

ELB LEARNING PRIVACY POLICY

Updated June 14, 2024 | [See previous versions](#)

Welcome to ELB Learning! Your privacy matters to us, and this Privacy Policy (“**Policy**”) sets forth our commitment to transparency and trust in our handling of your personal data. We urge you to read it carefully to ensure you're informed about our practices.

I. INTRODUCTION

Who We Are: ELB Learning (registered as Plato eLearning, LLC) develops organizational eLearning software solutions including authoring, reviewing, publishing, and course management tools and related professional services. Along with our affiliates like The Game Agency, LLC, we operate several websites (e.g., [elblearning.com](#), [thetrainingarcade.com](#), [thegameagency.com](#), [elearningbrothers.com](#), [cenariovr.com](#), [rockstarlxp.com](#)) (“**ELB Websites**”) and provide eLearning solutions therethrough (“**ELB Solutions**”). This Policy applies to the collection, use, and other processing of personal data by ELB Learning and its affiliates (herein “**ELB**,” “**we**,” “**us**,” “**our**”) while operating the Websites and providing the ELB Solutions.

Who Uses Our Solutions? ELB is a business-to-business provider. Our customers are businesses, government agencies, NGOs, educational institutions, healthcare organizations, and other entities (“**Customers**”). Our solutions are designed to help Customers enhance the professional and organizational training and development needs of those employed by or associated with them. Accordingly, ELB Websites and Solutions are intended for business or professional use, not for individual consumers or households.

Access to certain parts of an ELB Website and Solutions are restricted to those individuals authorized by a Customer under our [Subscription and License Agreement](#), unless otherwise agree upon (each a “**Subscription Agreement**” or “**SALA**”). These restricted services (the “**Subscription Services**”) require authentication credentials (e.g., username and password) linked to the Customer’s account and assigned to the authorized individual (hereinafter “**User Credentials**”).

How This Privacy Policy Applies To You? This Policy’s applicability depends on your relationship with us and the context of our interaction. If you access Subscription Services using User Credentials, your relationship with ELB is as an “**Authorized User**” of our Customer. Based on this relationship, this Policy outlines the additional personal data collected from Authorized Users and the different practices and standards applied compared to other users (See [Personal Data Collected From Authorized Users](#), [Authorized User Data Use](#), and [Authorized User Data Sharing](#)).

IMPORTANT NOTE REGARDING ELB’S CONTRACTUAL COMMITMENTS TO CUSTOMERS

ELB’s processing of Authorized User data, is at all times subject to and governed by the applicable terms of the SALA and the associated [Data Processing Addendum](#) (“**DPA**”) between ELB and the Customer. Terms of the DPA include ELB’s commitment to:

- Refrain from using Authorized User Personal data for marketing purposes other than where the Authorized User has expressly opted in to receive such marketing.
- Refrain from adding Authorized User personal data to its enterprise general marketing database.
- Refrain from selling Authorized User Personal data, which ELB also commits to you as an individual under this Policy (See [Note Regarding Selling & Sharing for Marketing Purposes](#)).

In addition to this Privacy Policy, your use of the ELB Websites and Solutions (excluding the Subscription Services) is subject to our [Website Terms of Use](#) (“**Website TOUs**”) and your use of the Subscription Services is subject to the applicable Subscription Agreement.

What Is Not Covered By This Policy?

- [Third-Party Websites](#). ELB Websites and Solutions may include links to websites (including social media sites and organizers of webinar and other events) owned or operated by third parties (“**Third-Party Websites**”). Clicking on those links or otherwise enabling those connections allows third parties to collect your personal data. ELB does not control these websites, and the processing of your personal data by such

Third-Party Websites is not covered by this Policy. However, to the extent that Third-Party Websites act as sources of personal data for ELB (See [Third-Party Sources](#)), this Policy governs ELB's use of any personal data received from them. We recommend that you review the privacy policies of such Third-Party Websites to understand how they use your information.

- **Third-Party Services.** ELB Websites and Solutions may permit or facilitate interactions with online platforms, applications, and services owned or operated by third-parties (“**Third-Party Services**”). Use of those services or otherwise enabling those connections allow third parties to collect your personal data. ELB does not control these services, and the processing of your personal data by such Third-Party Services is not covered by this Policy. However, to the extent that Third-Party Services act as sources of personal data for ELB (See [Third-Party Sources](#)), this Policy governs ELB's use of any personal data received from them. We recommend that you review the privacy policies of such Third-Party Services to understand how they use your information.
- **Customer Use of Personal Data.** If you are an Authorized User, we will disclose your personal data to the Customer through which you received access to the Subscription Services. The use of your personal data by the applicable Customer will be governed by the Customer’s privacy policy (See [Authorized User Data Sharing](#)).
- **User Contributions.** If you choose to include personal data in [User Contributions](#), you do so understanding that such personal data will be made available on ELB Websites and Solutions and that access to such may be available generally to the public. Therefore, we advise you to exercise caution and discretion when sharing personal data in User Contributions, as such data will not be covered by this Privacy Policy. We are not responsible for the privacy practices of third parties who may access it through the ELB Websites or Solutions.
- **Data that is not Personal Data.** This Policy does not cover data that does not constitute “personal data” or “personal information” under applicable data protection laws. Depending on the data protection laws applicable to you, exclusions may include data that is publicly available as government records or found in the public domain, and data related to individuals acting in a commercial, professional, business, or employment context, rather than in a personal or household capacity.
- **Aggregated, Deidentified, & Anonymous Data.** ELB may aggregate, deidentify, or anonymize personal data. Provided we implement measures in accordance with applicable data protection laws to adequately deidentify or anonymize data, such data will not be treated as “personal data” or “personal information” under this Policy. Except as prohibited by applicable law and/or our Subscription Agreement with the applicable Customer, ELB may use, process, and share such non-personal information without limitation.

II. PERSONAL DATA COLLECTED

A. Standard Personal Data Collected. Regardless of whether you are an Authorized User or not, personal data collected includes:

1. **Data You Provide.** Depending on how you interact with the ELB Websites or Solutions, you may choose to provide us, our agents, vendors, consultants, and other service providers (collectively, “**Service Providers**”) and/or those event/program operators, organizers or sponsors, and other third-parties that we work with in support of our brands (“**Brand Partners**”) with personal data that may include:
 - *Personally Identifying Information (“PII”):* information by which you may be personally identified, such as name, email address, telephone number, or any other identifier by which you may be contacted online or offline. Purposes for which you may provide PII include requests for access to certain informational resources such as ebooks, infographics or whitepapers, to submit comments to a Blog post or Knowledge Base content, request a product demo, membership to ELB’s Learning Community, subscription to our Newsletter, webinar notifications, or information about being a webinar presenter, and to contact us via webforms or email.
 - *Professional or Employment Information:* information related to your business or employer including your business contact information. This information is commonly provided in the same contexts as PII as described above.

- *Submission Information*: information that directly or indirectly identifies you that you elect to include in any communications with us and/or submit as a User Contribution pursuant to the [Website Terms of Use](#).
2. **Data Collected Automatically**. ELB, our [Service Providers](#), or [Brand Partners](#) you elect to interact with implement common information-gathering tools such as cookies, web beacons, pixels, and other similar tracking technologies (collectively, “**Cookies**”) to automatically collect information as you navigate our respective online properties, your accounts with us, our advertisements and/or when you interact with emails sent by or on our behalf. Cookies do not typically contain any information that personally identifies you, but personal information that we store about you may be linked to the information stored in and obtained from Cookies. Information about Cookies and how to exercise your choices over the use of these can be found in our [Cookie Policy](#).
 3. **Third-Party Sources**. We may obtain personal data from third parties as follows:
 - *Data Providers*: We may obtain personal data from reputable third-party providers of licensed data derived from public and non-public sources to correct or supplement personal data we collect.
 - *Service Providers*: Our [Service Providers](#), such as payment processors, email marketing service providers, and third parties who conduct analytics and other business activities on our behalf, may share with us some or all of the personal data they collect in the course of performing their services. For example, we may engage and work with Service Providers to help process transactions, manage customer relationships, and analyze user engagement. These Service Providers may provide us with aggregated and individualized data, which enhances our marketing efforts and provides deep insights into user behavior, usage patterns, and preferences to better tailor and optimize ELB Websites and Solutions.
 - *Third-Party Websites and Services*: In connection with your use of the ELB Websites and Solutions, you may provide Personal Data to [Third-Party Services](#) (see [Data You Provide](#)) and/or such Third-Party Services may use Cookies to collect Personal Data (See [Data Collected Automatically](#)) that is shared with us. For example, ELB may maintain its own branded pages on various social networks. When you visit these branded social media pages, the provider of the social network and other Third-Party Services may set Cookies on your browser or device and provide us with the types of personal data identified in our [Cookie Policy](#).
 - *Brand Partners*: If you participate in a live or online event or request access to resources made available by our [Brand Partners](#), the applicable Brand Partner may provide us with your personal data pursuant to the agreement between us.

B. Personal Data Collected from Authorized Users. Additional personal data may be collected from Authorized Users based on their interaction with the ELB Websites and Solutions and the access role assigned to them in the applicable Customer account. Subcategories of Authorized Users include:

- “**Administrators**” Authorized Users that administer and manage Customer “instance” of the Subscription Services including: (i) inviting, authorizing, and managing access to the Subscription Services by other Authorized Users; (ii) defining and/or accessing learning/training results, outcomes, metrics; and (iii) adding, deleting, and otherwise managing Subscription Services features and functions available to other Authorized Users.
- “**Creators**” Authorized Users that create, customize learning modules, training tools, learning simulations, learning games, and content used therein / therewith.
- “**Learners**” Authorized Users that actively participate in the learning activities designed, provided, or managed via the Subscription Services, with the goal of fulfilling the learning objectives set by the Customer.

In addition to the personal data set forth in the [Standard Personal Data Collected](#) above, Authorized User personal data collected includes:

1. **Data You Provide**.

- a. *All Authorized Users*: Depending on the settings established by applicable Customer, you may provide ELB with additional:
 - *PII and Professional Information*: information for registration purposes such as job title, group/team/function designation, primary job location, employer provided contact email and telephone number. Please note that, to provide the Subscription Services, the only PII necessary is an Authorized User's email address and, for Administrators only, their name (and for certain Subscription Services telephone contact number). Any other PII collected in connection with registration is done at the request of the Customer.
 - *Log-In Data*: username or other unique ID and password that enables access to the Subscription Services.
 - *Submission Information*: information that directly or indirectly identifies you that you elect to include in any communications effectuated via Subscription Services functionality with other Authorized Users.
 - b. *Learners*: Depending on which learning activities you participate in and the settings established by the applicable Customer, Learners may provide ELB with additional:
 - *PII, Professional Information and Demographic Data*: information types as designated by the Customer to be requested in connection with Learner registration which, in addition to PII and Professional Information, may include demographic data such as age and education level or area of study; provided that no such Demographic Data should be, include, or reveal [Prohibited Data](#). It is the Customer's responsibility to ensure that no [Prohibited Data](#) is made available to ELB.
 - *Audio/visual Data*: information consisting of the video and audio that Learners can submit in connection with certain Subscription Services such as [Rehearsal](#).
2. Data Collected Automatically.
 - a. *All Authorized Users*: usage data such as log-in times, functions or features used, and duration of use.
 - b. *Learners*: additional usage data such as learner interactions with scenarios (See [CenarioVR](#)), and learner performance (See [CourseMill®](#), [Rehearsal](#), [RockStar Learning Platform](#), [MicroBuilder®](#), and [The Training Arcade®](#).)
3. Third Party Sources. In connection with your use of the Subscription Services, ELB may receive personal information from third-parties including Customers and those third-party resellers, distributors, and providers of products and/or services that are complementary to, or compatible or interoperable with, ELB Solutions ("**Product Partners**").
 - *Customers*: If elected by the Customer, it may provide all or some of the PII, Professional Information, and Demographic Data set forth above in the [Data You Provide](#) section rather than having ELB collect such data directly from you.
 - *AI Service Providers*: Select ELB Solutions may use large language models (LLMs) or other advanced machine learning or AI technologies ("**AI Functionality**") within or alongside ELB Solutions. If the Customer elects to use AI Functionality, inferences will be made and insights will be derived regarding the applicable Learner's communication style, skill proficiency, and other performance indicators from your assignment, game play, or other learning activity. Such inferences and insights are provided by ELB's third-party AI Functionality providers and may be considered personal data under applicable data privacy regulations.
 - *Product Partners*: ELB Solutions are interoperable and/or integrate with a variety of applications including those used for communications (e.g., [Slack](#), [GoTo Meeting](#), [Zoom](#), and [Teams](#)), monetization (e.g., [Stripe](#) and [Shopify](#)), creating courseware (e.g., [BizLibrary](#), [OpenSesame](#), and [Traliant](#)), and delivering and reporting on training courses and programs (i.e., LMS) (e.g., [Docebo](#)). If Customer elects to enable any such integrations, the applicable Product Partner may, on behalf of the applicable Customer, provide ELB all or some of the PII, Professional Information, and Demographic Data set forth above in the [Data You Provide](#) section.

C. Personal Data ELB Aims to Avoid. Regardless of whether or not you are an Authorized User, certain categories of personal data are just not needed for the proper operation of ELB Websites and Solutions or your use thereof. Accordingly, ELB classifies such personal data as “**Prohibited Data**,” User Contributions does not seek to collect such data and takes proactive measures to avoid obtaining it. The [ELB Website Terms of Use](#) prohibits your User Contributions from including Prohibited Data. ELB also requires Customers to contractually agree to not use ELB Solutions to collect or otherwise use such data. If you are an Authorized User, this restriction applies to you also. If we discover that we have received or processed Prohibited Data, we will take reasonable steps to delete that data. If you believe we might have any Prohibited Data, please contact_us according to the [Contact Information](#) section.

III. USE OF PERSONAL DATA

A. Standard Personal Data Use. Except as otherwise provided in the DPA entered into by ELB and the applicable Customer (See [Important Note Regarding ELB’s Contractual Commitments to Customers](#)) ELB may use the [Standard Personal Data](#) described above as follows:

1. [Provision, Maintenance, and Improvement of ELB Websites & Non-Subscription ELB Solutions.](#)
 - Creating and managing access to content and services that does not require User Credentials.
 - Facilitating interaction with Third-Party Services.
 - Providing technical support and responding to inquiries submitted via webforms or email.
 - Monitoring performance metrics to optimize website functionality and improve user engagement.
 - Conducting analytics to identify popular features, learning paths, and content.
2. [Marketing and Advertising.](#)
 - Sending newsletters, product updates, promotional content, and event invitations to subscribed visitors.
 - Notifying individuals about new features, courses, or educational materials like eBooks, whitepapers, and infographics.
 - Recommending relevant learning resources based on user preferences and past engagement.
 - Delivery and measurement of tailored marketing campaigns by our Service Providers.
3. [Content Personalization and Improvement.](#)
 - Tailoring the user experience based on previous interactions with ELB Websites and Solutions.
 - Customizing suggested educational resources to align with user interests.
 - Analyzing engagement patterns to refine ELB Websites and Solutions for improved usability.
4. [Event Management and Collaboration.](#)
 - Coordinating live and online events with Brand Partners, including registration and follow-up communications.
 - Managing webinar presenter applications and event notifications.
5. [Research and Development.](#)
 - Conducting surveys and gathering feedback to innovate and improve ELB Solutions.
 - Testing new features or functionalities on a limited group of users.
6. [Security.](#)
 - Detecting and preventing unauthorized access, fraudulent activities, and security breaches.
 - Monitoring behavior patterns for unusual activity that could indicate a security issue.
 - Analyzing threat intelligence to identify and respond to potential cyber threats.

- Implementing firewalls, encryption, multi-factor authentication, and other measures to safeguard personal data.
- Maintaining records of access and activity for security analysis.
- Developing and executing response plans in case of security incidents.

7. Legal and Regulatory Compliance.

- Complying with applicable data protection laws, including GDPR, CCPA/CPRA, and other relevant regulations.
- Responding to lawful requests and subpoenas for information from public authorities.
- Monitoring compliance with Website Terms of Use, Cookie Policy, and Privacy Policy.

8. Fulfill Other Disclosed Purposes.

- Fulfilling other purposes disclosed to you at the time you provide personal data or otherwise where legally permitted.

B. Authorized User Data Use. Except as otherwise provided in the DPA entered into by ELB and the applicable Customer (See [Important Note Regarding ELB's Contractual Commitments to Customers](#)) [Authorized User Personal Data](#) is used for the same purposes described in the [Standard Personal Data Use](#) section. Additionally, this data is used as follows:

1. Provision of Subscription Services to the Applicable Customer.

- Creating and managing individual Authorized User accounts, including setting up user credentials.
- Managing team structures, job titles, primary job locations, and other professional information based on Customer requirements.
- Facilitating access to and participation in learning activities, assessments, and training programs.
- Providing technical support and responding to inquiries submitted via Subscription Services.

2. Learner Performance Analysis and Improvement.

- Providing detailed feedback, scoring, and assessment reports.

Note Regarding Use of Video and Audio in Rehearsal -

ELB uses video and audio recordings in the Rehearsal product to enable Customers to provide personalized feedback and mentorship, enhancing user learning and performance. Importantly, video recordings are not digitally analyzed for facial recognition, and audio recordings are subjected to speech analysis solely to provide information such as the average pace of speech, time spent speaking vs. pausing, total word count, and whether any questions were asked. These analyses do not involve voice recognition technologies intended to identify an individual.

While Rehearsal is not designed to identify individuals, it is important to note that the underlying data could capture unique physiological traits and therefore could be considered "biometric information" under privacy statutes such as GDPR, CCPA, and BIPA. Notwithstanding the above, it is the responsibility of the Customer to determine if its use of the Rehearsal product triggers any additional disclosure and/or consent requirements typically associated with biometric data and to comply with any such requirements.

3. Communication and Collaboration between Authorized Users.

- Enabling messaging and other communication features between Authorized Users within the Subscription Services.
- Facilitating group activities and collaboration based on team, function, or group designation set by the Customer.
- Allowing Users to share feedback and comments related to learning activities.

4. Interoperability/Integration with Third-Party Services.
 - Facilitating interoperability or integration with complementary Third-Party Services like communication tools (e.g., [Slack](#), [GoTo Meeting](#), [Zoom](#), and [Teams](#)), monetization services (e.g., [Stripe](#) and [Shopify](#)), and courseware creation platforms (e.g., [BizLibrary](#), and [OpenSesame](#)).
 - Sharing or receiving personal data with Product Partners to facilitate learning activities and reporting.
5. Usage Analysis and Service Optimization.
 - Tracking and analyzing Authorized User interactions with Subscription Services to improve overall functionality.
 - Monitoring usage patterns to optimize Subscription Services features and enhance the user experience.
6. AI-Based Insights and Recommendations.
 - Using advanced [AI Functionality](#) to derive insights regarding communication style, skill proficiency, and other performance indicators from assignments, gameplay, or other learning activities.
 - Providing tailored training recommendations, goal-setting suggestions, and personalized learning plans based on AI Functionality insights.
7. Customer-Specific Reporting and Insights.
 - Generating Customer-specific reports that include aggregated and individualized learner performance data for the applicable Customer.
 - Providing insights into team structures, job titles, and learner demographics to help Customers better manage their training programs.
8. Compliance with Customer Agreements.
 - Ensuring compliance with Subscription Agreements, Data Processing Addendums, and Customer-specific security requirements.
 - Adhering to Customer-imposed restrictions on data sharing and processing.

Authorized User personal data that is separate from and in addition to the [Standard Personal Data](#) that Authorized Users, the applicable Customer, and our Product Partners provide to ELB is used by ELB to provide the Subscription Services to the applicable Customer. ELB processes this data in accordance with the [Data Processing Addendum to the Subscription and License Agreement](#) between ELB and the Customer.

IV. SHARING OF PERSONAL DATA

- A. **Standard Personal Data Sharing.** Except as otherwise provided in the DPA entered into by ELB and the applicable Customer (See [Important Note Regarding ELB's Contractual Commitments to Customers](#)) ELB may share [Standard Personal Data](#) described above as follows:
1. Affiliated Companies.
 - Managing internal administration and decision-making within ELB's family of companies.
 - Enhancing services by leveraging shared technologies and insights across our affiliated companies.
 2. Service Providers.
 - Supporting marketing and advertising efforts through service providers specializing in such services.

- Providing services for:
 - Hosting infrastructure, user data and cloud computing.
 - Data visualization and analysis.
 - Automated email correspondence.
 - Credit card payment processing.
 - Customer support, success, and purchasing communications and data processing.

3. Third-Party Services.

- Resulting from interactions initiated by users with third-party social networks from an ELB Website or Solution. Examples include "liking" or "sharing" content.
- Working with Brand Partners to facilitate user registration and participation in live and online events or webinars, enhancing the user experience and providing interoperable and/or integrated services.

4. Legal and Regulatory Compliance.

- Responding to legal requirements when compelled by law, such as to fulfill lawful requests by public authorities.
- Ensuring compliance with applicable laws and protecting the rights and safety of ELB, our users, and the public from fraud and abuse.

5. Business Transfers.

- Disclosing data during the due diligence process of mergers, acquisitions, or bankruptcy.
- Sharing data as part of corporate reorganization processes.

6. Protection and Safety.

- Taking action if we believe your actions are inconsistent with our user agreements or policies, or to protect the rights, property, life, health, security, and safety of ELB or any third party.
- Responding to instances where we have a good faith belief that a crime has been or is being committed by a user.

B. Authorized User Data Sharing. Except as otherwise provided in the DPA entered into by ELB and the applicable Customer (See [Important Note Regarding ELB's Contractual Commitments to Customers](#)) [Authorized User Personal Data](#) is shared with the same third parties and for the same purposes as in the [Standard Personal Data Sharing](#) section. Additionally, this data is shared with additional third parties and/or for different purposes as follows:

1. Provision of Subscription Services.

- *Product Partners:* ELB may share Authorized User Personal Data with [Product Partners](#) that provide services and technologies that integrate or are interoperable with the Subscription Services. When a Customer enables such integrations or interoperability, ELB may share relevant Authorized User Data with the applicable Product Partner as needed to fulfill the Customer's need.
- *AI Service Providers:* Select Subscription Services incorporate advanced [AI Functionality](#) to analyze and enhance learning outcomes ([See Note Regarding Use of Video and Audio in Rehearsal](#)). ELB currently uses third-party AI Service Providers OpenAI and Amazon Web Services ("**AI Providers**") for the natural language processing and analysis provided in [Rehearsal](#). We use OpenAI's Enterprise API license to leverage its natural language AI tools. Under the terms of this license, OpenAI does not use inputs and outputs to improve its AI models, ensuring privacy and compliance with relevant data protection laws. For detailed information on how OpenAI processes data and the specific terms of our engagement, Authorized Users can refer to OpenAI's [Terms & Policies](#). AWS provides functionality to enable its customers to opt-out of having their content stored or used to improve AWS's services (See

[AWS AI services opt-out policies](#)) and ELB has implemented an Amazon Transcribe opt-out policy. For more information about AWS's data privacy controls, please see its [Data Privacy FAQ](#) and the [AWS AI Service Card for Transcribe](#).

2. Customers.

- Facilitating the administration and delivery of Subscription Services.
- Customizing Subscription Services to meet specific Customer requests and support needs.
- Delivering Subscription Services performance analysis and reports to Customers.
- Providing strategic insights to aid Customers in decision-making and learning program adjustments.
- Enabling Customers to analyze Learner performance data to identify trends, skill gaps, and opportunities for improvement.
- Enabling Customers to generate and deliver personalized learning paths and training recommendations based on Learner interactions.

Notes Regarding Customer Use of Authorized User Data. While ELB does not control the specific use of Authorized User Data by Customers, it is important to note that under the terms of our [Subscription and License Agreement](#) (SALA), Customers contractually agree to use this data responsibly and ethically. Specifically, Customers agree to:

- Refrain from using Authorized User Data in ways that would violate any applicable local, state, national, and international laws and regulations, including but not limited to those pertaining to data protection, privacy, non-discrimination, and employment. Our [SALA](#) outlines these restrictions to ensure that all data usage aligns with legal standards and ethical practices.
- Ensure that the AI Functionality is used in compliance with applicable AI Provider's terms and conditions and in compliance with Customer's own policies, including any AI policy.
- Ensure that the [AI Functionality](#) is not used as the sole basis for making decisions that could significantly affect the rights and freedoms of individuals, especially in contexts related to employment, credit eligibility, healthcare decisions, insurance underwriting and claims, or any other decision-making processes that could lead to legal or significant personal impacts.

Customer is solely responsible for ensuring that the use of AI Functionality in decision-making processes adheres to all relevant legal standards and ethical guidelines, including obtaining necessary consents and providing requisite disclosures and explanations to affected individuals.

3. Protection of ELB's Legal Rights. ELB may share Authorized User Data as necessary to protect its legal rights, enforce its agreements, and defend against legal claims, including those that may arise from contractual relationships with Customers. This includes sharing data to respond to court orders, legal processes, or to establish, exercise, or defend legal claims related to our Subscription Services. Such sharing will be conducted in compliance with applicable laws and regulations to ensure the protection of all parties' legal interests.

NOTE REGARDING SELLING & SHARING FOR MARKETING PURPOSES: Whether or not an Authorized User is a "consumer" or "data subject" under any personal data regulation restricting or prohibiting the "sale" or "sharing for marketing purposes" of such (e.g., see [California Privacy Notice](#)), ELB commits to its Customers under the [DPA](#) to not sell any Authorized User personal data and to restrict its sharing other use of Authorized User personal data for marketing purposes as set forth [above](#).

V. DATA RETENTION AND SECURITY

A. Data Retention.

1. **Standard Personal Data.** ELB retains Standard Personal Data for as long as necessary to fulfill the purposes for which it was collected, including any legal, accounting, or reporting requirements, and to comply with our data processing obligations. Further, in accordance with data protection laws, data collection is limited to what is relevant and necessary for the intended purposes. We determine the appropriate retention period for Standard Personal Data on the basis of the amount, nature, and sensitivity of the data being processed, the potential risk of harm from unauthorized use or disclosure of the data, whether we can achieve the purposes of the processing through other means, and on the basis of applicable legal requirements (such as applicable statutes of limitation).
2. **Authorized User Personal Data.** When acting merely as a processor under GDPR or a service provider under CCPA, ELB processes personal data on behalf of our Customers that facilitate access to the ELB Solutions. Retention periods for personal data processed in the role of processor or service provider are determined by the Customer. Generally, we maintain this personal data for as long as our agreement with the applicable Customer provides. However, ELB is contractually obligated, and obliged under applicable data privacy regulations, to process personal data according to the Customer's instructions. This may include deleting data at any time upon the Customer's request.

B. Data Security. ELB is committed to protecting the personal data we hold and keeping it secure by taking appropriate technical and organizational measures against its unauthorized or unlawful processing and against its accidental loss, destruction, or damage. Such measures include the following:

1. **Technical Measures.** ELB implements robust technical security measures including encryption, secure network architectures, and identity and access management controls.
2. **Physical Security.** Physical access to our facilities and AWS data centers is controlled and monitored with modern security systems.
3. **Organizational Measures.** ELB maintains a documented security program that includes employee training, incident management, and regular audits.
4. **Continuous Improvement.** Security measures are continually evaluated and updated to address new and emerging threats.

For further Subscription Service specific data security information, please see the applicable ELB's Subscription Service [Security Program Overview](#).

Where we use third-party service providers to store data, we have appropriate agreements in place to ensure that your personal data is protected. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. We also require any third parties to whom we may transfer personal data to have appropriate security measures in place. They agree to only process your personal data on our instructions and they are subject to a duty of confidentiality.

While ELB employs robust technical and organizational measures to protect your personal data, it is important to recognize that no system can be completely secure. Therefore, while we strive to use commercially acceptable means to protect your personal data, we cannot guarantee its absolute security. We encourage you to exercise caution when providing personal information online and use security measures to protect your personal data, such as using strong passwords and ensuring that your personal devices are protected against malware and unauthorized access.

VI.YOUR RIGHTS

A. Universal Rights. ELB is committed to ensuring you have control over your personal data. Below are the rights you can exercise regardless of your location or jurisdiction of residence.

1. **Opting Out of Marketing Communications.** You have the right to opt out of receiving marketing communications from us at any time. To unsubscribe from our emails, you can follow the unsubscribe link at the bottom of each marketing email or contact us directly according to the [Contact Information](#) section. This will remove you from our email marketing lists.

2. **Cookie Preferences.** You have the right to control and manage cookies via the tools set forth in our [Cookie Policy](#). There, you can find detailed information on how to adjust your browser settings to decline cookies and how to manage other technologies that track your website usage. By adjusting these settings, you can enhance your privacy while using the ELB Websites and Solutions.
3. **Access and Changing Information.** ELB may provide mechanisms or processes allowing you to delete, correct, or update some of the personal data that we collect from you, and potentially certain other information about you (e.g., profile and account information). We will make good faith efforts to make requested changes in our then-active databases as soon as practicable, but it is not always possible to completely change, remove or delete all of your information from our databases and residual and/or cached data may remain archived thereafter. Further, we reserve the right to retain data: (a) as required by applicable law; and (b) for so long as reasonably necessary to fulfill the purposes for which the data is retained except to the extent prohibited by applicable law.

B. Regional Specific Rights. Your personal data may be stored in, transferred to, and processed in the United States and in any other country in which we, and/or service providers maintain facilities. The data protection laws in these countries may provide a different standard of protection for personal data than the country in which you are located or your country of residence. We may choose or be required by law to provide different or additional disclosures about our data privacy practices depending on your state or country of residence:

1. **European Economic Area, United Kingdom or Switzerland.** If you are located in the European Economic Area (“**EEA**”), or the United Kingdom (“**UK**”), or Switzerland, please see the [European Privacy Notice](#) for additional European-specific privacy information, including what constitutes your personal data, the lawful bases we rely on to process your personal data, and your rights in respect of your personal data.
2. **California.** If you are a California resident, please see the [California Privacy Notice](#).

For any concerns or questions about how we handle your personal data and your rights over it, please contact us according to the [Contact Information](#) section. We are committed to addressing your inquiries and providing the necessary support to exercise your rights.

VII. UPDATES TO THIS PRIVACY POLICY

ELB has the discretion to update this Privacy Policy at any time. When we do, we will revise the updated date at the bottom of this page. We encourage you to frequently check this page for any changes to stay informed about how we are helping to protect the personal data we collect. You acknowledge and agree that it is your responsibility to review this Privacy Policy periodically and become aware of modifications.

VIII. CONTACT INFORMATION

If you have any questions about this Privacy Policy, the operation of an ELB Website, or your use of an ELB Solution, please contact us at:

55 N. Merchant Street, #1221

American Fork, UT 84003

801.796.2767

privacy@elblearning.com

EUROPEAN PRIVACY NOTICE

This European Privacy Notice (“**European Notice**”) supplements the information contained in ELB's Privacy Policy and applies solely to individuals located in the European Economic Area (EEA), the United Kingdom

(UK), and Switzerland. As a U.S. company, ELB Learning processes personal data in accordance with applicable data protection laws, including the EU General Data Protection Regulation (GDPR), the UK Data Protection Act, and the Swiss Federal Data Protection Act.

I. DATA CONTROLLER AND DATA PROTECTION OFFICER

ELB Learning (registered as Plato eLearning, LLC) is the [data controller](#) for [Standard Personal Data](#) collected in connection with our European operations. For [Authorized User Personal Data](#) provide to ELB the applicable Customer is the controller and ELB processes such data as the Customer's [data processor](#). Those Product Partners who share Authorized User Personal Data with ELB on behalf of a Customer do so as a [data processor](#) of the Customer and, accordingly, ELB treats such data as though it was provided directly by the Customer.

Contact Information:

Plato eLearning, LLC (d/b/a ELB Learning)

55 N. Merchant Street, #1221

American Fork, UT 84003

801.796.2767

privacy@elblearning.com

In compliance with Article 27 of the EU General Data Protection Regulation (GDPR) and the UK GDPR, ELB Learning has appointed representatives in the European Union and the United Kingdom.

EU Representative

Rickert Rechtsanwaltsgesellschaft mbH,

Colmantstrasse 15, 53115 Bonn,

Germany

Email: art-27-rep-elblearning@rickert.law

UK Representative

Rickert Rechtsanwaltsgesellschaft mbH,

Colmantstrasse 15, 53115 Bonn,

Germany

Email: art-27-rep-elblearning@rickert-services.uk

II. PERSONAL DATA / PURPOSES OF PROCESSING / LEGAL BASIS AND PROCESSED

In the chart below, we outline the types of personal data collected from individuals located in the European Economic Area (EEA), United Kingdom (UK), and Switzerland, the purposes of processing, and the corresponding legal bases under GDPR and other applicable data protection laws.

NOTE REGARDING AUTHORIZED USER PERSONAL DATA: Notwithstanding anything set forth in the chart below, the limitations and restrictions ELB commits to in the [DPA](#) apply to ELB's use of Authorized User personal data (See [Important Note Regarding ELB's Contractual Commitments to Customers](#)).

Personal Data Categories	Examples	Purposes of Collection	Legal Basis for Processing
Identifiers	Name, email address, phone number, IP address, unique online identifier	<ul style="list-style-type: none"> - Providing and managing ELB Websites & Solutions - Communicating with users via newsletters, promotions, & updates - Authenticating user accounts - Personalizing user experience 	<ul style="list-style-type: none"> - Contract fulfillment (Art. 6(1)(b) GDPR) - Legitimate interests (Art. 6(1)(f) GDPR) - Consent (Art. 6(1)(a) GDPR)
Professional or Employment-Related Information	Job title, employer, business contact information	<ul style="list-style-type: none"> - Providing & managing ELB Subscription Services - Customizing learning paths & training programs - Providing customer support to Authorized Users 	<ul style="list-style-type: none"> - Contract fulfillment (Art. 6(1)(b) GDPR) - Legitimate interests (Art. 6(1)(f) GDPR)
Internet or Other Electronic Network Activity Information	Browsing history, search history, interactions with ELB Websites & Solutions	<ul style="list-style-type: none"> - Monitoring & improving ELB Websites & Solutions - Personalizing content based on user preferences - Security & fraud detection 	<ul style="list-style-type: none"> - Legitimate interests (Art. 6(1)(f) GDPR)
Audio/Visual Data	Videos or audio submitted by learners	<ul style="list-style-type: none"> - Providing feedback, scoring, & assessment reports - Generating personalized learning paths - Improving learning content & recommendations 	<ul style="list-style-type: none"> - Contract fulfillment (Art. 6(1)(b) GDPR) - Legitimate interests (Art. 6(1)(f) GDPR)
Geolocation Data	Approximate location based on IP address	<ul style="list-style-type: none"> - Personalizing user experience - Providing location-based training resources 	<ul style="list-style-type: none"> - Consent (Art. 6(1)(a) GDPR) - Legitimate interests (Art. 6(1)(f) GDPR)
Inferences Drawn from Other Personal Data	AI-generated inferences & insights regarding communication style, skill proficiency, & overall performance	<ul style="list-style-type: none"> - Providing personalized feedback & learning paths - Improving learning content & recommendations - Suggesting relevant training resources 	<ul style="list-style-type: none"> - Legitimate interests (Art. 6(1)(f) GDPR) - Consent (Art. 6(1)(a) GDPR)
Education Information	Information related to learner assessments, training progress, & educational achievements	<ul style="list-style-type: none"> - Providing & managing ELB Subscription Services - Customizing learning paths & training programs - Providing customer support to Authorized Users 	<ul style="list-style-type: none"> - Contract fulfillment (Art. 6(1)(b) GDPR) - Legitimate interests (Art. 6(1)(f) GDPR)
Sensitive/Special Categories of Personal Data	Financial data (if applicable for transactions), demographic data (e.g., race, ethnicity), & precise geolocation (if requested by Customer)	<ul style="list-style-type: none"> - Financial data: Facilitating transactions (if applicable) - Demographic and/or Precise Geolocation: Provided to Customers in support of its use of the Subscription Services 	<ul style="list-style-type: none"> - Explicit consent (Art. 9(2)(a) GDPR) - Legitimate interests (Art. 6(1)(f) GDPR)

III. INTERNATIONAL TRANSFERS

Some of our processing of your data will involve transferring your data outside the EEA, UK, and/or Switzerland. Some of our external third-party service providers are also based outside of the EEA, UK, and/or Switzerland, and their processing of your personal data will involve a transfer of data outside the EEA, UK, and/or Switzerland. This includes the United States. Where personal data is transferred to and stored in a country not determined by the European Commission, the UK's Department for Digital, Culture, Media & Sport

(DCMS), or the Swiss Federal Counsel, as applicable, providing adequate levels of protection for personal data, we take steps to provide appropriate safeguards to protect your personal data, including entering into standard contractual clauses approved by the applicable regulator, obliging recipients to protect your personal data.

IV. DATA RETENTION

For more details on our data retention practices, please refer to Section V of our Privacy Policy.

IV. YOUR RIGHTS

NOTE FOR AUTHORIZED USERS: If you are an Authorized User and we are processing your personal data solely as a data processor on behalf of Customer that facilitated your access to the ELB Solutions, please direct your request to the applicable Customer. Given our limited role as a data processor, we cannot handle your request directly.

- A. Right of access to your personal data.** You have the right to ask us for confirmation on whether we are processing your personal data, and access to the personal data and related information.
- B. Right to correction.** You have the right to have your personal data corrected, as permitted by law.
- C. Right to erasure.** You have the right to ask us to delete your personal data, as permitted by law.
- D. Right to withdraw consent.** You have the right to withdraw consent that you have provided.
- E. Right to lodge a complaint with a supervisory authority.** You have the right to lodge a complaint with a supervisory authority in the member state of your habitual residence.
- F. Right to restriction of processing.** You have the right to request the limiting of our processing under limited circumstances.
- G. Right to data portability.** You have the right to receive the personal data that you have provided to us, in a structured, commonly used, and machine-readable format, and you have the right to transmit that information to another controller, including to have it transmitted directly, where technically feasible.
- H. Right to object.** You have the right to object to our processing of your personal data, as permitted by law, under limited circumstances.

In order to exercise any of these rights, please contact us according to the [Contact Information](#) section.

Please note that the above rights are not absolute and we may be entitled to refuse requests, wholly or partly, where exceptions under the applicable law apply. If you are not satisfied with our response, you may lodge a complaint with your local data protection authority as provided below.

V. COMPLAINTS

If you have any concerns about how ELB processes your personal data, you can file a complaint with your local data protection authority.

For EU residents:

European Union residents can also contact the relevant data protection authority in their country of residence. You can find the contact details of your local Data Protection Authority [here](#).

For UK residents:

Information Commissioner's Office (ICO)

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Telephone: +44 (0) 303 123 1113

Website: ico.org.uk

For Swiss residents:

Federal Data Protection and Information Commissioner (FDPIC)

Feldeggweg 1, CH - 3003 Berne, Switzerland

Telephone: +41 (0)58 462 43 95

Email: info@fedpol.admin.ch

Website: <https://www.edoeb.admin.ch/edoeb/en/home.html>

VI. CHANGES TO THIS NOTICE

We may update this European Privacy Notice from time to time in response to changing legal, technical, or business developments. Any changes will be posted on this page with an updated effective date. Where appropriate, we may also notify you via email or other direct communication.

CALIFORNIA PRIVACY NOTICE

The California Consumer Privacy Act (“**CCPA**”) as amended by the California Privacy Rights Act of 2020 (“**CPRA**”), hereafter referred to as CCPA, provides California Consumers certain rights regarding their personal information (“**PI**”) as those terms are defined in the CCPA. We are providing you with notice of the PI we collect, and our purposes for that collection of data that may be subject to the CCPA (“**CCPA Notice**”). This CCPA Notice supplements ELB’s Privacy Policy and applies solely to residents of California.

I. NOTICE OF COLLECTION / PURPOSES / SHARING

ELB collects various categories of personal information from California residents, which include identifiers, professional or employment-related information, education information, and internet activity, among others. Detailed information about the categories of personal information we collect is provided in the chart below.

We collect personal information for various business purposes such as providing the ELB Websites and Solutions, communicating with you, improving our offerings, and complying with legal requirements. The specific purposes for collecting and using personal information are outlined in the chart below.

Under the CCPA, a “sale” is defined as selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating personal information to a third party for valuable consideration. “Sharing” refers to disclosing personal information to a third party for cross-context behavioral advertising, whether or not for monetary consideration.

ELB does not sell personal information but may share personal information (other than that of Authorized Users) with certain third parties, such as marketing partners, to provide targeted advertising. The 3rd parties with which we may share personal information are described in the chart below.

To opt out of such sharing, please contact us according to the [Contact Information](#) section.

This chart provides details regarding the categories of personal information collected, the purposes of collection, and the sharing practices of ELB in compliance with the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).

NOTE REGARDING AUTHORIZED USER PERSONAL DATA: Notwithstanding anything set forth in the chart below, the limitations and restrictions ELB commits to in the [DPA](#) apply to ELB’s use of Authorized User personal data (See [Important Note Regarding ELB’s Contractual Commitments to Customers](#)).

Personal Information Categories	Examples	Purposes of Collection	Third Parties Shared With
Identifiers	Name, email address, phone number, IP address, unique online identifier	<ul style="list-style-type: none"> - Providing & managing ELB Websites and Solutions - Communicating with users via newsletters, promotions, & updates - Authenticating user accounts - Personalizing user experience 	<ul style="list-style-type: none"> - Service Providers (e.g., email marketing platforms, customer relationship management) - Product Partners (e.g., courseware platforms, LMS integrators) - Advertising Networks
Professional or Employment-Related Information	Job title, employer, business contact information	<ul style="list-style-type: none"> - Providing and managing ELB Subscription Services - Customizing learning paths & training programs - Providing customer support to Authorized Users 	<ul style="list-style-type: none"> - Service Providers (e.g., customer relationship management platforms) - Product Partners (e.g., courseware platforms, LMS integrators)
Internet or Other Electronic Network Activity Information	Browsing history, search history, interactions with ELB Websites and Solutions	<ul style="list-style-type: none"> - Monitoring & improving ELB Websites and Solutions - Personalizing content based on user preferences - Security & fraud detection 	<ul style="list-style-type: none"> - Service Providers (e.g., analytics platforms) - Advertising Networks
Audio/Visual Data	Videos or audio submitted by learners	<ul style="list-style-type: none"> - Providing feedback, scoring, and assessment reports - Generating personalized learning paths - Improving learning content & recommendations 	<ul style="list-style-type: none"> - Service Providers (e.g., video processing platforms) - Product Partners (e.g., courseware platforms)
Geolocation Data	Approximate location based on IP address	<ul style="list-style-type: none"> - Personalizing user experience - Providing location-based training resources 	<ul style="list-style-type: none"> - Service Providers (e.g., analytics platforms)
Inferences Drawn from Other Personal Information	AI-generated inferences and insights regarding communication style, skill proficiency, & overall performance	<ul style="list-style-type: none"> - Providing personalized feedback and learning paths - Improving learning content & recommendations - Suggesting relevant training resources 	<ul style="list-style-type: none"> - Service Providers (e.g., AI analytics platforms)
Education Information	Information related to learner assessments, training progress, and educational achievements	<ul style="list-style-type: none"> - Providing & managing ELB Subscription Services - Customizing learning paths and training programs - Providing customer support to Authorized Users 	<ul style="list-style-type: none"> - Service Providers (e.g., customer relationship management platforms) - Product Partners (e.g., courseware platforms, LMS integrators)
Sensitive Personal Information	Financial data (if applicable for transactions), demographic data (e.g., race, ethnicity), & precise geolocation (if requested by Customer)	<ul style="list-style-type: none"> - Financial data: Facilitating transactions (if applicable) - Demographic and/or Precise Geolocation: Provided to Customers in support of its use of the Subscription Services 	<ul style="list-style-type: none"> - Service Providers (e.g., payment processors, analytics platforms)

V. DATA RETENTION

For more details on our data retention practices, please refer to Section V of our Privacy Policy.

II. RIGHTS OF CALIFORNIA CONSUMERS

If you are a California Consumer and would like to exercise the rights afforded you under the CCPA (as identified below) please contact us according to the [Contact Information](#) section. You have the right to not receive discriminatory treatment in a manner prohibited by the CCPA because you exercise your rights under the CCPA.

To fulfill your CCPA request, we may require you to provide sufficient information to reasonably verify you are the California Consumer about whom we collected PI. This verification process may include providing us at least two unique data points, depending on the type of request.

California Consumers have the right to exercise CCPA privacy rights via an authorized agent who meets the agency requirements of the CCPA. Authorized agent requests must include a copy of the agency agreement between the authorized agent and the California Consumer. We will ask you to independently confirm the agency relationship if this section applies to you.

NOTE FOR AUTHORIZED USERS: If you are an Authorized User and we are processing your personal information solely as a service provider on behalf of the Customer that facilitated your access to the ELB Solutions, please direct your data privacy inquiries and requests to exercise your California privacy rights to the applicable Customer. As a service provider operating under the instructions of the Customer, ELB does not have the authority to act on such requests directly.

- A. The Right to Know Categories of Information.** You have the right, subject to statutory exceptions, to send us a request, no more than twice in a twelve-month period, for any of the following, for the period that is twelve months prior to the request date:
- the categories of PI we have collected about you;
 - the categories of sources from which we collected your PI;
 - the business or commercial purposes for our collecting or selling your PI;
 - the categories of third parties to whom we have shared your PI; and
 - a list of the categories of PI disclosed for a business purpose in the prior 12 months, or that no disclosure occurred.
- B. Right to Know Specific Pieces of Information.** You have the right, subject to statutory exceptions, to make or obtain a transportable copy, no more than twice in a twelve-month period, of your PI that we have collected in the period that is 12 months prior to the request date and are maintaining.
- C. The Right to Deletion.** You have the right, subject to statutory exceptions, to request that we delete your PI that we have collected directly from you and are maintaining. Note also that we are not required to delete your PI that we did not collect directly from you.
- D. Right to Correct.** You have the right to request we correct inaccuracies in PI we maintain about you.
- E. The Right to Opt-Out of the Sale or Sharing of Personal Information.** We may work with service providers and partner with advertising companies that use [cookies](#) to collect information about your visits to ELB Websites and your use of ELB Solutions, and then use that information to deliver advertisements relevant to your interests. Use of cookies associated with ELB Websites or Solutions may or may not be deemed to constitute a “sale” or “sharing” of your PI as defined by the CCPA. Regardless of any such classification, you may opt out of Interest-based Advertising using ad industry opt out tools identified [here](#). To effectively manage cookies via these tools, you must set preferences on all browsers and all devices that you use. If you clear the cookies on your device, you may need to set your cookie preferences again.

We are not responsible for the completeness, accuracy or effectiveness of any third-party programs, tools or frameworks, or the information they provide.

Please note that the rights outlined in the CCPA/CPRA are not absolute, and we may be entitled to refuse requests, wholly or partly, where exceptions under the applicable law apply.

California residents can file complaints with the California Privacy Protection Agency If they are dissatisfied with the handling of their privacy request or our response.

California Privacy Protection Agency

2101 Arena Blvd

Sacramento, CA 95834

Telephone: (916) 572-2900

Web Portal: <https://coppa.ca.gov/webapplications/complaint>

III. CALIFORNIA'S "SHINE THE LIGHT" LAW.

If you are a California resident, in addition to the rights set forth above, California's "Shine the Light" law permits customers in California to request certain details about how their personal information is shared with third parties if that personal information is shared for those third parties' own direct marketing purposes. We do not share personal information with third parties for those third parties' own direct marketing purposes. Californians may request information about our compliance with this law by contacting us according to the [Contact Information](#) section.

To make a request, please provide sufficient information for us to determine if this applies to you, attest to the fact that you are a California resident and provide your current California address to which we will send our response. Your inquiry must specify "California Privacy Rights Request" in the subject line of the email or the first line of the letter and include your name, street address, city, state, and ZIP code. Please note that we are only required to respond to one request per customer each year.

Previous Versions

ELB Learning Privacy Policy_v1_(14Mar2024)