Europa Media LLC
Privacy Policy
Effective: November 11, 2025

Europa Media LLC ("Europa Media," "we," "us," or "our") is committed to respecting your privacy and protecting your personal information. This Privacy Policy provides a detailed explanation of our practices regarding the collection, use, disclosure, and safeguarding of your personal information when you interact with our websites, mobile applications, platforms, services, and networks (collectively referred to as the "Europa Services"). The Europa Services deliver news, media content, and related features, including live and on-demand programs, articles, videos, audio, images, and user-generated contributions, primarily targeted at audiences in the United States and Europe. This Policy is designed to inform you about how we handle your data in a transparent manner, ensuring compliance with applicable laws, including U.S. federal regulations and state-specific privacy statutes, as well as the EU General Data Protection Regulation (GDPR) and the UK GDPR. By accessing or using the Europa Services, you agree to the terms outlined in this Privacy Policy. If you do not agree with these practices, we advise you not to use the Europa Services.

This Policy applies globally, with specific provisions for users in the United States, the European Union (EU), or the United Kingdom (UK). We adhere to data protection principles under GDPR/UK GDPR, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. We process only the minimum data necessary, ensure its accuracy, and conduct regular data protection impact assessments for high-risk processing. As a U.S.-based company hosting the Services in the U.S., we act as the data controller for your personal data. Please direct any inquires about this Privacy Policy or our data collection processes to legal@europa.com.

1. Scope and Application

This Privacy Policy applies to all personal information defined as “any data that identifies, relates to, or could reasonably be linked to you as an individual,” and non-personal information, such as aggregated or anonymized data, that we collect through the Europa Services. Personal information may include identifiers like your name or email address, while non-personal information encompasses broader categories like demographics or usage patterns that do not directly identify you. The Policy covers interactions such as browsing our websites, using our mobile apps, submitting User Content, registering accounts, subscribing to newsletters, or engaging with features like forums and personalized recommendations. It also applies to information collected offline, such as during events or customer support interactions related to the Europa Services. However, this Policy does not extend to information collected by

unaffiliated third-party websites, applications, or services that may be linked from or integrated with the Europa Services; those entities maintain their own privacy policies, and we encourage you to review them carefully. Additionally, if you access the Europa Services through social media or other third-party platforms, the privacy practices of those platforms will govern any data they collect or share with us.

The Europa Services are intended for a general audience and are not targeted at children. We do not knowingly collect personal information from children under 13 years of age without verifiable parental consent, in full compliance with the Children's Online Privacy Protection Act (COPPA). For users between 13 and 17, certain features may require parental consent, as detailed further in Section 9. This Policy applies regardless of whether you are a registered user or a guest, and it describes our practices for both personal and non-personal information, noting that the specifics of what we collect and how we use it may vary based on your interactions with us. Providing personal data is voluntary but may be necessary for certain features (e.g., account creation requires email); refusal may limit access, but we will inform you at collection if it's a statutory or a contractual requirement and the consequences of non-provision.

2. Collection of Information

We collect information from and about you through various methods to provide, maintain, and enhance the Europa Services. This includes data you voluntarily provide, information automatically gathered during your use of the Services, and details obtained from third-party sources. When you register for an account, submit User Content such as comments or forum posts, subscribe to newsletters, participate in surveys, or contact customer support, you may provide us with personal information including your name, email address, username, password, phone number, postal address, date of birth or age (to verify eligibility under our Terms of Service), payment details (such as credit card information processed securely through third-party providers), and any content you upload or share, like text, photos, videos, or audio clips. For instance, if you purchase a subscription or physical goods, we collect billing and shipping information to fulfill your order. If you do not provide required data (e.g., email for registration), you may not access certain features like personalized recommendations or forums.

In addition to direct submissions, we automatically collect data about your interactions with the Europa Services to improve functionality and user experience. This includes technical details such as your IP address, device type and unique identifiers, browser type and version, operating system, geolocation data (which may be coarse, like city-level, or precise with your consent for location-based features), and usage information such as pages visited, time spent on content,

search queries, and interactions with advertisements or videos. We employ cookies, pixels, web beacons, local storage, and similar tracking technologies to facilitate this collection.

We also obtain information from third-party sources to supplement what we collect directly. If you log in or connect via social media services (e.g., Facebook or Google), we may receive shared data such as your profile picture, username, or email address, subject to your permissions on those platforms. Additionally, we may receive data from business partners, such as subscription details from third-party payment services like Apple Pay or PayPal (governed by their privacy policies), or from analytics providers and advertising networks that help us understand user behavior. Publicly available sources or commercially available datasets may also inform our insights, such as demographic information to tailor content. We do not collect sensitive personal information, such as data revealing racial or ethnic origin, political opinions, religious beliefs, health conditions, or genetic data, unless you voluntarily include it in User Content, in which case it is processed only as necessary and with appropriate safeguards. Sources of data include: (i) directly from you (e.g., registration forms); (ii) automatically from your device/browser; (iii) third parties, such as social media platforms (e.g., profile data with your consent), payment providers (e.g., transaction confirmations), analytics partners (e.g., aggregated usage), or publicly available sources (e.g., for verification). Inferred data (e.g., preferences from usage) is derived from collected information but not sensitive categories.

3. Use of Information

The information we collect serves multiple purposes essential to delivering and optimizing the Europa Services. Primarily, we use it to provide the core functionalities you request, such as managing your account, personalizing content recommendations based on your viewing history and preferences, processing subscriptions or purchases, facilitating User Content submissions, and enabling interactive features like comments and forums. For example, your email address and communication preferences allow us to send service-related notifications, such as account updates, security alerts, or responses to your inquiries, ensuring a seamless user experience. We honor opt-outs for commercial emails generally within 10 business days, with no fee. We also rely on this data to improve the Services overall, conducting internal analyses to identify trends, troubleshoot issues, and develop new features, such as using aggregated usage data to refine our content algorithms or enhance mobile app performance.

Furthermore, we utilize your information for marketing and advertising purposes, where permitted, to deliver relevant promotions and targeted advertisements. This may involve analyzing your interests inferred from browsing behavior to show ads that align with your preferences, or sharing anonymized insights with advertisers to measure campaign effectiveness. Tools like Google Analytics help us in this regard, providing aggregated reports on

site traffic and user engagement without identifying individuals. In addition, we process data to ensure the security and integrity of the Europa Services, detecting and preventing fraud, unauthorized access, or violations of our Terms of Service, such as through IP address monitoring or automated fraud detection systems. Finally, we may use information to comply with legal obligations, including responding to government requests, maintaining records for tax or audit purposes, or enforcing our rights in legal disputes. All uses are conducted in a manner that respects your privacy and aligns with applicable laws, and we do not engage in automated decision-making that produces legal or similarly significant effects on you.

Your personal data is processed for specific, legitimate purposes aligned with providing high-quality Europa Services. We use it to fulfill contractual obligations, such as managing accounts, processing payments, delivering personalized content, and facilitating User Content features. For communications, like service updates or newsletters, we rely on consent where required. Analytics and improvements involve aggregating data to identify trends and enhance functionality, based on our legitimate interests. Targeted advertising uses consent for cookies and legitimate interests for broader personalization, always balancing against your rights via legitimate interest assessments. Security and fraud prevention are grounded in legitimate interests, while legal compliance meets obligations under law.

Below is our Legal Bases Chart under GDPR/UK GDPR (Art. 6):

- Provide Services (e.g., account management, content delivery): Contract necessity (Art. 6(1)(b)).
- Communications (e.g., marketing emails): Consent (Art. 6(1)(a)).
- Analytics/Improvement: Legitimate interests (Art. 6(1)(f)); service optimization, user experience enhancement; interests not overridden by your rights (e.g., via opt-out).
- Advertising: Consent (Art. 6(1)(a)) for tracking technologies; legitimate interests (Art. 6(1)(f)) for non-tracking personalization.
- Security/Fraud: Legitimate interests (Art. 6(1)(f)); protecting systems and users.
- Legal Compliance: Legal obligation (Art. 6(1)(c)). For any special category data (rarely processed), explicit consent (Art. 9(2)(a)) applies. We ensure processing is proportionate, with data minimization (collecting only what's needed) and accuracy (e.g., allowing updates via account settings).

4. Disclosure of Information

We may disclose your information to trusted third parties under specific circumstances to support the operation of the Europa Services and fulfill our business objectives. Service providers, such as cloud hosting companies, analytics firms, payment processors, and email

delivery services, receive limited access to your data solely to perform tasks on our behalf, such as processing transactions or analyzing usage patterns. These providers are contractually obligated to protect your information and use it only for the specified purposes. We may also share data with our affiliates or business partners for joint initiatives, like co-branded promotions or content collaborations, ensuring they adhere to similar privacy standards.

In the context of advertising, we disclose certain information, such as device identifiers or browsing history, to advertisers, ad networks, and technology companies to enable targeted advertising across devices and platforms. This sharing may qualify as a "sale" or "sharing" of personal information under certain state privacy laws, as detailed in Section 8, and you have the right to opt out. Additionally, we may transfer information in connection with corporate events, such as a merger, acquisition, or sale of assets, where the receiving entity agrees to maintain comparable privacy protections. Disclosures may also occur to comply with legal requirements, such as responding to subpoenas, court orders, or law enforcement requests, or to protect our rights, users, or the public from harm, including preventing illegal activities like fraud or copyright infringement. We do not sell or share personal information of known minors under 16 years of age, and all disclosures are limited to what is necessary and lawful.

We disclose personal data only when necessary and with appropriate safeguards, such as data processing agreements under GDPR Article 28. Categories of recipients include: (i) service providers like hosting firms, analytics tools , payment gateways, and email services, who access limited data to support operations and are bound by strict confidentiality and purpose limitations; (ii) affiliates within our group for internal administrative purposes; (iii) advertising networks or partners; (iv) professional advisors for legal/financial compliance; (v) successors in business transfers, with continued protections. We do not sell data and minimize sharing, ensuring recipients comply with GDPR/UK GDPR. No disclosures to non-adequate countries without safeguards (see Section 5).

5. International Transfers

As a U.S.-based entity, we transfer data to the U.S., which lacks an adequacy decision under GDPR/UK GDPR. All transfers are protected by appropriate safeguards to ensure an equivalent level of protection, including EU Standard Contractual Clauses (SCCs) under Commission Decision 2021/914 or the UK International Data Transfer Addendum/Addendum to SCCs. We may also rely on binding corporate rules if applicable or derogations. Supplementary measures, such as encryption and access restrictions, are implemented based on transfer impact assessments. Contact us for copies of safeguards, transfer details, or assessments.

6. Retention

We retain your personal information only for as long as necessary to fulfill the purposes for which it was collected, including providing the Europa Services, complying with legal obligations, resolving disputes, and enforcing our agreements. Usage logs and analytics data are typically retained for up to 12 months to support security and performance monitoring. Once retention periods expire, we securely delete or anonymize the data, ensuring it can no longer be associated with you. If you request deletion of your information, we will honor it subject to any legal retention mandates, and we periodically review our data holdings to minimize storage. Personal data is retained only as long as necessary for the specified purposes, with periodic reviews to delete unnecessary information in line with storage limitation principles.

7. Security

Protecting your personal information is a top priority for us, and we implement a range of reasonable administrative, technical, and physical safeguards to prevent unauthorized access, use, disclosure, alteration, or destruction. For instance, we use encryption for data in transit, access controls to limit employee access to necessary information, and regular security audits to identify vulnerabilities. Payment information is handled securely through PCI DSS-compliant third-party processors and is not stored on our servers. While we strive to maintain robust security measures, no system can guarantee absolute protection against all threats, such as cyberattacks or breaches. In the event of a security incident, we will notify affected individuals and authorities as required by law, and we encourage you to protect your account by using strong, unique passwords and enabling two-factor authentication where available.

We maintain appropriate technical and organizational measures to secure personal data against risks like breaches or unauthorized access, in compliance with GDPR Article 32, including pseudonymization and encryption, access controls (role-based, least privilege), regular vulnerability scans and penetration testing, employee training on data protection, and incident response plans. Measures are proportionate to risks, considering data sensitivity and processing nature. In case of breaches, we notify supervisory authorities and affected individuals without undue delay if high risk, providing details and mitigation advice. We conduct data protection impact assessments for high-risk processing activities, such as large-scale User Content analysis or new technologies, per Article 35, to identify and mitigate risks.

8. Your Choices and Rights

You have several options to control how we collect, use, and share your information, empowering you to manage your privacy preferences effectively. For marketing

communications, such as newsletters or promotional emails, you can opt out at any time by clicking the "unsubscribe" link in the email footer, updating your preferences in your account settings, or contacting us directly. Note that you cannot opt out of essential service-related communications, like account security alerts or transaction confirmations. Regarding cookies and tracking technologies, you can manage your preferences through our Cookie Notice, which provides details on essential versus optional cookies, or by adjusting your browser settings to block or alert you about cookies, though this may limit access to certain features. We also respect global privacy control signals (GPC) for opting out of targeted advertising where applicable.

Additionally, if you have provided geolocation data, you can revoke consent via your device settings. For "Do Not Track" (DNT) browser signals, we currently do not alter our practices in response to them, as there is no uniform standard for interpretation; instead, use the opt-out mechanisms described in Section 8 for targeted ads. If you wish to access, correct, or delete your information, or exercise other rights, please follow the processes outlined below for state-specific requests or contact us generally. We aim to respond promptly to your choices, and exercising these options will not result in discrimination, such as denial of services or higher prices.

For U.S. Users (State-Specific Rights):

Residents of states with comprehensive privacy laws, including California (CCPA/CPRA), Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA), Utah (UCPA), Texas (TDPSA), Oregon (OCPA), Montana (MCDPA), Delaware (DPDPA), Iowa (ICDPA), Tennessee (TIPRA), Minnesota (MCDPA), Maryland (MDPA), and others effective as of November 2025, have enhanced rights regarding their personal information. These laws provide similar protections, such as the right to know what data we collect, to opt out of sales or sharing, and to request deletion, with some variations in scope and applicability. Below, we provide the required disclosures and explain how to exercise these rights.

In the past 12 months, we have collected the following categories of personal information: (1) Identifiers (e.g., name, email, IP address, device IDs); (2) Personal records (e.g., phone number, address, payment info); (3) Protected classifications (e.g., age, if provided); (4) Commercial information (e.g., purchase history); (5) Geolocation data (coarse or precise); (6) Internet activity (e.g., browsing history, interactions); (7) Audio/visual data (e.g., User Content uploads); (8) Inferences (e.g., content preferences). Sources include you directly, automatic collection, and third parties like social media or partners. We use this for purposes like service provision, personalization, analytics, advertising, security, and legal compliance, as detailed in Section 3.

We do not use sensitive personal information for inferences without consent; you may limit its use by emailing legal@europa.com.

We disclose these categories to service providers, affiliates, ad partners (for targeted ads, which may be a "sale" or "sharing"), and in business transfers. We do not "sell" data for monetary value but may "share" identifiers, internet activity, and inferences with ad networks for cross-context behavioral advertising. To opt out of sales/sharing or targeted advertising, use our "Do Not Sell/Share My Personal Information" link in the site footer, enable GPC signals, or email legal@europa.com. We process opt-outs promptly and apply them globally where possible.

We do not offer financial incentives tied to the collection, sale, or sharing of personal information, such as discounts for allowing data use. If we introduce such programs in the future, we will provide details here, including the program's value and your right to opt out. For California residents under "Shine the Light" law (Cal. Civ. Code § 1798.83), we do not share personal information with third parties for their direct marketing purposes beyond targeted advertising (which is covered by opt-outs above). If you are a California resident and wish to request a list of third parties (if any) to whom we disclosed personal information for direct marketing in the prior year, email legal@europa.com once per year free of charge.

Your rights include:

(1) Know/Access: Confirm if we process your data and receive details/categories (twice per year free);

(2) Delete: Request deletion, subject to exceptions (e.g., legal retention);

(3) Correct: Rectify inaccuracies;

(4) Opt-Out: Of sales/sharing/targeted ads;

(5) Limit Sensitive Data: We do not process sensitive data for inferred characteristics without consent;

(6) Non-Discrimination: No penalties for exercising rights;

(7) Portability: Receive data in a portable format;

(8) Appeal: Submit requests by emailing legal@europamedia.com and appeal using the same email. We verify identity (e.g., via email confirmation or account login) and respond within 90 days. Authorized agents may submit with proof of authorization. For 2024 metrics (CCPA-required): We received 0 access requests (fulfilled 0), 0 deletion requests (fulfilled 0), 0

correction requests (fulfilled 0), and 0 opt-out requests (fulfilled 0), as we are a new service with limited data processing. Contact us for current figures. We do not engage in profiling with legal effects.

- Know/Access: Confirm if we process your data and receive details/categories (twice per year free).
- Delete: Request deletion, subject to exceptions (e.g., legal retention).
- Correct: Rectify inaccuracies.
- Opt-Out: Of sales/sharing/targeted ads.
- Limit Sensitive Data: We do not process sensitive data for inferred characteristics without consent.
- Non-Discrimination: No penalties for exercising rights.
- Portability: Receive data in a portable format.
- Appeal: Submit requests by emailing legal@europamedia.com and appeal using the same email. We verify identity (e.g., via email confirmation or account login) and respond within 90 days. Authorized agents may submit with proof of authorization. For 2024 metrics (CCPA-required): We received 0 access requests (fulfilled 0), 0 deletion requests (fulfilled 0), 0 correction requests (fulfilled 0), and 0 opt-out requests (fulfilled 0), as we are a new service with limited data processing. Contact us for current figures. We do not engage in profiling with legal effects.

For EU/UK Users:

Under GDPR/UK GDPR, you have absolute rights, exercisable free of charge (unless manifestly unfounded/excessive, where a reasonable fee may apply or request refused):

- Access (Art. 15): Obtain confirmation of processing, copy of data, and details (e.g., purposes, recipients).
- Rectification (Art. 16): Correct inaccuracies or complete incomplete data.
- Erasure ("right to be forgotten," Art. 17): Delete data if no longer necessary, consent withdrawn, or unlawful processing (subject to exceptions like legal obligations).
- Restriction (Art. 18): Suspend processing during verification or if you object.
- Portability (Art. 20): Receive data in structured, machine-readable format or transfer to another controller (for automated, consent/contract-based processing).
- Objection (Art. 21): To processing based on legitimate interests/public interest (including profiling), with compelling grounds; always to direct marketing.
- Withdraw Consent (Art. 7): Anytime, without affecting prior lawfulness; easy as giving consent (e.g., via account settings).

- Not be subject to automated decisions with legal/similar effects (Art. 22): We do not engage in such (see Section 10). You also have rights to compensation for material/non-material damages from unlawful processing (Art. 82) and to judicial remedies (Art. 79), including representation by non-profits (Art. 80).

You may exercise these rights by emailing legal@europa.com.

9. Children's Privacy

The Europa Services are designed for adults and are not intended for children under 13 years of age. In compliance with COPPA, we do not knowingly collect personal information from children under 13 without verifiable parental consent, such as through credit card verification, signed consent forms, or other methods approved by the FTC. If we become aware of such collection, we will delete the information promptly. For users under 18 (or the age of majority), features like account creation or User Content submission require parental consent and supervision, as outlined in our Terms of Service (Section 4). We do not condition a child's participation on providing more personal information than is reasonably necessary. Parents can review, delete, or refuse further collection of their child's data by contacting us. We may implement age-gating mechanisms, like self-declaration, to enforce these restrictions.

The Europa Services require users to be at least 18 or the age of majority, with minors under 16 needing verifiable parental consent for data processing. We use methods like email confirmation or third-party verification to obtain consent, explaining processing to parents. Parents/guardians can manage, review, delete, or withdraw consent by contacting us, assuming responsibility for the minor's use. No targeted ads or profiling for children; if aware of unauthorized collection, we delete promptly. For lower national ages, we apply the stricter threshold.

10. Automated Decision-Making

We do not engage in automated decision-making, including profiling as defined in Article 4(4), that produces legal effects or similarly significantly affects you. Any automated processes are not solely automated and include human oversight; you can object or request review. If we introduce such processing in the future, we will update this Policy, conduct a DPIA if high-risk, and seek explicit consent or provide safeguards like human intervention.

11. Changes to This Policy

We may periodically update this Privacy Policy to reflect changes in our practices, legal requirements, or the Europa Services. The "Last Updated" date at the top indicates the most recent revision. For material changes that affect your rights, we will provide notice via email (if we have your address) or a prominent alert on the Services at least 30 days in advance, allowing you to review and, if desired, discontinue use. Continued use after changes constitutes acceptance. We recommend checking this Policy regularly for updates.

12. Contact Us

If you have questions about this Privacy Policy or our practices, please contact us by email at legal@europa.com, or mail at Europa Media LLC, 30 N Gould St Ste R, Sheridan, WY 82801.