Mar 4, 2026

Publisher Onboarding Privacy Compliance Notice

Digital advertising and monetization rely on a complex ecosystem of technologies, vendors, and data flows. Many of these technologies can involve the collection or use of information about the individuals who use your services or consume your media. As a result, publishers are often subject to privacy, data protection, and consumer protection laws, as well as industry standards and self-regulatory frameworks.

This Onboarding Privacy & Data Compliance Notice ("Notice") is incorporated into and forms part of the Agreement between Marathon Ventures, LLC ("Marathon") and you ("Publisher"). It establishes certain privacy and data compliance obligations applicable to Publisher in connection with the monetization of its inventory through Marathon.

This Notice does not constitute legal advice. Publisher remains solely responsible for determining how applicable laws apply to its business and for consulting its own legal counsel as needed. However, Publisher's obligations under this Notice are contractual obligations under the Agreement.

Publisher acknowledges that Marathon's ability to provide monetization services depends on Publisher's compliance with this Notice. Failure to comply with the requirements of this Notice may constitute a material breach of the Agreement.

How Privacy and Digital Advertising Regulation Typically Applies to Publishers

Publishers are generally viewed to have direct relationships with users because they control the digital properties where advertising technologies operate, decide which vendors and technologies are implemented, and control design, content context, and user interactions.

As a result, Publisher must:

- Be transparent with users about advertising and data practices.
- Control where and how tracking technologies are deployed.
- Prevent inappropriate or unexpected data collection.
- Respect user choices and rights.

Publisher Responsibilities and Practices

1. Transparency, Disclosures, and User Choice

Most privacy and consumer protection laws are built around transparency and user control. Users are expected to understand how their data is used and have meaningful choices where required.

Publisher shall:

- Maintain clear, accurate, and up-to-date privacy policies describing data sharing practices.
- Disclose the use of cookies, pixels, SDKs, and similar technologies used to track users.
- Disclose sharing of information with advertising partners, intermediaries, and service providers, including Marathon and downstream vendors, where required by law.
- Honor user choices as required by law.
- Ensure disclosures and choices are presented in a clear, accessible manner, without unnecessary or extra steps required for users to make choices.

2. Consent and Preference Management

Publisher acknowledges that managing user consent and preferences is fundamental to lawful advertising operations.

Publisher shall:

- Implement and maintain a consent and/or opt-out mechanism as required by applicable law, including where applicable a "Do Not Sell or Share Personal Information" mechanism that responds to opt-out preference signals such as Global Privacy Control.
- Where appropriate based on jurisdiction and risk profile, implement a consent management platform (CMP) suitable for its properties.
- Maintain an inventory of all pixels, tags, scripts, and SDKs deployed across its properties.
- Ensure that technology configurations accurately reflect real-world data flows and user choice (e.g., where a user opts out or does not consent, cookies or pixels do not collect or transmit personal information in violation of law).

3. Limitations on Data Collection, Use, and Sharing

Understanding and controlling data flows reduces compliance risk and helps avoid unintended collection or sharing of personal information that can lead to litigation or enforcement. Publisher is expected to minimize the amount and variety of data it collects and limit the purposes for which it uses that data.

Publisher shall:

- Avoid transmitting personal data to MV unless expressly agreed in writing and legally permitted.
- Ensure that any data shared with advertising technology partners is limited to what is necessary for the intended advertising or measurement purpose.

4. User Rights and Requests

Many privacy and data protection laws grant users enforceable rights, including to access, delete, correct their personal information, or opt out of the sale or share of their personal information, which generally applies to disclosures for targeted advertising purposes. Requests can be made manually via email, phone, or privacy form, or through automated means, such as opt-out preference signals like Global Privacy Control. As users' primary point of contact, responsibility for responding to these rights requests falls on Publisher.

Publisher is responsible for:

- Receiving and responding to user privacy rights requests in accordance with applicable law.
- Ensuring opt-out or consent signals are communicated to relevant vendors, including Marathon where applicable.
- Documenting request handling processes.

5. Prohibited and Sensitive Data

Certain categories of data carry heightened legal risk, and the use of advertising technologies in sensitive contexts can attract unwanted scrutiny.

Publisher shall not:

- Send or enable the collection, use, or sharing of sensitive categories of data through advertising technologies, including data relating to:
    - Children, minors, or teens under 18 years old.
    - Health conditions, treatments, diagnoses, or providers.
    - Financial information.
    - Precise geolocation.
    - Sexual preferences or orientation.
- Deploy advertising or tracking technologies in ways that could allow sensitive information to be inferred or derived from page content or user behavior.

6. Sensitive Pages and Authenticated Environments

Publisher shall limit or disable advertising and tracking technologies by default in the following contexts:

- Pages referencing medical conditions, treatments, diagnoses, or providers.
- Authenticated or logged-in environments (e.g., user dashboards, portals, account areas) where user activity may be more readily associated with an identifiable individual.
- Pages that allow users to submit information (e.g., contact forms, registration forms, feedback forms).
- Other contexts where the subject matter, user interaction, or design of the page creates heightened privacy expectations or increased regulatory risk.

Publisher shall implement technical controls (e.g., tag management rules, page-level restrictions, or conditional loading) to prevent advertising and tracking technologies from running in these contexts by default.

7. Geographic and Jurisdictional Controls

Privacy obligations can vary significantly by region, and enforcement trends continue to evolve, which can affect whether and how advertising technologies may be deployed. For example, certain programmatic advertising or measurement tools may be used in some U.S. states subject to opt-out mechanisms, while those same tools may require affirmative consent or limited configurations in other regions.

Publisher shall:

- Implement jurisdictionally appropriate consent or opt-out mechanisms.
- Restrict or disable certain advertising or tracking technologies in higher-risk jurisdictions.
- Monitor regulatory developments that may affect monetization strategies.

8. Control Over Technology Deployment

Publisher is best positioned to understand its properties, content, and audiences, and thus is expected to control what runs on its sites or apps.

Publisher retains and accepts responsibility for:

- Deciding whether, where, and how advertising, tracking, or measurement technologies are deployed.
- Reviewing and approving all tags, pixels, scripts, SDKs, and similar technologies before implementation.
- Ensuring that deployments align with disclosed practices and user choices.

MV does not independently determine placement decisions on Publisher properties.

9. Vendor Due Diligence and Oversight

Publisher is responsible for:

- Conducting appropriate due diligence on SSPs, ad exchanges, platforms, and other technology partners.
- Reviewing vendor privacy practices, security measures, and contractual terms.
- Understanding role allocation (e.g., controller, processor, service provider).

Use of third-party vendors does not relieve Publisher of its compliance obligations.

10. Industry Frameworks and Standards

Digital advertising has several industry frameworks that can help standardize compliance and reduce operational challenges, including those offered by the Interactive Advertising Bureau, Network Advertising Initiative, Better Business Bureau, and Digital Advertising Alliance, among others. These frameworks are designed to provide shared technical, contractual, and signaling standards that allow privacy requirements (e.g., user opt-out or consent choices) to be communicated more consistently across the advertising supply chain, reducing fragmentation, misinterpretation, and implementation burden for publishers.

Publisher may consider:

- Participating in self-regulatory programs such as the IAB Multi-State Privacy Agreement (MSPA).
- Implementing available technical standards, including the IAB's Global Privacy Platform (GPP).
- Monitoring updates to industry guidance and specifications, and assessing which are achieving widespread adoption.

Participation in industry frameworks does not replace Publisher's independent legal compliance obligations.

11. Proactive and Continuous Monitoring

Noncompliant data collection and sharing practices frequently result not from intentional misconduct, but instead from legacy tags, unused or forgotten integrations, configuration drift over time, or the rapid deployment of new technologies without sufficient review.

Publisher shall:

- Conduct appropriate privacy and legal reviews before launching new campaigns and integrations.

- Periodically audit live implementations for consistency with disclosures and user choices.
- Remove unnecessary or duplicative tracking technologies.

12. Documentation and Governance

Privacy compliance is often evaluated based on what steps a business has taken and why, so written policies and recordkeeping are key practices for demonstrating good-faith compliance and accountability to regulators, consumers, and business partners.

Publisher shall:

- Maintain internal privacy and data governance documentation.
- Keep records of vendor reviews, consent configurations, and audits.
- Ensure relevant staff receive appropriate training, and document those training efforts.