DATA PROCESSING AGREEMENT

Last updated January 15, 2025

1. DEFINITIONS AND INTERPRETATION

This Data Processing Agreement ("DPA") is entered into between Foxtery S.L. ("Processor", "we", "us", or "our"), a company registered in Spain at Calle Marc Aureli 10, Barcelona, Barcelona 08006, and the Corporate Customer ("Controller", "you", or "your"). This DPA is incorporated into and forms part of the Agreement between the parties and reflects the parties' agreement with regard to the Processing of Personal Data.

This DPA applies to all activities where we process Personal Data on your behalf in the course of providing our AI-powered corporate learning platform and related services ("Services"). By using our Services, you acknowledge that you are entering into this DPA and agree to be bound by its terms.

Throughout this DPA, we use certain words and phrases with specific meanings. These definitions align with our Privacy Policy and Terms of Service while providing additional precision necessary for data processing operations.

Key Terms and Definitions:

The term "Agreement" refers to the main service agreement between us, including the Terms of Service available at [https://foxtery.com/policies/terms-of-service] and any other incorporated documents. "Applicable Data Protection Laws" encompasses the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the Spanish Organic Law 3/2018 on Personal Data Protection and Digital Rights Guarantee, and any other applicable data protection or privacy laws and regulations.

"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. For the purposes of this DPA, you, as our Corporate Customer, act as the Controller of Personal Data you provide to us or authorize us to collect.

"Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller. For the purposes of this DPA, Foxtery acts as the Processor of Personal Data under your instructions.

"Processing" means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means. This includes but is not limited to collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure, and destruction of data.

"Personal Data" means any information relating to an identified or identifiable natural person ("Data Subject"). This includes any information that can directly or indirectly identify someone, such as names, identification numbers, location data, online identifiers, or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.

"Customer Data" means all data, including Personal Data, that you provide to us or upload to our Services in connection with your use of the Services. This includes user account information, configuration settings, and any other data you input or upload to the Services.

"Training Materials" means any content, documentation, or materials that you provide to us or upload to our Services for the purpose of creating or generating learning content, including but not limited to corporate documents, training manuals, educational resources, and related materials used as input for our AI-powered content generation features.

"AI Processing" specifically refers to any automated processing of Personal Data using our artificial intelligence technologies, including machine learning algorithms, natural language processing, and automated content generation.

"Learning Data" encompasses all data related to user interaction with educational content, including progress tracking, completion rates, assessment results, and performance metrics.

A "Personal Data Breach" means any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

"Sub-processor" refers to any data processor we engage who agrees to receive Personal Data from us for Processing activities carried out on your behalf.

Document Interpretation:

Any reference to specific legal frameworks or legislation includes reference to modifications, amendments, and subordinate legislation. When we use terms like "including," "include," "in particular," or "for example," these are illustrative and don't limit the meaning of the preceding words.

Terms such as "commission," "data subject," "member state," "supervisory authority," and any other terms defined in Article 4 of the GDPR carry the same meaning as defined therein. All terms related to data protection should be interpreted in accordance with the GDPR and other Applicable Data Protection Laws.

Legal Hierarchy:

In case of any conflict or inconsistency between this DPA, our Privacy Policy, Terms of Service, or any other agreement between us, the documents will take precedence in the following order: (1) this DPA, (2) the Terms of Service, (3) the Privacy Policy, and (4) any other agreement. This ensures that data protection requirements receive the highest priority in our business relationship.

2. SCOPE AND PURPOSE

This DPA covers all processing activities undertaken by us in providing our AI-powered corporate learning platform and related services. We process your personal data strictly in accordance with your instructions and only for the purposes described in this Agreement or as otherwise agreed in writing.

Nature and Subject Matter of Processing

Our platform enables user authentication and account management, content generation and delivery (including AI-powered content), progress tracking and assessment, learning analytics, and related functionalities. The nature of our processing includes collection, storage, retrieval, use, analysis, and, where requested, anonymization or pseudonymization of personal data necessary to deliver and improve these services.

Categories of Data and Data Subjects

1. Account and Profile Data (e.g., names, emails, job titles) for identifying and managing user accounts.
2. Platform Usage Data (e.g., login records, feature usage patterns) for service delivery, security, and analytics.
3. Learning Data (e.g., course progress, assessment results, completion rates) related to user interaction with educational content.
4. Training Materials (e.g., documents, manuals, resources) which may contain personal data from third parties if provided by you.

Data subjects primarily include your employees, contractors, or other authorized personnel; in some cases, this may extend to individuals (e.g., clients) whose data appears in uploaded materials.

Purposes of Processing

We process personal data to operate and maintain the platform's core functions, such as:

- Managing user authentication and permissions
- Delivering AI-generated or customized learning content
- Tracking learning performance and enabling reports or certificates
- Ensuring the security, stability, and optimization of the platform

We also process data to comply with legal requirements (e.g., fraud prevention, fulfilling supervisory authority requests) and to fulfill our contractual obligations. We do **not** use personal data for any secondary purposes unrelated to these services (including our own marketing) without your explicit authorization.

Data Minimization and Duration

We adhere to the principle of data minimization, collecting and processing only the personal data necessary for the stated purposes. The duration of processing generally corresponds to the term of our main service agreement, unless otherwise required by law or agreed upon in writing.

Transparency and Control

We strive to maintain clarity about how personal data is processed within our platform. You may contact us in writing if you require specific configurations or requests related to data handling or retention.

We maintain internal transaction logs and documentation regarding key processing activities for troubleshooting and compliance purposes. We may share relevant information upon request to help you verify our adherence to applicable data protection requirements.

3. TERRITORIAL SCOPE

This DPA applies to the processing of personal data in the context of our activities regardless of whether the processing takes place in the European Union or not. Specifically, this DPA applies to:

Processing of personal data in the context of the activities of our establishment in the European Union. Our primary establishment is located in Spain, and we maintain data processing operations in Germany.

Processing of personal data of data subjects who are in the European Union, where the processing activities relate to the offering of our Services to these data subjects or the monitoring of their behavior within the European Union.

Processing of personal data of data subjects located outside the European Union, where such processing is subject to European Union data protection law by virtue of public international law.

For customers established in the European Union, we process and store personal data primarily within the European Union. Any transfer of personal data outside the European Union is conducted in accordance with Chapter V of the GDPR and as detailed in Section 7 (International Data Transfers) of this DPA.

For customers established outside the European Union, we may process and store their data in data centers located in their region or in the European Union, depending on specific requirements and agreements. In all cases, we maintain appropriate safeguards for the protection of personal data as required by applicable data protection laws.

When providing our Services to customers who process personal data subject to other regional or national data protection laws, including but not limited to the UK GDPR, Swiss Federal Data Protection Act, or other applicable laws, we comply with the specific requirements of those laws as they apply to our role as a data processor.

4. OBLIGATIONS OF THE DATA CONTROLLER

As the Data Controller, you retain primary responsibility for lawfully collecting and determining the purposes and means of processing personal data within our platform. In particular, you agree to:

1. Lawful Basis and Instructions
    - Ensure that all personal data you provide to us, or allow us to collect on your behalf, is processed under a valid legal basis (e.g., consent, contract, legitimate interests).
    - Provide clear, documented instructions for processing activities through your account settings, our admin interface, or other written communication channels.
    - Promptly inform us if any instruction might conflict with applicable data protection laws.
2. Rights and Permissions
    - Obtain all necessary rights, authorizations, and consents for any personal data included in Training Materials or otherwise uploaded to the platform.
    - Verify that data subjects are properly informed and have consented to (or are otherwise

lawfully subject to) the processing within our AI features, where applicable.

3. Data Accuracy and Quality
   - Maintain the accuracy and quality of personal data by updating records when changes occur.
   - Ensure that any third-party personal data in uploaded materials complies with data protection principles such as accuracy, fairness, and minimality.
4. Responding to Data Subject Requests
   - Serve as the primary contact for data subjects exercising their rights (e.g., access, rectification, erasure).
   - Handle such requests in accordance with relevant laws, with our reasonable cooperation.
   - Promptly provide us with documented instructions when you need our assistance in fulfilling these requests.
5. Security Cooperation
   - Follow our security guidance and configure access controls appropriately within your organization.
   - Report any suspected security incidents to us without delay.
   - Maintain confidentiality of login credentials, API keys, or other means of accessing the platform.
6. Documentation and Audit Support
   - Keep records of the nature and purposes of processing, authorized users, and any risk assessments or impact assessments you conduct.
   - Provide timely and accurate information if we request additional documentation to demonstrate compliance or respond to regulatory inquiries.
7. Risk Assessment and Compliance
   - Evaluate the risk profile of your data processing (including AI functionalities) and conduct Data Protection Impact Assessments (DPIAs) where mandated by law.
   - Inform us of any special legal or compliance requirements that might affect how we process personal data on your behalf.
8. Sub-processor Review
   - Review our list of sub-processors and timely object if you have legitimate concerns, as described in Section 7.
   - Propose reasonable alternatives or solutions if you believe the engagement of a new sub-processor risks non-compliance with applicable laws.

By fulfilling these obligations, you help ensure that data protection standards are upheld within the platform and that the rights of data subjects are respected.

5. OBLIGATIONS OF THE DATA PROCESSOR

As your Data Processor, we commit to processing personal data according to your instructions and applicable data protection laws. Specifically, we will:

1. Process Only on Documented Instructions
   - Act solely on the instructions you provide via our platform's admin interface, your written directives, or other agreed channels.
   - Promptly inform you if we believe an instruction is non-compliant with data protection laws and, if necessary, suspend the relevant processing until clarified.
2. Maintain Confidentiality
   - Ensure that any personnel authorized to process your personal data are bound by

confidentiality agreements or statutory obligations of confidentiality.
    - Limit access to personal data strictly to those individuals who require it to perform their job duties.

3. Sub-Processor Management
    - Engage sub-processors only if they provide adequate data protection commitments through publicly available DPA or equivalent legal terms. These commitments must impose obligations equivalent to those in this DPA and ensure compliance with Applicable Data Protection Laws.
    - Maintain an updated list of sub-processors and notify you of intended changes.
    - Remain liable for any actions or omissions of our sub-processors in relation to the processing of your personal data.
4. Assistance with Data Subject Requests
    - Provide reasonable technical or organizational measures (e.g., platform tools) to help you fulfill data subject requests.
    - Forward any direct data subject inquiries to you unless otherwise required by law to respond.
5. Personal Data Breach Notification
    - Notify you without undue delay upon becoming aware of a personal data breach affecting your data, providing information required for you to meet any breach reporting obligations.
    - Collaborate with you in investigating and mitigating any breach impact.
6. Compliance and Audit Support
    - Keep records of our data processing activities and make them available to you, upon request, to demonstrate compliance.
    - Contribute to audits or inspections you initiate (or by an auditor appointed by you), within reasonable notice and during normal business hours.
7. Data Return or Deletion
    - Upon termination or expiry of our services, delete or return all personal data in our possession, at your choice, except where retention is required by law.
    - Ensure that any data retained due to legal obligations remains protected under this DPA's confidentiality and security provisions.
8. Security Measures
    - Implement and maintain appropriate technical and organizational measures outlined in Section 6 (Security Measures) to protect personal data.
    - Regularly update and improve these measures to adapt to changing threats, technologies, or legal requirements.
9. AI Processing Safeguards
    - For AI-generated content, maintain data separation and anonymization/pseudonymization measures where feasible, ensuring that no personal data is disclosed within such output.
    - Refrain from using your data for training general-purpose AI models without your explicit authorization, unless anonymized in a way that no longer identifies data subjects.

By adhering to these obligations, we ensure that your personal data is processed lawfully, securely, and transparently.

6. SECURITY MEASURES

We implement the following technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

We regularly review and adapt these measures to evolving security threats and industry best practices.

Infrastructure and Network Security

Our services operate in secure data centers with stringent physical security controls, environmental monitoring, and high availability infrastructure. We employ network segmentation, firewalls, and intrusion detection systems to mitigate unauthorized access and DDoS attacks. Critical security patches and updates are applied promptly.

Encryption and Key Management

We encrypt personal data in transit using TLS (Transport Layer Security) and at rest using strong encryption algorithms (e.g., AES-256). Encryption keys are managed securely, with restricted access and regular key rotation. Backups are also encrypted and stored separately to ensure data resilience.

Access Control and Authentication

Access to systems and data is granted on a need-to-know basis, enforced through role-based permissions. All access is logged and subject to periodic review. Our employees are subject to background checks and confidentiality obligations. We maintain strict access lifecycle processes (provisioning and de-provisioning) to avoid unauthorized or outdated credentials.

Monitoring and Incident Response

We maintain logs and system metrics to help identify potential security issues. We do review logs and investigate potential anomalies. We also maintain a documented incident response plan that outlines detection, containment, remediation, and communication steps for security incidents.

In the event of a confirmed incident, we conduct a post-incident review to improve both our technical safeguards and internal processes, reducing the likelihood of similar events in the future.

Application Security

All changes to our application go through secure development practices (e.g., code reviews, vulnerability scanning). Separate environments exist for development, testing, and production, minimizing the risk of unauthorized data access. Our AI modules process data in isolated execution environments to prevent cross-customer data leakage.

AI-Specific Safeguards

Data used for AI-related features (like content generation or learning analytics) is stored and processed in logical isolation from other customers. Any anonymization or pseudonymization necessary for AI model training is performed in a way that preserves your ownership and confidentiality of sensitive data.

Business Continuity and Disaster Recovery

We maintain redundant systems, encrypted backups, and documented recovery procedures, tested periodically. This ensures that essential services can be restored within defined recovery time objectives if a disaster occurs.

Ongoing Security Assessments

We conduct regular vulnerability scans, penetration tests, and internal audits. When new threats or vulnerabilities are identified, we prioritize fixes based on risk severity. We continuously update our technical documentation and security policies to reflect lessons learned and maintain compliance with relevant standards.

By maintaining and updating these measures, we aim to provide a security baseline that aligns with industry norms and evolving regulatory expectations.

7. SUB-PROCESSORS

This section details our policies and procedures regarding the engagement and management of sub-processors who assist us in providing our Services. We carefully select and monitor all sub-processors to ensure they provide sufficient guarantees to implement appropriate technical and organizational measures in compliance with applicable data protection laws.

Authorization for Sub-processors

By accepting this DPA, you provide us with general written authorization to engage sub-processors for the processing of personal data. This authorization is subject to the conditions set forth in this section and our commitment to inform you of any intended changes concerning the addition or replacement of sub-processors.

Current Sub-processors

Our current sub-processors include essential service providers necessary for the delivery of our Services. Our platform infrastructure is hosted on Microsoft Azure's cloud infrastructure, with data centers located in Germany and the United States. For our AI technology capabilities, we work with OpenAI, which provides natural language processing features for content generation and personalization, while Microsoft Azure AI supports learning pattern analysis and NVIDIA AI offers computational acceleration for our AI models. We also use HubSpot for managing user support and CRM functionality. Additionally, Stripe handles all payment transactions, operating as an independent data controller for payment data.

Each sub-processor provides a publicly available Data Processing Agreement or equivalent terms as part of their standard contract. By using their services, we adhere to these DPA terms, ensuring data protection obligations that are substantially similar to those set out in this DPA. This approach limits each sub-processor’s activities to what is required for their specific portion of the Services.

Changes and Notifications

We maintain an up-to-date list of our sub-processors which is available upon request. When we intend to make changes concerning the addition or replacement of sub-processors, we will notify you through multiple channels. You will receive an email notification at least 30 days before we authorize any new sub-processor, and we will update the sub-processor list in your account dashboard with relevant information about the new sub-processor and their intended processing activities.

Objection Rights and Process

You have the right to object to our use of a new sub-processor within 14 days of receiving notification of the intended change. Any objection must be made in writing and include reasonable grounds related to the sub-processor's ability to protect personal data in accordance with this DPA or applicable data protection laws.

Upon receiving your objection, we will make commercially reasonable efforts to address your concerns by either making available a change in the Services or recommending a commercially reasonable change to your configuration or use of the Services to avoid processing of personal data by the objected-to sub-processor. If we are unable to make such changes available within 30 days of your objection, you may terminate the affected Services by providing written notice to us.

Sub-processor Obligations and Oversight

We remain fully liable for all obligations subcontracted to sub-processors, including their acts and omissions. We only engage sub-processors that commit to data protection obligations substantially similar to those outlined in this DPA and applicable data protection laws. In practice, this typically occurs by incorporating or adhering to each sub-processor’s publicly available Data Processing Addendum (DPA), contract terms, or equivalent legal frameworks.

These terms require the sub-processors to:

- Process personal data solely in accordance with our documented instructions;
- Implement appropriate technical and organizational measures to protect personal data;
- Assist us in meeting our obligations under this DPA and Applicable Data Protection Laws;
- Promptly inform us if they believe an instruction violates any applicable data protection regulations.

Through this approach, we ensure that all sub-processors provide guarantees for data protection, even when relying on their standard contractual documents rather than individual, separately signed agreements.

Compliance Monitoring

We maintain an ongoing program to monitor and assess our sub-processors' compliance with data protection requirements. This includes regular reviews of security measures, periodic assessments of data protection practices, and comprehensive documentation of all engagements. We verify sub-processors' compliance with geographical processing restrictions and maintain detailed records of all data flows.

Confidentiality Requirements

All sub-processors and their personnel must adhere to confidentiality obligations that are at least as protective as those in this DPA. Such obligations generally arise through each sub-processor's publicly available data processing terms or equivalent contractual provisions. These confidentiality obligations survive the termination of the sub-processor's services and apply to all personal data accessed or processed.

We confirm that sub-processors' confidentiality commitments are aligned with our own through internal reviews and due diligence. This approach ensures that, throughout our supply chain, personal data remains protected under confidentiality standards equivalent to those set forth in this DPA.

This comprehensive sub-processor framework ensures transparent and compliant handling of personal data while maintaining the flexibility needed to provide and improve our Services. We remain committed to protecting your data throughout our supply chain and will promptly address any concerns regarding our sub-processors.

Publicly Available DPA Terms

For large-scale service providers (e.g., Microsoft, OpenAI, HubSpot), we rely on their publicly available Data Processing Addenda or equivalent terms as part of their standard contractual documentation. By subscribing to their services, we and our customers benefit from the GDPR-compliant clauses within those terms, thus ensuring lawful and secure processing of any personal data transferred to them.

8. INTERNATIONAL DATA TRANSFERS

We ensure that all international data transfers comply with applicable data protection laws, including the GDPR. Where personal data is transferred outside the European Economic Area (EEA), we rely on lawful transfer mechanisms and supplementary measures.

Primary and Secondary Processing Locations

Our primary data processing occurs in Germany for EEA-based customers. Secondary facilities in the United States (or other regions) may be used for disaster recovery, global operations, or specific client requests. You may choose a preferred data residency option where feasible.

Lawful Transfer Mechanisms

Where personal data is transferred outside the EEA, we implement:

- Standard Contractual Clauses (SCCs) or other approved legal frameworks as appropriate
- Transfer Impact Assessments (TIAs) to evaluate destination countries' laws and practices, with a focus on ensuring substantially equivalent protection
- Supplementary Measures such as additional encryption, pseudonymization, or access restrictions if the TIA indicates elevated risks

Additional Safeguards

We use robust encryption for data in transit and at rest, detailed logging and monitoring, and strict access controls. Where technically feasible, we pseudonymize or minimize data to reduce exposure when transferring it across borders. We also maintain internal policies and staff training aimed at protecting data subject rights globally.

Updates and Notifications

We regularly monitor evolving regulatory guidance on cross-border data transfers. If at any time we determine that we can no longer comply with applicable transfer requirements, we will promptly inform you and collaborate on suitable remedial actions (e.g., modifying data routing or employing alternative transfer solutions).

Documentation and Transparency

We maintain records of the relevant transfer mechanisms used by our sub-processors, including references to Standard Contractual Clauses (SCCs) or other approved frameworks, as well as any Transfer Impact Assessments (TIAs) we conduct. This documentation can be made available upon reasonable request to demonstrate compliance or to support inquiries from supervisory authorities or your internal compliance teams.

Where sub-processors rely on publicly available DPAs or standard terms that incorporate SCCs, we track these agreements and ensure they match the data protection obligations required by Applicable Data Protection Laws. This approach allows us to verify that each sub-processor provides adequate safeguards for international data transfers and overall data privacy compliance.

By adhering to this framework, we strive to ensure that personal data remains protected with a level of security and privacy comparable to that within the EEA, regardless of its final geographic location.

9. DATA BREACH NOTIFICATION

This section outlines our procedures for handling and reporting personal data breaches, ensuring compliance with notification requirements under applicable data protection laws and maintaining transparency with our customers.

Breach Detection and Initial Response

Our security systems continuously monitor for potential security incidents and data breaches. Upon detection of a potential personal data breach, our incident response team immediately initiates our incident response protocol. This includes assessing the nature and scope of the incident, containing and mitigating any ongoing security risks, preserving evidence for investigation, documenting initial findings, and evaluating the potential impact on personal data.

Notification Requirements

In the event of a confirmed personal data breach, we will notify you without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Our notification will be sent to your designated contact person using our secure communication channels. The notification will include a description of the nature of the breach, the categories and approximate number of data subjects affected, the categories and approximate number of personal data records concerned, the likely consequences of the breach, the measures taken or proposed to address the breach, and recommended steps to mitigate potential adverse effects.

In situations where we are unable to provide all information simultaneously, we will provide information in phases without undue delay. We will continue to update you as our investigation progresses and new information becomes available.

Investigation and Documentation

Following any personal data breach, we conduct a thorough investigation to determine the root cause of the breach, identify all affected systems and data, document the timeline of events, assess the effectiveness of our response, and implement measures to prevent similar incidents. We maintain detailed records of all personal data breaches, including the facts relating to the breach, its effects, remedial actions taken, documentation of decisions made, communications with affected parties, and evidence of compliance with notification obligations. These records are maintained in accordance with applicable data protection laws and are available for review by supervisory authorities.

Cooperation and Support

We will cooperate fully with you to ensure compliance with your obligations regarding breach notification to supervisory authorities and affected data subjects. This includes providing additional information needed for your notifications, assisting in assessing the risk to rights and freedoms of data subjects, supporting your communication with affected data subjects, coordinating public communications if required, and assisting with any regulatory investigations.

Risk Assessment

For each confirmed breach, we conduct a risk assessment to determine the severity of the impact on data subjects and the likelihood of adverse effects occurring. This assessment helps us determine whether notification to data subjects is required, what mitigation measures are appropriate, and whether supervisory authorities need to be involved. The assessment considers various factors including the type of breach, the nature and sensitivity of the affected data, and the potential consequences for data subjects.

Mitigation and Prevention

Following any breach, we implement appropriate measures to address the incident and prevent recurrence. These measures may include immediate security fixes and system updates, enhanced monitoring and detection capabilities, updates to security policies and procedures, additional staff training, and comprehensive reviews of our technical and organizational measures.

Communication and Training

Our breach-related communications are always clear, written in plain language, and specific about the nature of the breach. We focus on providing relevant information for recipients in a timely manner, maintaining appropriate security and confidentiality throughout the communication process. Our staff receives ongoing security awareness training, which includes guidance on identifying potential security incidents, following incident response procedures, and maintaining proper documentation.

Continuous Improvement

We regularly review and update our breach notification procedures based on lessons learned from actual incidents, changes in regulatory requirements, evolving security threats, and industry best practices. This commitment to continuous improvement ensures our breach response capabilities remain effective and aligned with current requirements. We also conduct regular testing of our incident response procedures through various exercises and assessments to ensure our team remains prepared to respond effectively to any security incidents or data breaches.

10. DATA RETENTION

This section outlines our policies and procedures regarding the retention and deletion of personal data processed through our Services. We maintain clear retention schedules and deletion procedures to ensure that personal data is not kept longer than necessary for the purposes for which it is processed.

General Retention Principles

We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, including providing our Services, complying with legal obligations, resolving disputes, and enforcing our agreements. The specific retention period for different types of personal data varies based on the nature of the data, the purpose of processing, and applicable legal requirements.

Service-Related Data Retention

For active customer accounts, we retain account information and related personal data for the duration of our service relationship. This includes user profile information, authentication data, and account settings necessary for providing our Services. Learning-related data, including course completion records, assessment results, and performance metrics, is retained according to your organization's requirements and applicable educational or professional certification standards.

AI-generated content and associated training data is retained for the duration of your subscription to our Services. This allows for continuous improvement of our AI models while maintaining the context needed for effective learning experiences. You may export or delete this content at any time through your account settings, subject to any applicable regulatory requirements or legal holds.

Post-Termination Retention

Following the termination of Services, we implement a structured data retention and deletion schedule. Account data and personal information are retained for thirty days after service termination to allow for account recovery and data export. During this period, you may request an export of your data in a commonly used, machine-readable format.

After the thirty-day post-termination period, personal data is removed from our active systems. However, certain information may be retained in backup systems for a limited period or as required by law. This backup data is secured and isolated from our active environment, with access strictly controlled and limited to specific recovery purposes.

Legal and Compliance Requirements

Certain types of data must be retained to meet legal, tax, accounting, or regulatory requirements. This includes transaction records necessary for financial reporting, evidence of completed training and certifications required by professional standards, and documentation needed for compliance purposes. We maintain these records only for the period required by applicable laws and regulations.

In cases where personal data is subject to multiple retention requirements, we apply the longest retention period required. When retention is based on legal obligations, we maintain documentation of the specific legal basis and required retention period.

Data Minimization and Review

We regularly review our data holdings to ensure we maintain only the personal data necessary for our stated purposes. This includes periodic assessments of stored data to identify and securely delete information that is no longer needed. Our review process considers the amount, nature, and sensitivity of the personal data, as well as the potential risk of harm from unauthorized use or disclosure.

Technical Implementation

We currently delete user data immediately upon valid deletion requests or following account termination. Deletions happen promptly and securely when triggered by user action or upon written instruction.

AWe strive to ensure that once data is flagged for removal, it is purged from active systems in a manner consistent with recognized security practices. Backup copies, if any, are overwritten or expire according to our backup rotation, typically within a limited timeframe.

Special Circumstances

In certain situations, we may need to retain personal data beyond standard retention periods. This includes cases where the data is subject to a legal hold, ongoing dispute resolution, or regulatory investigation. In such cases, we ensure that the retained data is properly secured and accessed only for the specific purpose requiring extended retention.

Documentation and Transparency

We maintain detailed documentation of our retention policies, including retention periods for different data categories, the rationale for these periods, and the procedures for secure deletion. This documentation is regularly updated to reflect changes in legal requirements or operational needs. Upon request, we can provide you with specific information about retention periods applicable to your organization's data.

Data Export and Deletion Requests

Throughout the service period and during the post-termination retention window, you may request the export or deletion of personal data through our platform interface or by contacting our support team. We will respond to such requests in accordance with applicable data protection laws and our contractual obligations. Export requests will be fulfilled in a commonly used, machine-readable format, and deletion requests will be executed across all active systems while respecting any applicable legal retention requirements.

11. FINAL PROVISIONS

Term and Termination

This Data Processing Agreement will take effect on the date you accept our Services and will remain in effect until the termination of our main service agreement. The obligations that by their nature are intended to survive termination, including confidentiality obligations and data protection requirements, will continue to apply after termination of this DPA.

Amendments and Updates

We may update this DPA from time to time to reflect changes in our Services, organizational practices, or legal requirements. Any material changes will be communicated to you at least 30 days before they take effect. If you do not agree with the proposed changes, you may object to them before their effective date. If we cannot reach an agreement on the proposed changes, either party may terminate the Services with written notice.

Governing Law and Jurisdiction

This DPA is governed by and interpreted in accordance with the laws of Spain, without regard to its conflict of law provisions. Any disputes arising from or in connection with this DPA will be subject to the exclusive jurisdiction of the courts of Barcelona, Spain. This choice of law and jurisdiction does not affect your rights under applicable data protection laws.

Severability

If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions will remain in full force and effect. The parties will work together in good faith to replace any invalid or unenforceable provision with a valid and enforceable provision that achieves the same intended purpose to the greatest extent possible.

Precedence

This DPA forms an integral part of our service agreement. In case of any conflict between this DPA and any other agreements between us, including our Terms of Service and Privacy Policy, the provisions of this DPA will take precedence with respect to the subject matter of data processing.

Notifications

All notifications related to this DPA must be in writing and sent to the designated contact persons. For us, notifications should be sent to dpo@foxtery.com or to our postal address: Foxtery S.L., Calle Marc Aureli 10, Barcelona, Barcelona 08006, Spain. You are responsible for ensuring that your contact information remains current and accurate.

Audit Rights

In accordance with Article 28 of the GDPR, you may request evidence of our compliance with this DPA and Applicable Data Protection Laws. This request can take the form of security or compliance documentation (e.g., summary audit reports, certifications, or policies). Where a more direct audit is necessary (for instance, if mandated by supervisory authorities or by material compliance concerns), you may perform an on-site or remote assessment under the following conditions:

1. The audit must be limited to personal data processing relevant to your account and require at least 30 days’ prior written notice.
2. Audits may occur once per calendar year unless otherwise required by law or if a significant security incident justifies an additional audit.
3. Audits shall be conducted during regular business hours and in a manner that does not unreasonably interfere with our operations.
4. You may appoint an independent third-party auditor, subject to our prior approval and appropriate confidentiality obligations.

We reserve the right to offer alternative means of demonstrating our compliance (e.g., recent penetration testing reports, security certifications, or third-party audit attestations) if such means adequately address the scope of your audit request.

Assignment

Neither party may assign or transfer this DPA without the prior written consent of the other party, except that either party may assign this DPA without consent to a successor in connection with a merger, acquisition, or sale of all or substantially all of its assets.

Force Majeure

Neither party will be liable for any failure or delay in performing their obligations under this DPA where such failure or delay results from circumstances beyond that party's reasonable control. However, this provision does not apply to payment obligations or core data protection requirements.

Entire Agreement

This DPA, together with its appendices and referenced documents, constitutes the entire agreement between the parties with respect to the processing of personal data and supersedes all prior agreements, whether written or oral, relating to the same subject matter.

Interpretation

The section headings in this DPA are for convenience only and do not affect its interpretation. Words importing the singular include the plural and vice versa. References to including or includes mean including or includes without limitation.

12. CONTACT INFORMATION

In order to resolve a complaint regarding the Services or to receive further information regarding use of the Services, please contact us at:

Foxtery S.L.
Calle Marc Aureli 10
Barcelona, Barcelona 08006
Spain

Phone: +34 936 940 325
Email: info@foxtery.com

Company Details:

Registration No.: B16372799
VAT: ESB16372799
Director: Artem Maslov

Payment Details:

Account holder: Foxtery S.L.
Bank name: BANCO BILBAO VIZCAYA ARGENTARIA S.A.
SWIFT/BIC: BBVAESMMXXX
IBAN: ES3501821015040202514386
Bank Address: C/ SAUCEDA 28, MADRID, Spain

Last updated: January 15, 2025

ANNEX I

DETAILS OF PROCESSING: SUBJECT MATTER, DURATION, NATURE AND PURPOSE, TYPES OF PERSONAL DATA, AND CATEGORIES OF DATA SUBJECTS

1. Subject Matter of the Processing

The subject matter of the processing is the provision of Foxtery's AI-powered corporate learning platform and related services ("Services") to the Customer (Controller), as set out in the main Agreement and the DPA.

2. Duration of the Processing

- **Term**: The processing shall be carried out for the duration of the Agreement between Foxtery S.L. (Processor) and the Customer (Controller).
- **Termination**: Upon termination or expiry of the Agreement, Foxtery will either delete or return personal data in accordance with the DPA, subject to any further retention obligations under applicable laws.

3. Nature and Purpose of the Processing

- **Nature**: Collection, storage, organization, adaptation, AI-based analysis, retrieval, use, and other operations necessary to provide corporate learning functionalities.
- **Purpose**:
  - Creating and managing user accounts
  - Generating and delivering AI-powered learning materials
  - Tracking progress, assessments, and learning performance
  - Enabling analytics, reports, and certifications
  - Improving and securing the Services, including fraud prevention and compliance with legal obligations

4. Types of Personal Data

Depending on the Controller's configuration and usage of the Services, the following categories of personal data may be processed:

1. Identification Data: Names, emails, job titles, or other profile fields
2. Login and Authentication Data: Usernames, hashed passwords, tokens
3. Contact Data: Business contact details (phone numbers, addresses) if provided
4. Learning Data: Course progress, completion rates, assessment results, performance metrics
5. Training Materials: Any personal data embedded in corporate documents, manuals, or resources uploaded by the Controller for AI processing
6. Technical Data: IP addresses, browser type, device identifiers, usage logs

5. Categories of Data Subjects

1. Employees or Contractors of the Controller who use the learning platform
2. Authorized Personnel of the Controller with administrative or instructor roles
3. Any Third Parties whose personal data is included in the training materials or other content uploaded by the Controller (e.g., client references, case studies)

ANNEX II

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES (TOMS)

This Annex describes the minimum technical and organizational measures that Foxtery implements to protect personal data processed on behalf of the Controller. These measures may be updated from time to time to reflect technological progress or new best practices, provided that such updates do not diminish the overall security level.

1. **Physical Access Control**
    - Data centers with restricted entry, 24/7 security, CCTV, and multi-factor authentication for on-site staff.
    - Environmental controls (fire detection, cooling, backup power).
2. **Logical Access Control**
    - Role-based access permissions (least privilege principle).
    - Unique user IDs; secure password policies.
    - Centralized directory services with periodic access reviews.
3. **Data Access Control**
    - We maintain policies ensuring that only authorized personnel with a legitimate business need can access data.
    - While we do log certain access attempts, we review relevant logs to detect anomalies.
    - We conduct periodic checks of user permissions and logs to confirm compliance with our internal access policies.
4. **Transmission Control**
    - TLS (Transport Layer Security) for encrypted communication over public networks.
    - VPN or other secure channels for internal administration and sub-processor connections.
    - Enforced security headers for web interfaces (e.g., HSTS, X-Frame-Options).
5. **Data Input Control**
    - We apply basic validation of incoming data to mitigate risks like malicious payloads or injection attacks.
    - We do track critical events for troubleshooting and compliance where feasible.
    - Certain critical data may be versioned or backed up for traceability, but not all actions are individually logged at this time.
6. **Job Control**
    - Procedures ensuring data is processed strictly per the Controller’s instructions.
    - Regular staff training on data protection, confidentiality, and secure handling.
    - Execution and scheduling of AI tasks configured to prevent unauthorized data blending.
7. **Availability Control**
    - Redundant infrastructure, failover mechanisms, and load balancing to ensure high availability.
    - Encrypted backups stored in geographically separate locations, tested periodically.
    - Cloud provider’s infrastructure includes redundancy, backup processes, and regional failover options.
8. **Separation Control**
    - Logical isolation of each Controller’s environment; no commingling of data sets.
    - We use a multi-tenant approach where data is encrypted under a shared key management scheme. We ensure logical isolation and strict access controls to prevent cross-customer data leakage.

- Segregated AI models or dedicated namespaces to avoid cross-contamination of learning data.

9. **Pseudonymization and Encryption**

    - Data minimization and pseudonymization where feasible, especially for AI training or analytics.
    - AES-256 or equivalent encryption for data at rest; TLS 1.3 or equivalent for data in transit.
    - Key management system with restricted permissions and periodic key rotation.

10. **Incident Response and Notification**

    - We maintain an incident response procedure describing how we identify, contain, and remediate security incidents. We review logs and address detected issues promptly.
    - In the event of a confirmed personal data breach, we will notify the Controller without undue delay, providing details of the incident, potential impact, and mitigation steps.
    - For critical alerts or significant anomalies, we have internal escalation paths. Post-incident analysis helps us improve our detection capabilities and processes.

11. **Monitoring**

    - We conduct vulnerability scans and may perform or commission penetration tests to identify potential system weaknesses.
    - We review logs and system metrics at intervals to spot issues.
    - We address discovered vulnerabilities based on a risk-based remediation process, prioritizing fixes according to severity and potential impact.

12. **AI-Specific Controls**

    - Validation checks and filters on input data fed into AI models to prevent injection of sensitive or unlawful content.
    - Application-layer isolation so that one customer’s training data or results are not visible or accessible to another.
    - Mechanisms to prevent re-identification if anonymized data is used for general AI model improvements.

ANNEX III

AUTHORIZED SUB-PROCESSORS AND SUB-PROCESSING ACTIVITIES

The following is a non-exhaustive list of sub-processors engaged by Foxtery to fulfill the Services. This list may be updated as per the notification procedure described in Section 7 of the DPA.

Sub-Processor	**Location**	**Service Provided**	**Transfer Mechanism**
Microsoft Azure	EU (Germany), US	Hosting infrastructure and data storage	Standard Contractual Clauses (SCCs)
OpenAI	US/EU	Natural language processing for AI features	SCCs / TIAs & supplementary measures
HubSpot	US/EU	CRM and user support functionality	SCCs / HubSpot Data Processing Agreement
NVIDIA AI	US/EU	Computational AI model acceleration	SCCs / TIAs
Stripe	Various	Payment processing (Controller for payment)	N/A (Separate Controller role)

Notes:

1. Sub-processors marked as “Controller for payment data” operate under their own privacy policies for financial details, though we require them to protect end-user data as well.
2. We may engage additional sub-processors or replace existing ones according to the procedure in the DPA (Section 7), providing at least 30 days’ notice to the Controller.

ANNEX IV

STANDARD CONTRACTUAL CLAUSES (SCCs)

If and to the extent that the GDPR applies to the processing of personal data under this DPA and any such processing involves the transfer of personal data to a third country outside the EEA, the parties agree that:

1. **SCC Incorporation**
   The Controller (as “data exporter”) and Foxtery (as “data importer,” or as “processor”) hereby enter into the relevant modules of the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914 of 4 June 2021) for the transfer of personal data to third countries.

2. **Interpretation and Precedence**
   - The SCCs are hereby incorporated by reference and form an integral part of this DPA.
   - In the event of a conflict between the SCCs and this DPA or any other related agreement, the SCCs shall prevail with respect to the transfer of personal data.

3. **Module Selection**
   - **Module 2** (Controller to Processor) typically applies to personal data flows between the Controller and Foxtery in the context of providing the Services.
   - **Module 3** (Processor to Processor) may apply where Foxtery engages sub-processors located in third countries.

4. **Appendices to the SCCs**
   - **Appendix I** to the SCCs: Corresponds to Annex I (Details of Processing) and the parties’ identities.
   - **Appendix II** to the SCCs: Corresponds to Annex II (Technical and Organizational Security Measures).
   - **Appendix III** (where relevant): References the list of sub-processors in Annex III.

5. **Execution and Effect**
   - By executing the main Agreement and the DPA, the parties are deemed to have executed the SCCs, including the relevant appendices.
   - If required, the parties may sign the SCCs separately for formality, referencing the details in this DPA.

6. **Supplementary Measures**
   - The parties acknowledge that they may implement additional supplementary measures (e.g., encryption, pseudonymization, policy commitments) in accordance with any Transfer Impact Assessments performed.

7. **Governing Law of the Clauses**
   - As required under the SCCs, the law of an EU Member State that recognizes third-party beneficiary rights (e.g., Ireland or the Netherlands) shall govern the clauses.