Read First: Privacy Policy Requirements

02/01/2026 1:41 pm EST

1. Introduction& Disclaimer

Overview

Transparency is the foundation of the ID5 ID. To ensure the ID5 ID Service operates securely and in compliance with global data protection standards, ID5 requires all partners and their downstream parties (collectively, "**Partners**") maintain privacy notices that accurately describe the scope and technical reality of the data flows.

Contractual Status

The standards below constitute mandatory requirements for all Partners utilizing the ID5 ID Service. Depending on the specific agreement you executed with ID5, these standards constitute:

- "ID5 ID Requirements" as defined in your ID5 ID Agreement;
- "ID5 ID Site Offering Requirements," "ID5 IdentityCloud Requirements," or similar (for Partners on the legacy ID5 ID Site Agreement, MSA, or other agreement with ID5); OR
- Any similar term associated with your use of the service in which signals are sent to ID5, for ID5 to return an encrypted ID5 ID in real time (the "**ID5 ID Service**").

(collectively, the "**ID5 ID Requirements**" and the "**Agreement**" as applicable).

Per your Agreement, Partners must comply with the ID5 ID Requirements to activate and maintain the ID5 ID Service. Failure to implement these disclosures constitutes a material breach of your Agreement with ID5, puts both the Partner and ID5 at risk, and may trigger your indemnification obligations to ID5 for any resulting claims or regulatory fines.

> ⚠ IMPORTANT OPERATIONAL DISCLAIMER
>
> ID5 Technology Ltd. provides this document to define the operational and technical parameters for utilizing the ID5 ID Service. This content specifies what must be disclosed to users to ensure the data signals sent to ID5 are valid.
>
> *This document **DOES NOT CONSTITUTE LEGAL ADVICE**. Privacy laws (including the CCPA, CIPA, VPPA, and GDPR) are complex and fact-specific. You are solely responsible for consulting your own legal counsel to ensure your privacy policy, user notices, and consent mechanisms comply with all applicable laws and accurately reflect your specific data practices.*

2. US Publisher Requirements

Applicability: Partners with traffic originating from the United States.

To mitigate risks associated with evolving US privacy litigation - including claims regarding real-time data processing ("Wiretapping"/"Trap and Trace", e.g., CIPA) and video privacy (i.e., VPPA) - and to comply with state privacy laws (CCPA/CPRA and other state laws), Partners must include the following substantive elements in their Privacy Policy:

A. "Sale" and "Sharing" Classification

- **Requirement**: Explicitly state that the transmission of personal data (e.g., IP, Hashed Email, MAIDs) to ID5 constitutes a "Sale" (transfer for value) and/or "Sharing" (transfer for cross-context behavioral advertising) under applicable US State Laws for ID5 to process the data as a "Third Party" or "Business".
    - **Note**: Do NOT classify ID5 as a Processor or Service Provider. As described in your Agreement, ID5 retains the right to use the data for its own purposes (including Graph Building), which creates a "Third Party" or "Business" relationship under California law.
- **Signal Flow:** Ensure ID5 is included in the signal flow of the Partner's "Do Not Sell/Share My Personal Information" mechanism (e.g., GPP string, GPC Signal) so that ID5 is able to ascertain when a particular user has opted-out and automatically suppress processing for opted-out users.

B. Disclosure of "Real-Time" Interception

To ensure transparency regarding automated technologies, you must explicitly state that third-party vendors operate on the digital property concurrently with the user's visit.

- **Requirement:** Disclose that third-party vendors (specifically ID5) are authorized to access the user's device, intercept, and collect signals derived from pseudonymous device info "in real-time" and "during the user's interaction" with the page.
- **Drafting Example:** *We utilize third-party tracking technologies [link to ID5] that operate concurrently with your visit to intercept, monitor, and record your interactions with our page, including the collection of device identifiers and IP addresses, for the purposes of identity resolution and security.*

C. Strict Purpose Bifurcation (Identity vs. Security)

The Partner's privacy policy must legally distinguish between data collected for identity/advertising and data collected for security. This distinction is a condition of ID5 accepting the data.

- **Identity & Advertising:** Disclose that IP Addresses, Hashed Emails, and User Agent strings are shared with ID5 for "Identity Resolution," which enables "Profiling", "Automated Decisioning" "Cross-Device Graphing," and "Targeted Advertising" (or "Cross-Context Behavioral Advertising").
- **Security & Error Detection:** Disclose that Page URLs (Uniform Resource Locators) and Timestamps are collected by ID5 specifically for "Security," "Fraud Prevention," and "Error Detection" purposes. Do **not** list ID5's collection of Page URLs under "Advertising" or "Profiling" purposes. This distinction is critical for compliance with video privacy and pen register statutes.
- **Restriction on Video URLs:** You must NOT transmit full URLs to ID5 if those URLs contain video titles or content descriptions (e.g., site.com/video/how-to-treat-depression) unless you have obtained a standalone, VPPA-compliant consent form.

D. Mandatory Links

- **Requirement:** Include a direct link to the ID5 Platform Privacy Policy: https://id5.io/platform-privacy-policy
- **Requirement:** Include a direct link to the ID5 Opt-Out: https://id5-sync.com/privacy

3. "Consent" Jurisdiction Requirements (e.g., EEA, UK, Quebec, Brazil)

Applicability: Partners with traffic originating from the EEA, UK, Switzerland, Brazil, or Quebec. These jurisdictions are referred to as "Opt-In Jurisdictions" in the ID5 DPAs.

A. ID5 Status: Independent Controller

- **Requirement:** The Partner's Privacy Policy and CMP must identify **ID5 Technology Ltd.** as a data partner and an Independent Controller and/or third-party (not a Processor). ID5 independently determines the means and purposes of building the identity graph.
    - *Note:* Identifying ID5 as a "Processor" or "Service Provider" is inaccurate and is a material breach of your Agreement, as it legally restricts ID5's ability to maintain its Identity Graph.

B. Legal Basis & TCF Compliance

- **For TCF Participants:** Partner must configure its Consent Management Platform (CMP) to signal consent/legitimate interest for **Vendor ID #131 (ID5)** for the appropriate TCF Purposes required by ID5's TCF Global Vendor List.
- **For Non-TCF Participants:** Partner must obtain legally valid opt-in consent for the transmission of IP addresses and Partner signals to ID5 for the specific purpose of creating a persistent advertising ID before the ID5 ID Service initializes on the page.

Note: ID5 must grant a specific exception for any partner processing data in the EEA which does not utilize a TCF-compliant CMP. Please speak to your account manager or primary point of contact at ID5, or email privacy@id5.io for more information.

C. International Data Transfers

- **Requirement:** Disclose that personal data may be transferred to the United Kingdom for processing. ID5 relies on the EU-US Data Privacy Framework, UK Data Bridge, and/or Standard Contractual Clauses to safeguard these transfers.

4. Rest-of-World Requirements

Applicability: Partners with global traffic (outside the US, EU, UK)

If you utilize a single global policy, you must include a "Vendor/Partner" section specifically covering**ID5 Technology Ltd** that addresses the following:

Disclosure Element	Required Standard
Role	Independent Controller (Global/EU); Third Party (US).
Timing	Data collection occurs "in real-time" or "concurrently" during the user interaction, *except*: in jurisdictions where affirmative opt-in is required, data collection occurs only after the user's affirmative consent (including via CMP).
Identity Data	Data such as IP Address, User Agent, Timestamp, and Unique User IDs are used for Identity Resolution, Cross-Device Graphing, and Ad Targeting. In some cases, partners may elect to send Hashed Emails, MAIDs, and/or Cookie IDs.

User Rights	Must link to ID5 Privacy Policy and ID5 Opt-Out.