IAB Europe Transparency & Consent Framework Policies

This document lays out policies applicable to participants in the Transparency & Consent Framework ("Policies"). Participants may include publishers, vendors or CMPs. Each category of participant has specific obligations and requirements which are included in this policy document.

Participants must adhere to these policies to maintain their participation in the Framework.

All Participants must follow applicable data protection laws. In the event of a conflict between applicable law and the Policies or Specification, then law prevails.

Participants may amend, supplement, or modify their implementation of the Framework only as expressly provided for in these policies.

Outline

Definitions

“Managing Organization” means the entity that manages and governs the Framework, including the Policies, Specification, and the GVL. The Managing Organization may update these policies from time to time, as it reasonably determines is necessary to ensure the ongoing success of the Framework.

“Consent Management Provider (or CMP)” means the company that centralizes and manages transparency for and consent of the end user. The CMP can read and update the legal basis status of Vendors on the GVL, and acts as intermediary between a Publisher, an end user, and Vendors to provide transparency, help Vendors and Publishers establish legal bases for processing, acquire user consent as needed, and communicate legal basis or consent status to the ecosystem. A CMP may be the party that surfaces, usually on behalf of the publisher, the UI/UX to a user, though it might also be another party. CMPs may be private or commercial. A private CMP means a publisher that implements its own CMP for its purposes. A commercial CMP offers CMP services to other parties. Unless specifically noted otherwise, these policies apply to both private and commercial CMPs.

“Framework Policies (or “Policies”)” means this or any other official policy documentation disseminated by the Managing Organization, and updated from time to time, that defines the policies for compliant participation in, and use of, the Framework, including, but not limited to, any policy guidance or publicly released enforcement actions.

“Framework Specification (or “‘Specification’”)” means any official documentation disseminated by the Managing Organization, and updated from time to time, that defines the technical implementation of the Framework, including but not limited to the Global Vendor List (GVL) format specification, the API documentation, and any associated implementation guidance.

“Framework UI (or UI)” means the user interface/user experience (UI/UX) defined by the Specification for presentation to a user in order to establish legal bases for Vendors on the GVL as part of their compliance with European privacy and data protection laws. The Policies and Specification will define requirements for the UI along with aspects that are configurable by Publishers.

“Global Vendor List (GVL)” means the global master list of Vendors participating in the Framework. The list is managed and maintained by the Managing Organization, and is

referenced by CMPs, Publishers and individual Vendors. It's structure and content will be defined by the Specification.

"Publisher" means an operator of a website, app, or other content where digital ads are displayed or information is collected and/or used for digital advertising, and who is primarily responsible for ensuring the Framework UI is presented to users and that legal bases, including consent, are established with respect to Vendors that may process personal data based on users' visits to the Publisher's content..

"Purpose" means one of the purposes for processing of personal data by participants in the Framework that are defined in the Framework Policies or the Specification.

"Vendor" means a company that participates in the delivery of digital advertising within a Publisher's website, app, or other digital content, to the extent that company is not acting as a Publisher or CMP, and that either accesses an end user's device or browser, or processes personal data about end users visiting the Publisher's content, and that adheres to the Policies. A Vendor may be a Controller, Processor, or both, depending on specific circumstances.

Policies for CMPs

Applying and registering

CMPs will apply to the MO for participation in the Framework. The MO will vet and approve a CMP's application according to procedures adopted, and updated from time to time, by the MO.

CMPs must provide all information requested by the MO that is required to fulfil the MO's application and approval procedures.

The MO will not approve a CMP's application unless or until the MO can verify to its satisfaction the identity of the party or parties controlling the CMP, as well as the CMP's ability to maintain its service and adhere to the Framework policies.

Adherence to Framework Policies

In addition to only implementing the Framework according to the Specification, a CMP must adhere to all policies applicable to CMPs that are disseminated by the MO in the Framework Policies or in documentation that implements the Policies, such as in operating policies and procedures, guidance, and enforcement decisions. See Accountability below regarding enforcement.

Adherence to the Specifications

A CMP must support the full Specification, including providing consent revocation services and a revocation mechanism.

A private CMP need only implement the Specifications to the extent necessary to support the legal bases required by Vendors selected by its Publisher owner.

A CMP must disclose Vendor's legal bases as declared, and update Vendors' legal bases status in the Framework, wherever stored, according to the Specification, without extension, modification, or supplementation, except as expressly allowed for in the Specification.

A CMP must not read, write, or communicate any Vendor's legal bases except according to and as provided for under the Specification, and using the standard API.

Managing legal bases

Unless otherwise allowed under the Specification, a CMP will use 13 months as the maximum lifetime of a user's consent with respect to any Vendor and Purpose.

A CMP must resolve conflicts in the DaisyBit before transmitting (i.e. reconciliation between Service-specific and global transparency and consent).

Working with Vendors

If a CMP works with Vendors who are not registered with the MO, the CMP must make it possible for users to distinguish between Vendors registered with the Framework, and those who are not. CMPs must not mislead others as to the Framework participation of any of the Vendors who are not registered with the MO.

If a Publisher or Vendor operates a CMP, the Policies for CMPs apply only to the extent of that party's CMP operation. For example, if a Publisher operates a CMP, the prohibition against a CMP discriminating against Vendors applies to the Publisher's CMP, while the Publisher remains free to make choices with respect to Vendors appearing on its sites or apps.

In any interaction with the Framework, a CMP may not exclude, discriminate against, or give preferential treatment to a Vendor except pursuant to explicit instructions from the Publisher(s) involved in that interaction and in accordance with the Specification and the Policies. For the avoidance of doubt, nothing in this paragraph prevents a private CMP from fully implementing instructions from its Publisher owner.

If a CMP reasonably believes that a Vendor is not in compliance with the Specification, the Policies, or the law, it must promptly file a report with the MO according to MO procedures and may, as provide for by MO procedures, pause working with a Vendor while the matter is addressed.

Working with Publishers

A CMP will only work with Publishers that are in full compliance with Framework Policies, including but not limited to the requirement to make a public attestation of compliance in a prominent disclosure, such as in a privacy policy.

Record keeping

A CMP will maintain records of consent, as required under Framework Policies and the Specification, and will provide the MO access to such records upon request without undue delay.

Accountability

The MO may adopt procedures for periodically reviewing and verifying a CMP's compliance with Framework Policies. A CMP will provide, without undue delay, any information reasonably requested by the MO to verify compliance.

The MO may suspend a CMP from participation in the Framework for its failure to comply with Framework Policies until the CMP comes into full compliance and demonstrates its intention and ability to remain so. The MO may expel a CMP from participation in the Framework for violations of Framework Policies that are wilful and/or severe.

Additionally, the MO may, at its discretion and according to MO procedures, take additional actions in response to a CMP's non-compliance, including public notice of the CMP's non-compliance and reporting the non-compliance to data protection authorities.

Policies for Vendors

Applying and registering

Vendors will apply to the MO for participation in the Framework. The MO will vet and approve a Vendor's application according to procedures adopted, and updated from time to time, by the MO.

Vendors must provide all information requested by the MO that is reasonably required to fulfill the MO's application and approval procedures.

Vendors must have all legally required disclosures in a prominent, public-facing privacy policy on their website.

The MO will not approve a Vendor's application unless or until the MO can verify to its satisfaction the identity of the party or parties controlling the Vendor, as well as the Vendor's ability to maintain its service and adhere to the Framework policies.

A Vendor will provide to the MO, and maintain as complete and accurate, all information required for inclusion in the GVL, according to the GVL specification.

Adherence to Framework Policies

In addition to implementing the Framework only according to the Specification, a Vendor must adhere to all policies applicable to Vendors that are disseminated by the MO in this document or in documentation that implements the Policies, such as in operating policies and procedures, guidance, and enforcement decisions. See Accountability below regarding enforcement.

A Vendor must make a public attestation of compliance with the Policies in a prominent disclosure, such as in a privacy policy.

Adherence to the Specification

A Vendor will determine the Purposes and associated Legal Bases for which it collects and processes personal data, the Features it relies on in pursuit of such Purposes, and its requirements regarding accessing a user's device. It will ensure its Purposes, Legal Bases, and access of a user's device, are completely and accurately included in the GVL.

Working with CMPs

A Vendor will work with a CMP only if it is in full compliance with Framework Policies, including but not limited to the requirement to make a public attestation of compliance.

Purposes and legal bases

A Vendor will not access a user's device or process personal data about a user without a legal basis to do so.

A Vendor will not process personal data without a legal basis to do so.

Vendors may establish legal bases outside of the Framework, for example by receiving consent from a user offline, for processing in association with a user's visit to a Publisher that participates in the Framework, so long as the legal bases are sufficient for such processing.

A Vendor may choose not to transmit data to another Vendor for any reason, but a Vendor must not transmit data to another Vendor without a justified basis for relying on that Vendor's having a legal basis for processing the personal data.

If a Vendor has or obtains personal data and has no legal basis for the access to and processing of that data, the Vendor should quickly cease collection and storage of the data and refrain from passing the data on to other parties, even if those parties have a legal basis.

Accountability

The MO may adopt procedures for periodically reviewing and verifying a Vendor's compliance with Framework Policies. A Vendor will provide, without undue delay, any information reasonably requested by the MO to verify compliance.

The MO may suspend a Vendor from participation in the Framework for its failure to comply with Framework Policies until the Vendor comes into full compliance and demonstrates its intention and ability to remain so. The MO may expel a Vendor from participation in the Framework for violations of Framework Policies that are willful and/or severe.

Additionally, the MO may, at its discretion and according to MO procedures, take additional actions in response to a Vendor's non-compliance, including public notice of the Vendor's non-compliance and reporting the non-compliance to data protection authorities.

Policies for Publishers

Participation

A Publisher may adopt and use the Framework in association with their content as long as they adhere to the Framework Policies and the Specification.

A publisher must attest in a prominent public notice, such as a privacy policy, to its compliance with the Framework Policies. The MO may disseminate guidelines for how and where such attestation must be made.

Additionally, Publishers must have and maintain all legally required disclosures in a public-facing privacy policy prominently linked from the content in association with which they are using the Framework.

Adherence to Framework Policies

In addition to implementing the Framework only according to the Specification, a Publisher must adhere to all policies applicable to Publishers that are disseminated by the MO in this documentor or in documentation that implements the Policies, such as in operating policies and procedures, guidance, and enforcement decisions.. See Accountability below regarding enforcement.

A Publisher must make a public attestation of compliance with the Policies in a prominent disclosure, such as in a privacy policy.

Adherence to the Specification

A Publisher must support and adhere to the full Specification, without extension, modification, or supplementation except as expressly allowed for in the Specification.

A Publisher must not read, write, or communicate any Vendor's legal bases except according to and as provided for under the Specification, and using the standard API.

Working with CMPs

Publisher as CMP

A Publisher will work with a CMP only if it is in full compliance with the Policies and the Specification.

A Publisher may operate a private CMP. A Publisher's private CMP will be subject to the Framework Policies for CMPs just as a commercial CMP would, unless expressly stated otherwise in the Framework Policies or the Specification.

Working with Vendors

A Publisher may choose the Vendors it wishes to be included in the Framework UI. The Publisher communicates its preferences to the CMP, who in turn implements them in the Framework, all in accord with the Specification.

A Publisher may work with Vendors that are not in the GVL but as explained below must be careful not to confuse or mislead users as to which Vendors are operating within the Policies.

Managing Legal Bases

The Framework does not dictate how Publishers respond to a user's acceptance or rejection of Purposes and/or Vendors .

A Publisher is responsible for using the Framework in accord with the Policies and the Specification to help Vendors establish legal bases for all Purposes they claim. This includes, for example, that when a Vendor that was not included in a prior use of the Framework UI is added by the Publisher, the Publisher must resurface the Framework UI to establish that Vendor's legal bases.[1] It also means resurfacing the UI, for example, when a previously surfaced Vendor claims a previously undisclosed Purpose.[2]

Publishers should remind users of their right to object to processing or withdraw consent, as applicable, at least every 13 months.

Accountability

The MO may adopt procedures for periodically reviewing and verifying a Publisher's compliance with Framework Policies. A Publisher will provide, without undue delay, any information reasonably requested by the MO to verify compliance.

The MO may suspend a Publisher from participation in the Framework for its failure to comply with Framework Policies until the Publisher comes into full compliance and demonstrates its intention and ability to remain so. The MO may block a Publisher from participation in the Framework for violations of Framework Policies that are wilful and/or severe. The MO may enact a suspension or block of a Publisher by notifying CMPs that the Publisher is not in full compliance.

Additionally, the MO may, at its discretion and according to MO procedures, take additional actions in response to a Publisher's non-compliance, including public notice of the Publisher's non-compliance and reporting the non-compliance to data protection authorities.

[1] This can be done by comparing current vs prior version of the GVL.
[2] This can be done by comparing current vs prior version of the GVL and then comparing to Publisher's list.

Policies for Interacting with Users

This section applies to any party deploying the Framework UI/UX in interactions with users, typically a Publisher or CMP. The first party in the interaction with the user, typically a Publisher is responsible to ensure that these requirements are met.

A Publisher is responsible for determining when the Framework UI will be shown in accord with the Framework Policies and the Specification, consistent with legal requirements to support the legal bases and device access needs declared by Vendors. A Publisher will typically be aided in this by a CMP.

The Framework Policies and the Specification will establish baseline requirements for language, design, and other elements in the UI. Some requirements are included in the Appendix B to this document. The Specification may include additional requirements.

The list of Vendors generated from the GVL must display at least the minimum information for each Vendor as defined by the Specification.

If a UI is to include non-GVL parties, the party deploying the UI must ensure those parties are prominently distinguished from the GVL parties and do whatever is necessary to avoid confusing or misleading users as to the Framework participation of any of the parties.

The UI must not include representations that may conflict with Vendor's legal bases. Parties should take into account that Vendors may have legal bases established outside of the Framework so

The UI may be used for transparency and consent for the Publisher's own processing of personal data.

Users must be provided clear, prominent instructions for revoking consent or objecting to processing, as applicable.

Appendix A: Purpose and Feature Definitions

A "**Purpose**" is a data use that drives a specific business model and produces specific outcomes for users and businesses. Purposes must be itemised at the point of collection, either individually or combined.

A "**Feature"** is a method of data use or data sourcing that overlaps across multiple purposes. Features must be disclosed at the point of collection, but can be itemised separately to cover multiple purposes.

Purposes

1. **Information storage and access**: The storage of information, or access to information that is already stored, on your device such as advertising identifiers, device identifiers, cookies, and similar technologies.
2. **Personalisation**. The collection and processing of information about your use of this service to subsequently personalise advertising and/or content for you in other contexts, such as on other websites or apps, over time. Typically, the content of the site or app is used to make inferences about your interests which inform future selection of advertising and/or content.
3. **Ad selection, delivery, reporting**: The collection of information, and combination with previously collected information, to select and deliver advertisements for you, and to measure the delivery and effectiveness of such advertisements. This includes using previously collected information about your interests to select ads, processing data about what advertisements were shown, how often they were shown, when and where they were shown, and whether you took any action related to the advertisement, including for example clicking an ad or making a purchase. This does not include Personalisation, which is the collection and processing of information about your use of this service to subsequently personalise advertising and/or content for you in other contexts, such as websites or apps, over time.
4. **Content selection, delivery, reporting**: The collection of information, and combination with previously collected information, to select and deliver content for you, and to measure the delivery and effectiveness of such content. This includes using previously collected information about your interests to select content, processing data about what content was shown, how often or how long it was shown,

when and where it was shown, and whether the you took any action related to the content, including for example clicking on content. This does not include Personalisation, which is the collection and processing of information about your use of this service to subsequently personalise content and/or advertising for you in other contexts, such as websites or apps, over time.

5. **Measurement**. The collection of information about your use of the content, and combination with previously collected information, used to measure, understand, and report on your usage of the service. This does not include Personalisation, the collection of information about your use of this service to subsequently personalise content and/or advertising for you in other contexts, i.e. on other service, such as websites or apps, over time.

Features

1. **Offline data matching**. Combining data from offline sources that were initially collected in other contexts with data collected online in support of one or more purposes.
2. **Device linking.** Processing data to link multiple devices that belong to the same user in support of one or more purposes.
3. **Precise geographic location data.** Collecting and supporting precise geographic location data in support of one or more purposes.

Appendix B: UI/UX Guidelines and Requirements

UI/UX Guidelines and Requirements

When this appendix refers to “Purposes” or “Vendors”, it refers to purposes and vendors within the Framework. Nothing in this appendix shall prevent service operators from adding other purposes or vendors managed outside of the Framework, as long as these are not presented in such a way that may give the impression that they are part of the Framework.

Bundling of Purposes and/or Vendors

Purposes and/or Vendors must be disclosed without modification in such a way that it is clear to the user that each Purpose and/or Vendor is a separate and distinct processing purpose and/or entity.

User choices about all or some Purposes and/or Vendors may be bundled, i.e. presented to the user in a way that he or she is only able to exercise a choice about all or some purposes *en bloc* but not separately.

Without prejudice to paragraph 2, a user should be allowed to exercise choices about Purposes and/or Vendors at a granular or semi-granular level, i.e. a user should be able to exercise separate and different choices about some or all Purposes and/or Vendors presented to him or her.

Formatting of UI/UX

When providing transparency about Purposes and/or Vendors in combination with requesting a user’s consent, the transparency and consent prompt must be presented in a modal that covers all or substantially all of the content of the page. If the modal does not cover all or substantially all of the content of the page, it must be prominently displayed.

When providing transparency about Purposes/and or Vendors without requesting a user’s consent, transparency may be provided in an easily accessible privacy notice.

The calls to action in a transparency and consent prompt must be presented with equal prominence in a manner that does not suggest that one option is preferable over another. Publishers must offer the possibility to obtain more detailed information, where the user should be offered ways to exercise choices about Purposes and/or Vendors at a granular or semi-granular level. Publishers may (but do not have to) offer the user the possibility to say no.

The UI must disclose the following information at a first layer of information that is presented in line with paragraph 1:

- Personal data is processed, and examples of personal data processed
- The purposes for which personal data is processed and the features used by vendors to support those purposes
- Data is processed by third parties, and a link to enumerated list of such third parties.
- The possibility to exercise choices/consent and the possibility to revisit and change (consent)-choices at any time

The UI may disclose the following information at first level, but must at the very least disclose the following information in a secondary layer that is easily accessible from the first layer that is presented in line with paragraph 1:

- The purposes for which personal data is processed, including the standard definition of that purpose
- The vendors who are processing personal data

Examples of ways in which a list of purposes and vendors may be provided via secondary screens include, but are not limited to, a link or a drop-down menu.

The list of purposes and/or vendors shown in the UI must have the following characteristics:

- It must be generated from information taken from the global vendor list
- At a minimum, vendor name, link to privacy policy, purposes and features must be displayed

Publishers may allow users to select or deselect individual purposes and/or vendors. Publishers may choose how to present these choices. Publishers may decide what the consequences are of a user's choices, if any.

When should a user be shown disclosures and asked for consent (or given a choice to object if a vendor is relying on legitimate interests)?

Publishers may determine when and how often to to trigger a UX/UI. The publisher can rely on its UI provider and/or the CMP to do so. It should be triggered at a minimum:

- Where a user is visiting a site for the first time and the site is operated from a country where the GDPR/ePrivacy is applicable.
- Where a user is visiting a site for the first time from and the user's IP address indicates that he or she is in a country where the GDPR/ePrivacy is applicable.
- When a publisher has added a new vendor to its list of vendors and needs to provide notice of and transparency into that new vendors data processing and obtain consent from a user or provide information about how to exercise the right to object with respect to that vendor.

Language of text presented to end users

The UI must support the language(s) in which the service on which the UI is surfaced is offered. In addition, the UI may support other language(s), for example, language(s) used in the country from which a user is accessing a service.

First Layer:

"Ads help us run this [site] [app]. When you use the [site] [app] selected companies may access and use information about your device to serve relevant ads.

[drop down of purposes]
[drop down of information about your device]

Learn more and manage your choices.

You can change your mind and revisit your choices at any time."[MM(E1] [MM(E2]

Second Layer:
"**Purposes**

We and selected companies may access and use information for the purposes below. You may customize your choice or continue using our [site] [app] if you are OK with the purposes.

[list of purposes and their definitions (definitions may be presented as an expandable "learn more link") and on or off toggle (if granular choice offered)]"

Vendors

I don't want any of these vendors accessing information on my device or using information about my device: ON/OFF

[list of vendors, their consent purposes, and consent toggle]

Note: a Publisher may choose to no longer display purposes that a user has deselected under purposes, and remove vendors all of whose purposes the user has already deselected.

Depending on the type of data they collect, use and process and how they collect, use and process it, including other factors such as how their systems are designed, certain vendors are not seeking your consent for the use of information for certain purposes, but you can always opt out. For information on each vendor and to exercise your choice, see below:

[insert table of vendors, legitimate interest purposes, and other disclosures]"

Note: a Publisher may insert a paywall on any of the screens

How often does the text need to be presented to end users?

If an end user interacts with the prompt and makes a choice, a Publisher may display a confirmation of the user submitting a choice with instructions on how to change settings later. A user should be reminded of the option to change their settings at least every 13 months.

If an end user does not interact with the prompt but instead moves into the [site] [app] and begins using the site, the prompt should be shown to that end user at least a second time, if not more frequently. The Publisher should run a "privacy toolbar" reminder at the bottom of its page.

Version History and Changelog

- Version 2018-04-10.1 – Initial Framework Policies
- Version 2018-04-25.2 – Added Purpose and Feature Definitions to Appendix A, and UI/UX Guidelines and Requirements to Appendix B
- **Version 2018-10-03.2a** – Removed a provision stating CMPs must only work with Vendors registered with the MO. Clarified conditions for providing services to Vendors not registered with the MO.