forensic analysis capabilities to investigate security incidents and identify root causes.
- **Measures for Ensuring Business Continuity**
    - Business continuity plan addressing recovery from various disaster scenarios.
    - Regular testing of business continuity procedures with documented results.
    - Redundant infrastructure and failover capabilities for critical systems.
    - Backup power systems (generators, UPS) at data centers to ensure continued operation during power outages.
- **Measures for Ensuring Compliance**

- Designated privacy contact responsible for overseeing data protection compliance.
- Privacy by design principles integrated into system development processes.
- Regular training for employees on data protection obligations and security best practices.
- Documentation of processing activities as required by GDPR Article 30.

B. Security Measures for API Request Data Transmission

These measures apply to API Request Data that is transmitted through the Service to LLM Providers. Because this data is not stored, security measures focus on protecting data during transmission and preventing any possibility of storage, interception, or inspection.

- **Encryption During Transmission.** All API requests are encrypted using TLS 1.3 or higher during transmission from Client Applications to Service API endpoints, from Service to LLM Provider APIs, and for responses returned through the same path. Perfect forward secrecy ensures that compromise of long-term keys does not compromise past session keys. Certificate validation ensures encrypted connections are established only with legitimate servers.
- **Stateless Architecture Preventing Storage.** Stateless HTTP request handling ensures no session data persists between requests. No application-level caching or buffering of request content occurs at any layer of the infrastructure. Memory is cleared immediately after each request is processed using explicit memory management to prevent residual data. Containerized or isolated execution environments for processing requests prevent cross-contamination between user sessions. No debugging or diagnostic logging of request content in production systems ensures that request content cannot inadvertently be captured in logs.
- **Absence of Logging and Storage Mechanisms.** Application logs are explicitly configured to exclude request and response content, logging only metadata such as timestamps, user identifiers, request sizes, and status codes. Network logs capture connection information without packet inspection or content logging. No debugging tools that could capture request content are enabled in production environments. Monitoring systems track only aggregate metrics and performance data without accessing individual request content.
- **Network Isolation** Network-level isolation between user sessions prevents any possibility of requests from one user being visible to another user. Dedicated network paths for request transmission with no intermingling of traffic. Firewall rules restrict communication to only necessary endpoints (Client Applications and LLM Provider APIs). Rate limiting and traffic shaping operate on connection-level metadata without inspecting content.
- **Secure API Authentication with LLM Providers** API credentials for authenticating with LLM Providers are stored encrypted and accessed only by authorized service components.

- **Access Controls Preventing Inspection** Service architecture is designed such that personnel have no technical ability to intercept or view request content during transmission. Administrative access to request transmission infrastructure is restricted to essential personnel and comprehensively logged.
- **Security Monitoring Without Content Inspection.** Anomaly detection for unusual usage patterns uses only metadata analysis (request frequencies, sizes, error rates) without inspecting content. Automated blocking of malicious traffic patterns operates on connection-level indicators, not content. Security alerts are triggered by metadata anomalies such as excessive request rates or unusual destination patterns.

C. OAuth Authentication Security Measures

These measures apply to the OAuth authentication process through which users create accounts and authenticate to the Service.

- **OAuth Protocol Security**
  - Implementation of OAuth 2.0 standard with all required security features.
  - State parameter validation to prevent CSRF attacks during OAuth flow.
  - Nonce validation in OpenID Connect flows to prevent replay attacks.
- **Token Management**
  - Secure storage of OAuth access tokens and refresh tokens (if applicable) with encryption at rest.
  - Short expiration times for access tokens, requiring regular token refresh.
  - Revocation of tokens immediately when a user logs out or when suspicious activity is detected.
  - No storage of OAuth tokens in client-side cookies or local storage without appropriate security measures.
- **OAuth Provider Verification**
  - Validation of OAuth provider identity to ensure users are authenticating with legitimate Google or GitHub services.
  - Monitoring for OAuth-related vulnerabilities and prompt patching when vulnerabilities are disclosed.
- **Scope Limitation**

- Requesting only the minimum OAuth scopes necessary (typically profile information and email address).
- Clear disclosure to users of what information is being requested during OAuth consent.
- No request for excessive permissions beyond what is needed for account creation and authentication.

D. Organizational Measures

These organizational measures complement the technical measures described above.

- **Security Policies and Procedures**
  - Comprehensive information security policy covering all aspects of data protection and security.
  - Acceptable use policy for employees governing use of corporate systems and access to Personal Data.
  - Incident response policy and procedures, regularly updated and tested.
  - Data retention and deletion policy aligned with this DPA and applicable laws.
- **Personnel Security**
  - Background checks conducted for employees with access to Personal Data, to the extent permitted by applicable law.
  - Confidentiality agreements signed by all employees, contractors, and consultants with access to Personal Data.
  - Security awareness training provided to all employees upon hire and at least annually thereafter.
  - Specialized data protection training for employees who regularly handle Personal Data.
  - Role-based access provisioning ensuring employees have access only to the data necessary for their job functions.
  - Prompt deprovisioning of access when employees leave the company or change roles.
- **Vendor Management**
  - Due diligence conducted on all Sub-processors before engagement, including review of security practices and certifications.
  - Contractual requirements for Sub-processors to implement security measures equivalent to those described in this Annex.
  - Regular review of Sub-processor security practices and compliance with contractual obligations.
- **Compliance and Audit**

    - Annual internal audits of security controls and data protection practices.
    - Third-party audits and certifications (such as ISO 27001) where applicable.
    - Regular reviews of this Annex to ensure security measures remain appropriate given evolving threats and technologies.
    - Documentation of all security incidents and remediation actions taken.
- **Data Protection Governance**
    - Designated privacy contact responsible for overseeing data protection compliance.
    - Privacy committee or working group meeting regularly to address data protection issues.
    - Privacy impact assessments conducted for new processing activities or significant changes to existing processing.
    - Regular reporting to management on data protection compliance and security metrics.

E. Update and Improvement of Security Measures

Syncro Soft is committed to continually improving security measures in response to:

- Evolving threat landscape and new attack vectors.
- Technological advances that enable enhanced security controls.
- Feedback from security audits, penetration tests, and security incidents.
- Changes in Data Protection Laws or guidance from supervisory authorities.
- Best practices and standards from industry organizations and security frameworks.

Syncro Soft will notify Customer of any material changes to security measures that enhance data protection. If any changes result in a material degradation of security, Syncro Soft will obtain Customer's consent before implementing such changes or will provide alternative security measures that maintain an equivalent level of protection.

ANNEX III: LIST OF SUBPROCESSORS

This Annex III forms part of the Data Processing Agreement, corresponds to Annex III of the Standard Contractual Clauses and lists the Sub-processors engaged by Syncro Soft to process Account and Billing Data, as well as the LLM Providers available through the Service for processing API Request Data.

Customer hereby provides general authorization for Processor to engage Subprocessors in accordance with Section 6 of this DPA, subject to the notification and objection procedures specified therein.

A. Sub-processors for Account and Billing Data

The list of Sub-processors engaged by Syncro Soft to process Account and Billing Data is available at:

Subprocessor List

This list forms an integral part of this Annex III. Changes to this list are subject to the notification and objection procedures set forth in Section 6 of the DPA.

B. LLM Providers (Not Sub-processors)

IMPORTANT: These entities are independent controllers for API Request Data transmitted through the Service.

The list of LLM Providers available through the Service is available at:

LLM Providers List

They are NOT Sub-processors under this DPA. Users (through Client Applications) select which LLM Provider to use for each API request, and API Request Data is transmitted directly to the selected provider. Changes to this list are subject to the notification procedures set forth in Section 7 of the DPA but do NOT trigger objection or termination rights.

Note for Customers:

- The above list represents LLM Providers currently available or planned to be available through the Service. Before configuring Client Applications to use any LLM Provider, Customer should review that provider's privacy policy, terms of service, and data processing practices to ensure they are acceptable for Customer's intended use. Syncro Soft provides this information for Customer's convenience but does not control or warrant LLM Provider practices.

- Customer acknowledges that selection of an LLM Provider (through Client Application configuration) constitutes an instruction to transmit API Request Data to that provider's jurisdiction and infrastructure. Customer is responsible for assessing whether such transmission complies with applicable Data Protection Laws for Customer's specific use case.
- Unlike Sub-processors listed in Section A above (who process Account and Billing Data on Syncro Soft's behalf as data processors), LLM Providers process API Request Data as independent controllers or under their own processor agreements with users.

C. Client Application Providers (Independent Controllers)

While not Sub-processors under this DPA, Client Application providers are independent data controllers for processing that occurs within their applications. For transparency, the following Client Applications integrate with the Service:

1. Syncro Soft SRL - Oxygen AI Positron for Desktop Plugin
    - Purpose: Provides AI-powered features within the Oxygen XML Editor application
    - Data Processing: The plugin processes user documents and actions to generate API requests sent to the Service
    - Privacy Policy: [Oxygen XML Editor Privacy Policy URL - separate from this DPA]

    Note: Although provided by Syncro Soft, the Oxygen AI Positron for Desktop plugin is governed by a separate privacy policy because they process data differently and for different purposes than the Service.

2. Syncro Soft SRL - Oxygen Positron for Content Fusion Plugin
    - Purpose: Provides AI-powered features within the Oxygen Content Fusion collaborative platform
    - Data Processing: The plugin processes collaborative documents and review workflows to generate API requests sent to the Service
    - Privacy Policy: [Oxygen Content Fusion Privacy Policy URL - separate from this DPA]

    Note: Although provided by Syncro Soft, the Oxygen AI Positron for Content Fusion plugin is governed by a separate privacy policy

[Additional authorized Client Applications to be listed as integrations are developed]

Customer Responsibility: Customer should review the privacy policy of each Client Application used to access the Service, as each application may have its own data collection, storage, and processing practices independent of the Service.

D. Updates to This Annex

This Annex may be updated from time to time:

1. Updates to Sub-processors for Account and Billing Data (Section A) will be made in accordance with Section 6 of the DPA, with 30 days' advance notice and objection rights for Customer.
2. Updates to LLM Providers (Section B) will be made in accordance with Section 7 of the DPA, with notice to users but no objection rights (Customer simply chooses which providers to configure in Client Applications).
3. Updates to Client Application providers (Section C) are for informational purposes only, as these are independent controllers not subject to this DPA.