Reliz - Brand Safety & Advertising Content Guidelines

Effective date: 01.05.2026

Company: Reliz Ltd (Malta, C 96147)

Contact: info@reliz.com

Introductory statement

These Brand Safety & Advertising Content Guidelines describe Reliz's advertising standards and enforcement posture for advertisements, creatives, landing pages, and related advertising materials delivered through or in connection with Reliz Exchange and related services.

These guidelines are intended to support publisher controls, platform integrity, user trust, and risk management. They are a public-facing summary only and do not create any obligation for Reliz to pre-screen, approve, detect, restrict, or block every advertisement, advertiser, campaign, domain, or targeting practice before delivery.

Reliz may review, restrict, reject, suspend, disable, remove, or request the blocking of advertising activity at its discretion, including where Reliz determines or suspects that such activity presents legal, regulatory, contractual, technical, security, fraud, privacy, reputational, or publisher-suitability risk.

1. Scope and purpose

These guidelines apply to advertisements, creatives, landing pages, post-click experiences, advertiser content, and related delivery or targeting practices made available through Reliz's advertising supply.

Reliz maintains these guidelines in order to support publisher brand safety and suitability requirements; reduce exposure to unlawful, harmful, deceptive, insecure, or inappropriate advertising activity; preserve platform integrity and user trust; and enable operational controls over advertising demand and delivery.

These guidelines describe categories and practices that Reliz may restrict or prohibit. They are not exhaustive and do not limit Reliz's right to take action with respect to any advertising activity that Reliz considers unsuitable, non-compliant, high-risk, or inconsistent with Reliz's commercial, legal, operational, technical, or publisher requirements.

2. Partner responsibility and legal roles

Each DSP, buyer, advertiser, agency, demand partner, and other partner providing or enabling advertising demand through Reliz remains responsible for ensuring that its advertisements, creatives, landing pages, disclosures, claims, targeting parameters, consent mechanisms, and related practices comply with applicable law, applicable self-regulatory standards, applicable platform or publisher requirements, the relevant agreement with Reliz, and any applicable technical or integration requirements.

Reliz may rely on partner representations, warranties, classifications, technical signals, and documentary materials, and Reliz shall have no obligation to independently verify the legality, accuracy, substantiation, or suitability of any advertisement or associated practice.

Nothing in these guidelines limits any separate obligations that Reliz may have under applicable law for processing activities for which it acts as controller, joint controller, or processor, as the case may be.

3. Prohibited content and practices

The following categories are prohibited and must not be submitted, delivered, promoted, linked, or otherwise made available through Reliz.

3.1 Always prohibited. Advertisements or advertising materials that contain, promote, facilitate, or are reasonably associated with: hate speech, discriminatory content, harassment, or content promoting violence against individuals or groups; violent extremist, terrorist, or criminal organization propaganda, glorification, or recruitment; pornography, explicit sexual content, or adult sexual services; graphic violence, gore, or shocking imagery; weapons, ammunition, explosives, or instructions for their unlawful use; illegal drugs, controlled substances, or related paraphernalia; malware, spyware, adware, malicious code, hacking tools, phishing tools, unauthorized access tools, or other harmful software or code; fraud, impersonation, scams, counterfeit goods, forged documents, or deceptive commercial practices; copyright infringement, piracy, or other intellectual property infringement; deceptive system alerts, fake functionality, forced redirects, misleading downloads, or other manipulative post-click or device-level behavior; or unlawful products, unlawful services, or unlawful conduct in any relevant jurisdiction.

3.2 Political and public affairs restrictions. Unless expressly agreed by Reliz in writing in advance, advertisements or advertising materials relating to political advertising, election-related communications, referendum campaigns, lobbying or legislative influence campaigns, issue advocacy intended to influence public policy or public opinion on matters of political or social controversy, or political fundraising are prohibited.

3.3 Restricted categories. The following categories may be restricted, conditionally permitted, or prohibited by Reliz in its discretion, including by territory, publisher, format, inventory type, age-gating considerations, or partner status: gambling, betting, lotteries, fantasy gaming, or similar services; alcohol; financial services, credit, lending, insurance, investments, securities, foreign exchange, or similar products; cryptoassets, digital tokens, wallets, exchanges, staking, or similar services; health, wellness, medical, pharmaceutical, or treatment-related products or claims; age-restricted products or services; and any category subject to heightened legal, regulatory, or publisher sensitivity. Reliz may require prior written approval, additional documentation, certifications, disclosures, targeting restrictions, or other conditions before permitting any restricted category.

The examples above are illustrative and non-exhaustive. Reliz may classify or restrict content based on substance, presentation, landing page behavior, targeting method, or reasonably associated risk, whether or not expressly listed above.

4. Technical, creative, and landing page standards

All advertisements, creatives, tags, scripts, landing pages, and post-click experiences must function in a safe and technically compliant manner; be free from malicious or harmful code; not damage, interfere with, exploit, or gain unauthorized access to devices, networks, systems, software, accounts, data, or personal information; accurately represent the advertiser, offer, and destination; not contain false, misleading, deceptive, or unsubstantiated claims; not use dark patterns, coercive design, hidden charges, fake urgency, or deceptive calls to action; not trigger unauthorized downloads, browser behavior, auto-redirects, or disguised UI elements; and be consistent with the creative's message and not materially mislead users as to the nature of the advertised product or service.

Reliz may reject or suspend any creative or destination that, in Reliz's judgment, creates technical, user-safety, fraud, privacy, or reputational risk, whether or not the issue is expressly listed in these guidelines.

5. Targeting, privacy, advertising transparency, and minors

Partners remain responsible for ensuring that their advertising, measurement, targeting, profiling, data use, consent flows, and related adtech practices comply with applicable privacy, consumer protection, children's protection, and advertising laws.

Where the use of cookies, mobile identifiers, pixels, SDK signals, or similar technologies for targeting, measurement, personalization, or attribution requires consent under applicable law, partners must ensure that such consent is validly obtained, specific, informed, freely given, unambiguous, and capable of being evidenced on request. Pre-ticked, bundled, coerced, or otherwise invalid consent mechanisms are not permitted.

Advertisements and associated practices must not rely on unlawful profiling or unlawful tracking; use sensitive personal data for advertising where prohibited by applicable law; target minors where prohibited by applicable law; promote or deliver age-inappropriate advertising in a manner inconsistent with applicable law, publisher requirements, or reasonable child-safety expectations; or omit legally required disclosures or transparency information.

Where applicable law or platform functionality requires advertising transparency, partners must provide accurate advertiser identity, payer identity where required, required disclosures, and sufficient metadata to support labelling of advertisements and explanation of why an advertisement is shown.

Partners must apply data minimisation and storage limitation principles to advertising-related processing and must not aggregate, retain, or reuse personal data for targeting or profiling beyond what is objectively necessary and lawful for the relevant purpose.

Reliz may restrict, suspend, or refuse advertising activity that presents heightened privacy, child-safety, data protection, platform integrity, or publisher-suitability risk.

6. Industry standards and technical compatibility

Where relevant and technically supported in the applicable integration, Reliz may use, require, or support compatibility with commonly adopted industry specifications, taxonomies, creative-approval tools, or transparency mechanisms, including OpenRTB 2.6 or 2.6.x updates, IAB Tech Lab Content Taxonomy 3.1, IAB Tech Lab Ad Product Taxonomy 2.0, ads.txt/app-ads.txt, sellers.json, the OpenRTB SupplyChain object, and the Ad Management API.

Any reference to industry specifications is descriptive only and does not constitute a representation by Reliz that any specific standard, object, taxonomy, field, identifier, or transparency mechanism is universally available, implemented in full, or supported across all traffic, publishers, formats, devices, or partner integrations.

Partners are responsible for ensuring that any technical metadata, classifications, identifiers, declarations, and consent or transparency signals provided by them are accurate, complete, lawful, and suitable for the relevant integration.

7. Blocking, suppression, information requests, and suspension

To support publisher controls, platform integrity, and risk management, Reliz may require partners, where technically supported in the applicable integration, to enable or implement blocking, suppression, exclusion, or suspension at one or more of the following levels: advertiser, brand, creative, landing page or destination domain, app bundle, site, inventory source, campaign, seat, deal, demand source, or any other identifier, object, or signal reasonably requested by Reliz.

Reliz may require documentary evidence, technical metadata, advertiser identification information, domain or app ownership information, licenses, approvals, substantiation of claims, and evidence of legally required consent or disclosure mechanisms, and may suspend delivery pending receipt and review of such information.

Reliz may take immediate temporary or permanent action, with or without prior notice, where Reliz reasonably determines or suspects that advertising activity presents legal, regulatory, contractual, security, fraud, privacy, reputational, technical, or publisher-suitability risk.

Partners shall maintain an operational contact for brand safety, abuse, blocking, and escalation matters and shall cooperate promptly with reasonable requests from Reliz.

8. Review, enforcement, and reconsideration

Reliz may, but is not obligated to, review advertisements, creatives, landing pages, demand sources, and related practices for compliance with these guidelines, the relevant agreement, technical requirements, or publisher requirements.

Reliz may, at any time and in its discretion, reject or refuse onboarding of advertising demand; reject, disable, suspend, or remove creatives or campaigns; require changes or additional information; request blocking or suppression measures; limit delivery by publisher, geography, format, or inventory type; or terminate or restrict access as provided in the relevant agreement.

Reliz will generally review reports and internal escalations in accordance with its internal risk procedures and may, where practicable, notify the relevant partner of enforcement action. Reliz shall have no obligation to provide advance notice, detailed reasoning, a formal appeal process, or continued delivery during any review.

Reliz may, in its discretion, consider good-faith requests for reconsideration supported by sufficient information. Submission of such a request does not require Reliz to reverse, delay, or suspend any enforcement action.

9. Relationship to agreements

These guidelines are a public-facing summary of Reliz's advertising standards and enforcement posture. They do not create third-party rights and do not amend any signed agreement unless that agreement expressly provides otherwise.

In the event of any inconsistency between these guidelines and a signed agreement, order form, data protection addendum, integration documentation, or other contractual document, the signed and applicable contractual documents shall prevail.

10. Updates

Reliz may update, revise, expand, or replace these guidelines from time to time.

Any such update applies prospectively to this public guidance only, unless a signed agreement expressly states that these guidelines, as amended from time to time, are incorporated by reference.

11. Reporting concerns

Reports of suspected violations, unsafe advertising activity, or requests for blocking or suppression updates may be submitted to: info@reliz.com

Suggested subject line: Brand Safety - [partner name]

Reliz will review reports in accordance with its internal risk procedures, may request additional information, and may take action in its discretion. Reliz is not required to disclose the outcome of any review except where required by applicable law or an applicable signed agreement.