PRIVACY POLICY

(Safelora – www.safelora.com)

ARTICLE I: INTRODUCTION AND PURPOSE

1.1 *Objective of this Policy.*
This Privacy Policy (the "Policy") is issued by Safelora ("Safelora," "we," "us," or "our") to explain how we collect, process, store, share, and protect personal data of individuals ("Users," "Consumers," or "you") who access or purchase pre-recorded cybersecurity training courses through our website www.safelora.com.

1.2 *Legal Foundations.*
This Policy has been prepared to comply with:
(a) Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR).
(b) Spanish Organic Law 3/2018 on Data Protection and Digital Rights (LOPDGDD).
(c) Applicable guidance of the European Data Protection Board (EDPB) and the Spanish Data Protection Authority (AEPD).

ARTICLE II: DATA CONTROLLER AND CONTACT

2.1 *Identity of the Controller.*
The data controller responsible for your personal data is:
Safelora
Street 534, Number 20, La Cañada, Paterna, Valencia, Spain
Email: admin@safelora.com

2.2 Data Protection Officer.
At present, Safelora has not appointed a mandatory Data Protection Officer, as our core activities do not involve large-scale monitoring of sensitive data. However, privacy-related inquiries may be directed to admin@safelora.com. If in future a DPO is appointed, updated contact details will be published promptly.

2.3 *User Inquiries.*
All Users may exercise their privacy rights or direct questions about this Policy by writing to admin@safelora.com. Safelora may require verification of identity before responding.

ARTICLE III: CATEGORIES OF PERSONAL DATA COLLECTED

3.1 *Information You Provide Directly.*
When registering, purchasing, or communicating with us, you may provide:
(a) Identity Data – full name, username, date of birth (where necessary for verification).
(b) Contact Data – email address, billing address, phone number (optional).
(c) Account Data – login credentials, course selections, preferences.
(d) Payment Data – transaction identifiers, billing details (payment credentials are processed only by third-party providers).

(e) Support Data – information contained in support tickets, chat messages, or email correspondence.

3.2 *Information Collected Automatically.*
We may automatically collect:
(a) Device and Technical Data – IP address, browser type, operating system, device identifiers.
(b) Telemetry Data – access logs, course progress records, session duration, LMS interactions.
(c) Cookies and SDK Data – as detailed in our Cookie Policy, subject to consent where required.

3.3 *Information from Third Parties.*
We may receive confirmation of payments or fraud alerts from payment processors (e.g., PayPal, Stripe, card acquirers) and technical incident data from hosting and LMS providers.

3.4 *Sensitive Data.*
Safelora does not intentionally process sensitive categories of data (health, political, biometric, religious, or otherwise special categories under GDPR Art. 9). Users are instructed not to submit such data to Safelora.

ARTICLE IV: LEGAL BASES AND PURPOSES OF PROCESSING

4.1 *Overview.*
We process personal data strictly within the boundaries of GDPR Article 6, selecting the appropriate legal basis depending on the purpose.

4.2 *Matrix of Purposes and Legal Bases.*
(a) *Account Registration & Course Access:* Necessary for contract performance (Art. 6(1)(b)).

(b) *Payment Processing & Fraud Prevention:* Contract performance (Art. 6(1)(b)); compliance with legal obligations (tax/PSD2) (Art. 6(1)(c)); and legitimate interests in fraud prevention (Art. 6(1)(f)).

(c) *Customer Support:* Contract performance (Art. 6(1)(b)); legitimate interest in service continuity (Art. 6(1)(f)).

(d) *Marketing Communications:* Consent obtained (Art. 6(1)(a)).

(e) *Analytics and Tracking:* Consent where non-essential (Art. 6(1)(a)); legitimate interest for essential analytics ensuring system integrity (Art. 6(1)(f)).

(f) *Legal Compliance:* Processing to comply with tax, accounting, or consumer protection laws (Art. 6(1)(c)).

(g) *Security and Enforcement:* Legitimate interest in protecting systems, IP rights, and enforcing policies (Art. 6(1)(f)).

ARTICLE V: CHILDREN AND MINORS

5.1 *Age of Digital Consent.*
In accordance with the LOPDGDD, Safelora does not knowingly process data of children under the age of 14 without verified parental authorization.

5.2 *Parental Consent.*
Where a minor between 14 and 18 registers, we may request verification of parental consent. If such authorization is not verifiable, access shall be denied.

5.3 *Discovery of Underage Users.*
If Safelora becomes aware that personal data of a child under 14 has been collected without consent, we will promptly delete such data and terminate the related account.

ARTICLE VI: SOURCES OF DATA

6.1 *Direct Sources.*
Data provided directly by Users through registration, checkout, or communication.

6.2 *Automated Sources.*
Data collected through cookies, LMS monitoring, and device logs.

6.3 *Processor Sources.*
Data communicated by our third-party providers (e.g., payment confirmation, fraud prevention alerts, error logs).

ARTICLE VII: RECIPIENTS OF DATA AND PROCESSORS

7.1 *General Rule.*
Safelora does not sell personal data. However, we share data with third parties strictly as required for service provision, under GDPR-compliant Data Processing Agreements.

7.2 *Categories of Recipients.*
(a) Hosting Providers – cloud infrastructure located within the EEA or with adequate safeguards.

(b) Learning Management System Providers – platforms integrated into Tutor LMS.

(c) Payment Processors – Stripe, PayPal, and card acquirers.

(d) Email and Communication Platforms – for account notifications, support responses, and marketing (where consent exists).

(e) Analytics Tools – used only after valid consent, unless essential for system functioning.

(f) Legal Authorities – where required by law or judicial order.

ARTICLE VIII: INTERNATIONAL TRANSFERS

8.1 *General Principle.*
Safelora may transfer data outside the EEA where necessary for hosting, payment, communication, or analytics services.

8.2 *Adequacy Decisions.*
Where transfers are made to countries recognized by the European Commission as providing adequate protection, no additional authorization is required.

8.3 *Standard Contractual Clauses (SCCs).*
For transfers to non-adequate jurisdictions (e.g., United States), Safelora relies on SCCs adopted by the European Commission, supplemented by additional technical and organizational measures.

8.4 *Key Processors Outside EEA.*
(a) Payment processors (Stripe, PayPal – US-based).
(b) Email platforms (may operate servers outside the EEA).
(c) Cloud providers (where applicable).

8.5 *User Acknowledgment.*
By using our services, you acknowledge that some of your data may be processed outside the EEA subject to these safeguards.

ARTICLE IX: DATA RETENTION

9.1 *General Retention Principles.*
Safelora retains data only as long as necessary to fulfill contractual obligations, legal requirements, and legitimate interests, after which data is securely deleted or anonymized.

9.2 *Specific Retention Schedules.*
(a) Account Data – retained for the duration of the User's account plus 12 months post-termination for dispute handling.
(b) Payment/Invoice Data – retained for 6 years in accordance with Spanish tax and accounting law.
(c) Course Progress Data – retained for as long as the account remains active; deleted upon request or account deletion.
(d) Support Tickets – retained for 24 months to allow proper follow-up and quality audits.
(e) Cookies – retained in accordance with our Cookie Policy, varying from session-only to up to 24 months depending on consent and type.

Note: Safelora reserves the right to extend retention where necessary to protect against fraud, enforce contractual rights, or comply with legal obligations.

ARTICLE X: DATA MINIMIZATION AND ACCURACY

10.1 *Minimization.*
We commit to collecting only the data strictly required for stated purposes.

10.2 *User Responsibility.*
Users are responsible for ensuring their data is accurate and up to date. Failure to provide accurate information may impair Safelora's ability to provide services and may lead to account suspension.

10.3 *Periodic Review.*
Safelora periodically reviews stored data to ensure accuracy and relevance, deleting or anonymizing data no longer required.

ARTICLE XI: SECURITY MEASURES

11.1 *Organizational Measures.*
Safelora implements internal protocols to ensure that only authorized staff and processors have access to personal data. Access is restricted on a need-to-know basis, and employees are bound by confidentiality obligations.

11.2 *Technical Measures.*
Data is secured through encryption in transit (TLS/SSL) and at rest where applicable. Systems are monitored with logging and intrusion detection tools.

11.3 *Payment Security.*
Safelora does not store payment card details. All financial transactions are handled by third-party providers compliant with PCI-DSS standards and PSD2 Strong Customer Authentication (SCA) rules.

11.4 *Incident Response.*
In the event of a personal data breach, Safelora shall notify the competent supervisory authority (AEPD) within 72 hours where required, and affected Users without undue delay when high risk to their rights and freedoms exists.

11.5 *User Responsibility.*
Users must safeguard their login credentials and devices. Safelora is not responsible for unauthorized access resulting from negligence in protecting account details.

ARTICLE XII: RIGHTS OF USERS (DATA SUBJECTS)

12.1 *Overview.*
Users enjoy the full spectrum of GDPR rights, exercisable by contacting admin@safelora.com. Safelora will respond within one month, extendable by two months in complex cases, with reasons provided.

12.2 *Right of Access.*

You may obtain confirmation of whether we process your personal data and access a copy, including information on processing purposes, categories, recipients, retention, and safeguards for international transfers.

12.3 *Right of Rectification.*
You may request correction of inaccurate data or completion of incomplete data without undue delay.

12.4 *Right of Erasure ("Right to be Forgotten").*
You may request deletion of your data where:
(a) It is no longer needed for its original purpose.
(b) Consent is withdrawn and no other lawful basis exists.
(c) You object to processing and no overriding legitimate interest exists.
(d) Processing was unlawful.
(e) Deletion is required by law.
Safelora may refuse erasure where retention is legally required (e.g., invoices for tax purposes).

12.5 *Right to Restriction.*
You may request processing restriction while accuracy is verified, legality contested, or pending an objection.

12.6 *Right to Portability.*
You may request a structured, machine-readable copy of your data and transmit it to another controller where processing is based on consent or contract.

12.7 *Right to Object.*
You may object to processing based on legitimate interests or direct marketing. Safelora will cease processing unless compelling legitimate grounds exist.

12.8 *Automated Decisions.*
You have the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects, except as provided in Article XV below.

12.9 *Verification of Identity.*
Safelora reserves the right to verify User identity before fulfilling rights requests, using reasonable methods such as confirmation of email ownership.

ARTICLE XIII: WITHDRAWAL OF CONSENT

13.1 *Withdrawal Rights.*
Where processing is based on consent (e.g., marketing, non-essential cookies), you may withdraw consent at any time without affecting the lawfulness of prior processing.

13.2 *Mechanisms.*
Withdrawal may be exercised through:
(a) "Unsubscribe" links in marketing emails.
(b) Cookie preference center on the website.
(c) Direct email request to admin@safelora.com.

13.3 *Consequences.*
Withdrawal may prevent us from delivering optional services (e.g., newsletters, analytics-based personalization), but does not affect contractual obligations such as course delivery.

ARTICLE XIV: MARKETING COMMUNICATIONS

14.1 *Email Marketing.*
Safelora sends promotional or informational emails only with prior opt-in consent. Every communication contains an unsubscribe link.

14.2 *Legal Basis.*
Marketing is based on explicit consent (Art. 6(1)(a) GDPR) or, where legally permitted, legitimate interest in contacting existing customers about similar services.

14.3 *Opt-Out.*
Users may opt out at any time without charge. Unsubscribing does not affect the legality of prior communications.

Note: Safelora reserves the right to continue sending non-promotional service notices (e.g., account or transactional messages) regardless of marketing preferences.

ARTICLE XV: AUTOMATED DECISION-MAKING AND PROFILING

15.1 *General Statement.*
Safelora does not generally engage in automated decision-making producing legal effects.

15.2 *Fraud Screening.*
Payment processors may perform automated fraud checks when processing transactions. This may result in temporary holds or refusals. Such measures are necessary to prevent fraud and comply with legal obligations.

15.3 *Transparency.*
Where automated tools are used, Users may request human intervention, express their view, and contest the decision by contacting admin@safelora.com.

ARTICLE XVI: CONTRACTUAL NECESSITY VS. CONSENT

16.1 *Data Required for Contract.*
Certain data (identity, contact, account, payment) must be provided to register, purchase, and access courses. Without such data, Safelora cannot perform its contractual obligations.

16.2 *Data Subject to Consent.*
Other data (marketing preferences, analytics cookies) is optional and processed only with consent. Refusal does not affect contract performance.

Note: Safelora reserves the right to deny access where mandatory data is not provided, clarifying that service cannot be delivered without such processing.

ARTICLE XVII: INTERNATIONAL TRANSFERS

17.1 *Safeguards.*
Where transfers occur outside the EEA, Safelora implements legal safeguards including Standard Contractual Clauses, technical encryption, and limited data disclosure.

17.2 *Key Processors.*
(a) Stripe/PayPal – payment data may transit through US servers.
(b) Email platforms – transactional emails may involve US-based infrastructure.
(c) Cloud providers – hosting may rely on global servers.

17.3 *User Acknowledgment.*
By using our services, you acknowledge such transfers are necessary for global service provision and that appropriate safeguards are in place.

ARTICLE XVIII: COMPLAINTS AND SUPERVISORY AUTHORITY

18.1 *Internal Escalation.*
Users should first direct complaints to admin@safelora.com, where Safelora undertakes to respond within 30 days.

18.2 *Supervisory Authority.*
If unsatisfied, Users may lodge a complaint with the Agencia Española de Protección de Datos (AEPD): Website: www.aepd.es

18.3 *Other EU Supervisory Authorities.*
Users located outside Spain may file with their local supervisory authority under GDPR Art. 77.

ARTICLE XIX: CHANGES TO THIS POLICY

19.1 *Right to Amend.*
Safelora reserves the right to amend this Policy at any time to reflect legal, technical, or business developments.

19.2 *Notification of Changes.*
Significant changes will be communicated through banners on our website and/or email notifications.

19.3 *Consent Renewal.*
Where changes affect consent-based processing (e.g., marketing, cookies), Safelora will request fresh consent before applying the changes.

Note: Continued use of services after notice of change constitutes acceptance of the updated Policy, except where explicit consent is legally required.

ARTICLE XX: GENERAL

20.1 *Survival.*
Sections relating to retention, security, complaints, and rights survive account termination as long as Safelora retains data under Article IX.

20.2 *Contact.*
For privacy questions, rights requests, or complaints, contact:
Safelora
Street 534, Number 20
La Cañada, Paterna, Valencia, Spain
Email: admin@safelora.com

BY USING SAFELORA'S WEBSITE AND SERVICES, YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD THIS PRIVACY POLICY, AND AGREE TO THE COLLECTION, PROCESSING, AND HANDLING OF YOUR PERSONAL DATA IN ACCORDANCE WITH ITS PROVISIONS.