ELB LEARNING AND GDPR

At ELB Learning, we are committed to protecting the privacy and security of our Customers' and users' personal data. As a U.S.-based company, we recognize the importance of adhering to the European Union's General Data Protection Regulation (GDPR) and other data protection laws.

Our Approach To GDPR Compliance

1. **Data Processing Addendum (DPA)**

   We provide a comprehensive Data Processing Addendum (DPA) that outlines our responsibilities as a data processor on behalf of our Customers. The DPA includes information on data handling, security measures, and data subject rights, ensuring compliance with GDPR requirements.

2. **Privacy Policy and Cookie Notice**

   Our Privacy Policy provides information about how we collect, use, and share personal data in accordance with GDPR requirements, including:

   - Data Collection and Use: Disclosing the categories of personal data we collect, the purposes of processing, and the legal bases.
   - Data Subject Rights: Explaining the rights of data subjects under GDPR, such as the right to access, rectify, erase, and restrict processing of personal data.
   - Data Sharing and Transfers: Describing our data sharing practices with third parties and safeguards for international data transfers.

   Our Cookie Policy provides information on how cookies and similar technologies are used on ELB Websites and Solutions, including:

   - Technical Forms and Categories of Cookies: Explanation of different cookie technologies, including essential, performance, functionality, advertising, and analytics cookies.
   - Personal Data Collected via Cookies: Explanation of the personal data collected through cookies, such as browsing history, IP address, and device identifiers.
   - Tracking Choices: Instructions on managing cookies through browser settings and opt-out tools.
   - Opt-In Management of Non-Essential Cookies: Ensuring that non-essential cookies (e.g., advertising and analytics) are used only with user consent, as required by GDPR.

3. **Data Security Measures**
   - Access Controls:
     - Strict access control policies ensure that only authorized personnel can access personal data.
   - Encryption and Anonymization:
     - Personal data is encrypted in transit and at rest, and anonymization or pseudonymization is used where appropriate.
   - Incident Response Plan:
     - We have a comprehensive incident response plan to detect, respond to, and recover from data breaches promptly.
   - SOC 2 Compliance:
     - We have substantially implemented SOC 2 security standards to strengthen our data security framework and ensure the confidentiality, integrity, and availability of personal data. We are actively seeking certification to further demonstrate our commitment to data security.

4. **Vendor Management**

   We maintain a rigorous vendor management program to ensure that all third-party vendors adhere to GDPR and our data protection standards. We rigorously vet our vendors and service providers to ensure compliance with our data security and privacy standards. This includes:

   - Conducting thorough due diligence to assess their security measures.
   - Implementing data processing agreements that align with GDPR requirements.

5. **Rights of Data Subjects**

We support our Customers in meeting data subject rights under GDPR, including the right to access, rectify, erase, and restrict processing of personal data. For Authorized Users, these rights can be exercised directly through the applicable Customer.

6. **European Representatives & Supervisory Authority**

In compliance with Article 27 of the GDPR, ELB has appointed representatives in the European Union and the United Kingdom to facilitate GDPR compliance and data subject rights. As ELB does not maintain affiliates or a physical presence in the EU (i.e., is not "established in the Union" as defined under the GDPR), it is not subject to the jurisdiction of any specific EU supervisory authority. However, any relevant supervisory authority within the EU retains the authority to enforce compliance and address grievances related to our data processing activities.

7. **Commitment to Continuous Improvement**

We are committed to continuous improvement in our privacy and security practices. Therefore, the policies and agreements identified above are constantly updated to reflect changes in regulations and the rapid pace of emerging technologies like AI. Our objective is to ensure that our Customers' personal data remains protected and that we consistently meet the highest standards of data privacy and security.

8. **EU-US Privacy Framework Agreement**

ELB's GDPR compliance program does not include participation in the EU-US Data Privacy Framework (the "Framework"). To ensure lawful transfers from the EU to the U.S., ELB enters into Standard Contractual Clauses (SCCs) as part of its DPA. As a company that does not maintain affiliates or a physical presence in the EU (i.e., is not "established in the Union" as defined under the GDPR), our decision to utilize the SCCs rather than participate in the Framework was influenced by several factors, including the following:

- Simplicity and Efficiency: Use of SCCs allows ELB to maintain streamlined and consistent data protection practices across all jurisdictions. This approach not only simplifies compliance processes but also ensures that these processes are deeply integrated with the company's broader global data governance policies.

- Tailored Data Protection Commitments: The SCCs provide the flexibility to tailor data protection commitments directly to the needs and expectations of both ELB and its EU Customers. This tailored approach is particularly advantageous because it allows for precise alignment with the specific data handling and security requirements of Customers, enhancing mutual confidence and trust in the business relationship.

- Legal Clarity and Predictability: Utilizing SCCs offers a clear and legally predictable framework for data transfers between the EU and the U.S., providing a well-defined legal basis for data processing activities. This approach not only meets GDPR standards but also addresses the instability of previous frameworks like Safe Harbor and Privacy Shield, which faced legal challenges and invalidations. By choosing SCCs, ELB ensures a more reliable and secure method for managing transatlantic data transfers, enhancing trust with its EU Customers.