Transparency & Consent Framework

FAQ

WORK IN PROGRESS – NOT FINAL – NOT LEGAL ADVICE

The IAB Europe GDPR Implementation Working Group ("GIG") has created this document for discussion and collaboration purposes. It may contain errors and omissions, is subject to iteration, and should not be taken as legal advice.

The intention of this document is to present the working group's current position on key questions relevant to the deployment of the Transparency & Consent Framework ("Framework"). This document is expected to iterate in the coming months as additional questions are raised, key stakeholders provide feedback and deferred questions are addressed.

Table of Contents

Introduction

In February 2017, the IAB Europe assembled parties representing various participants in the online advertising ecosystem, in particular parties from both the supply and demand side of the ecosystem, to work collectively on guidance and solutions to the requirements of the General Data Protection Regulation ("GDPR"). That working group is known as the GDPR Implementation Working Group ("GIG"). One of the working groups within the GIG was tasked with developing guidance on consent as a legal basis of processing and out of that group an additional working group was formed to develop a technical solution for companies to use, where and if necessary, to request, obtain and disseminate consent to various parties in the online advertising ecosystem that may be relying on consent as a legal basis of processing and/or may have parties integrated with them that rely on consent.

About the Transparency & Consent Framework ("Framework")

The scope of the technical working group's initiative increased further into a broader initiative to develop an industry solution to allow website operators to

1. Control the vendors they wish to allow to access their users' browsers and devices and process their personal data and disclose these choices to other parties in the online advertising ecosystem
2. Seek user consent under the ePrivacy Directive (for setting cookies or similar technical applications that access information on a device) and/or the GDPR in line with applicable legal requirements and signal the consent status through the online advertising ecosystem

In summary have one place to go to:

- Understand privacy-related disclosures about those vendors
- Use those disclosures to make privacy-related disclosures to its users
- Disseminate the disclosure status through the online advertising ecosystem.

The various pieces of the framework are the following:

- A global vendor list
- The technical specification for capturing, storing and signalling user consent in the context of digital advertising
- Policy underlying the
    - Disclosures to be made by vendors included on the global vendor list
    - Use of the global vendor list and the reference architecture

For purposes of this documentation, the following terms have the following definitions:

Definitions

- "***CMP***" means a company that can read the vendors chosen by a website operator and the consent status of an end user (either service specific (through a first-party cookie) or global (through a third-party cookie). A CMP is not synonymous with a company that surfaces the user interface to a user (although it can be the same).
- "***Purposes***" mean the purposes for which a Controller enabled by a website operator is using personal data collected from (or received by a third party) about an end user.
- "***DaisyBit***" means information compressed into a binary value and passed throughout the online advertising ecosystem through the OpenRTB specification.
- "***Vendor***" means a third party that a website operator is using in connection with surfacing content to its end users that either (1) accesses an end user's device or browser; and/or (2) collects or receives personal data about the website operator's end users. As such, a vendor need not be a Controller.

License

FAQ

Section One: **WHY WAS THE FRAMEWORK CREATED AND HOW WILL IT BE USED?**

1. Background

In November 2017, IAB Europe and a cross-section of the publishing and advertising industry, announced the Framework to help publishers, advertisers and technology companies comply with key elements of GDPR – a new EU data protection regulation that comes into effect on 25th May 2018. In addition to clarifying the definition of 'personal data', the new regulation will require companies to change the way they inform consumers about how their data is used. It will also mean changes to how those companies obtain consent before personal data is used (where consent is necessary) or before accessing a device or using cookies (or other information storage mechanics) on user devices under the ePrivacy Directive.

2. What exactly does consent mean under GDPR?

EU law creates an exhaustive "positive list" of legal bases for data processing the GDPR lays down six possible legal bases for the processing of personal data. Personal data may only be processed if the processing can be justified by one of these six legal bases. It is up to the company that determines the purposes and means of processing the data, the so-called "data controller", to decide which legal basis is most appropriate for the processing that needs to be done, and to be able to justify and document the choice.

Three of the six legal bases are most relevant for digital advertising: legitimate interests of the data controller, consent of the data subject, and performance of a contract. Conceptually, legitimate interests may be utilised when the interest is documented and articulates the results of a three stage balancing test. "Consent" under the regulation requires an unambiguous action and may not merely rely on providing the consumer with the ability to opt out. Both legitimate interest and consent appear to be more narrowly drawn in the GDPR than under the old rules. The Regulation contains significantly expanded requirements with respect to information disclosure to users about how their data are being processed. A working paper discussing the requirements of consent under the GDPR can be found here: https://www.iabeurope.eu/policy/gig-working-paper-on-gdpr-consent/.

3. How does the Framework assist website operators?

As companies prepare for May 2018, a key challenge is ensuring that data processing for digital advertising falls within the scope of at least one relevant legal basis, that there is an audit trail to demonstrate that, and that the associated information disclosure requirements are met. The IAB Europe Framework aims to help companies meet these requirements. The Framework will help website operators become GDPR-ready by giving them a standardized framework with which to disclose the companies they wish to allow to access their users' browsers and devices and process their personal data and disclose these choices to other parties in the online advertising ecosystem and a common language with which to communicate consumer consent (where necessary) for the delivery of relevant online ads and content. Among other things this includes:

- Controlling which companies they wish to allow to access their users' browsers and devices and process their personal data and disclose these choices to other parties in the online advertising ecosystem
- Seeking user consent under the ePrivacy Directive for setting cookies or similar mechanics that access information on a device and signaling the consent status through the online advertising ecosystem
- In relation to GDPR provide one go-to place to understand privacy-related disclosures about vendors and make these disclosures to its users. Provide disclosures that must be provided by vendors that are Controllers. Seek user consent where vendors may require it under GDPR (as a legal basis for processing data)

4. How does the Framework operate?

The Framework is based on a JavaScript API and will enable the passing of selected vendor information and user consumer consent signals. The framework will be open source and distributed across participating organisations which meet the criteria of becoming a Consent Management Provider (CMP). Each CMP's website will act as an entry point to the framework for consumers when receiving disclosures about companies accessing their devices, using their personal data and when sharing their consent.

5. Who will use the Framework?

We're encouraging any company worldwide that needs to access the devices or browsers of individuals located in the EU or use the personal data of people in the EU to make use of this framework, including publishers, advertising technology companies and advertisers.

6. What are the benefits of the Framework?

- Any vendors (SSPs, DSPs, ad servers, etc.) used on a publisher site can be disclosed to consumers with up to date information obtained from an industry operated Global Vendor List (see section three for details on Global Vendor List) and (where necessary) can receive their consent status via the industry-accepted Consent Manager JavaScript API installed by a publisher
- Highly flexible and affordable solution that supports both global and server-specific consent (where necessary)
- A solution that is both open-source and not for profit with consensus based industry governance
- Multiple organisations can serve as CMPs and develop their own API and UI. This gives publishers choice over who they work with and flexibility in format of UI. Publishers can implement their own customised UI, work with an industry coalition or use another UI that can integrate with various CMPs
- Industry association development that reduces dependency on single development resource or company - a consolidated effort that improves efficiency and time to

market

7. What would be the impact of not having the Framework?

Website publishers generate a significant proportion of their revenue from advertising (digital news organisations generate 80% of their revenue from advertising). Without a framework publishers, advertisers and advertising technology companies that work together to effectively deliver digital advertising would have no common language to understand which consumers should see which advertisements. This impact would be in three key areas:

- **Publishers**: whose business models are already under pressure would lose access to this vital source of revenue and revert to alternative approaches to funding content creation such as putting their content behind pay walls
- **Consumers:** online audiences would see the relevancy and standard of advertising noticeably reduced, lowering the quality of their online experience or lose access to quality free content if publishers can no longer fund their content
- **Jobs and the economy:** significant revenue is generated each year by the European advertising industry. The 2016 research study conducted by HIS Markit '*The economic contribution of digital advertising in Europe"* jointly commissioned by IAB Europe and EDAA revealed that contribution of the digital advertising industry to the EU economy was Euro 526 billion in 2016 and accounted for over 6 million of jobs

Section Two: **PUBLISHERS AND THE FRAMEWORK**

1. Do service-specific preferences override global? Can publishers revert to a service-specific disclosures and consent if they choose to?

The CMP concept foresees that service-specific disclosures and consent take priority over global disclosures and consent. If a user makes a global transparency and consent choice first, and later makes a service-specific choice, the service-specific transparency and consent choice will determine a user's status for that service

2. Can publishers operate without a CMP?

Yes, a CMP is essentially just a protocol for making sure that disclosures about a publishers approved vendors are made and the consent signal is collected and transmitted in a standardised way, rather than new protocols needing to be written and agreed to for each publisher/vendor relationship. A publisher does not need a CMP to collect and store service-specific consent. A publisher may choose to act as a CMP

3. Can publishers work with vendors who are not on the GVL?

We are proposing that publishers only work with vendors on the GVL. The proposed GVL will be vetted and all vendors will be required to strictly follow policies and procedures in order to participate. Registration by vendors on the vendor list will be required to use the Framework. Vendors will be responsible for complying, not publishers. Publishers control which vendors they want to use from the GVL. Publishers are not required to use, disclosure and seek consent (where necessary) for all vendors on the GVL but they can only use the Framework if they work with vendors registered on the GVL.

4. Can publishers avoid passing consent to companies they don't trust?

Publishers have full control over who they partner with, who they disclose to their users and who they obtain consent for.

5. How do publishers differentiate between those who have opted out vs. those not opting in?

A consent signal will either be 1 (user has given consent) or 0 (user has not given consent). If the user has not yet expressly given consent, there will be no cookie containing the consent signal and therefore the user will be prompted for consent. The Framework applies to obtaining, managing and transmitting consent not how a publisher responds to consent or lack of consent

6. Can publishers define permissions (i.e. purposes) for which they're using personal data that they're disclosing to their users and for which they're gathering consent (where necessary)?

The Framework supports this as well as the ability to add more purposes going forward - standardisation is an important feature of the success of the Framework therefore it is important that purposes are collectively agreed

7. Is there flexibility to add new purposes in future?

Yes, the Framework is flexible in this regard.

8. Do vendors need to justify why permission is sought for consent and how they will use it?

The GVL includes standardized purposes. When signing up to the GVL, vendors are required to choose the purposes for which they are collecting and processing personal data. One vendor may be collecting and processing personal data in a manner that they believe requires consent while another may be collecting and processing personal data

in a manner that does not require consent. Additionally, many vendors will be collecting and processing personal data for more than one purposes included in the GVL in which case they need to meet the transparency and control requirements for each of those purposes.

9. Can publishers control how vendors disclosures are presented to their users?

Publishers decide how consent is presented to consumers. We have proposed minimum policies related to the vendor disclosures to ensure the manner in which preferred vendors are disclosed to a publisher's users meets legal requirements. Section four of this document includes proposed language publishers can use in their UI.

10. How is transparency and consent expiry managed? If transparency and consent is managed globally, can one publisher override the expiry?

In line with guidance from the CNIL, we are recommending a 13-month maximum period for surfacing disclosures and obtaining consent (where necessary) for approved vendors. This can be reset by a disclosure and consent refresher that each publisher can activate.

11. What is the cost for publishers to participate in this framework?

The industry solution is an open-source solution and will be maintained as such by the industry.

12. Does each vendor have visibility of other vendors and whether they are an approved vendor and whether they required and obtained user consent?

A vendor can only provide disclosures and request user consent for their purpose via the standard API. Only CMPs can read consent status per website where approved vendors and consent per vendor is stored. The OpenRTB request will contain the entire DaisyBit, allowing a vendor to see which other vendors are an approved vendor or a publisher and whether they have obtained consent (and for which purposes) and which have not.

Section Three: **GLOBAL VENDOR LIST (GVL) SUPPORTING THE FRAMEWORK**

1. Who will be included on the GVL and what are their obligations?

- The GVL will include all vendors (whether Controllers or Processors) that agree to the following:
    - Compliance with industry protocol policies that may be adopted in the future for this Framework
    - Updating its code so cookies are not set unless they have received a consent signal from a CMP JS API or in the bid request, or unless they have an applicable legal basis to set a cookie
    - Not to process personal data for a purpose that relies on consent until the vendor has received a consent signal directly from a CMP or in the request in any given online request for that purpose. For example, if a vendor receives a bid request and does not have consent to process the personal data contained in that bid request, it may not process any personal data contained in that bid request unless it has another legal basis for doing so
- Vendors may choose not to pass bid requests containing personal data to other vendors who do not have consent. In the event a bid request is passed containing personal data to a receiving vendor without consent, the vendor that does not have consent is responsible to only act upon that data if it has another applicable legal basis for doing so.
- Publishers, advertisers and advertising technology providers may impose additional obligations. They may require an SSP or Ad Exchange to adhere to a consent signal when passing along a bid request. They will restrict DSP using creatives served by vendors that have not received consent or are not participating in the industry framework.

2. What vendor disclosure will be required through the global vendor list? In the first instance will include but not limited to

- Legal name
- Status: clarification regarding status as Controller/Processor in ecosystem for various purposes
- If a Controller - purposes for which they're using personal data and associated features
- If a Controller - legal basis for processing for each purpose
- Link to its privacy policy

- GDPR Chapter III disclosures for example type of personal data being collected, retention period, data subject rights, etc.

3. Can Publishers choose which vendors they wish to work with on the global vendor list and disclose to their users and, where necessary, obtain consent for?

Yes, publishers maintain complete control over which vendors they wish to work with. Publishers also choose whether to surface transparency disclosures and obtain service-specific or global consent for their vendors.

4. How is the global vendor list managed and updated?

- When new vendors are added to the vendor list and a publisher chooses to work with them, disclosures will need to be made to the user and (where necessary) user consent will need to be obtained for those new vendors. They cannot rely on a global consent given to a prior list of vendors
- A central entity will manage and update the vendor list, consistent with predefined policy rules
- Similarly, if a vendor adds a new purpose for which it needs disclosures to be made on its behalf or for which it relies on consent, new disclosures must be made and consent must be obtained for that new purpose

5. Is there process for exclusion from the global vendor list for infractions?

Yes, the central entity will set the process and rules

6. Can cookies be read and set, pixels or tags rendered, or bid requests transmitted, if the receiving vendors have not received consent, but also do not receive personal data associated with the pixel, tag or request?

Cookies should not be read or set, pixels or tags shouldn't be rendered, and personal data shouldn't be processed without consent or another applicable legal basis

Section Four: **CONSENT UI AND THE FRAMEWORK**

Once a publisher has chosen which vendors it wishes to work with from the global vendor list, it will surface these vendors and disclosures about these vendors through a user interface (UI) of its choice

1. Can purposes and vendors be bundled in the consent UI?

- No, purposes cannot be bundled the end user must have a choice over each purpose in the UI, similarly the publisher may offer their users a choice over each vendor choice
- However, the lists of purposes and/or vendors can be collapsed if the user has the ability to expand the list

2. Other than the consent language, what other requirements should the UI include?

- The transparency and consent prompt should be presented in a format that covers all or substantially all of the content of the page
- The calls to action to give (or if a publisher wishes to give that option: not give consent) must be presented with equal prominence
- The UI may choose to present the purposes and list of vendors in a secondary screen that is accessible from a format where consent choices are provided
- Examples of ways in which a list of purposes and vendors may be provided via a secondary screen include but are not limited to a link or a dropdown menu.
- The list of vendors shown in the UI must have the following characteristics:
  - It must be generated from information taken from the GVL
  - Publisher may allow users to select or deselect individual vendors. At a minimum, vendor name, link to privacy policy, purposes and features (if a Controller relying on consent) should be displayed with link to other Section 14 disclosures
  - Publisher may choose how to present choices for purposes and vendors, however the user must confirm their choice with an affirmative act
- The UI should support obtaining consent for the publisher (website operator)
- The UI should provide clear instructions (such as a link on the primary page) for opting out of purposes for which a vendor may be relying on legitimate interests or revocation of consent

3. When should a user be shown disclosures and be asked for consent?

- The publisher determines when and how often to trigger a UI. The publisher can rely on its UI provider and/or the CMP to do so.
- Generally, it should be triggered when a user visits a site for the first time from an IP address in the EU or when a publisher has added a new vendor to its list of

vendors and needs to make disclosures to its users about those vendors and obtain consent from a user for that vendor
- The Publisher/UI/CMP may trigger it in other instances.

4. What are the rules around when and how often to trigger the UI after a consumer has said no or revoked consent or when a new vendor or purpose is added?

- It is up to the Publisher and CMP to determine how often/whether to surface the UI
- For those CMPs and Publishers looking for guidance, it is recommended that disclosures may be made and consent may be re-requested once every 30 days

5. What language is required to show to the consumer?

- In order that all companies and vendors participating in the industry framework understand the scope and validity of the disclosures made about them and consent where they require it, the following is suggested language which may be customised by a publisher or advertiser (landing page) as long as the following is conveyed:
  - Multiple parties will be setting/reading cookies of a user either on that site (if publisher will only obtain and provide service-specific consent) or globally
  - Purposes for which the vendors set/read cookies and/or process personal data with consent
  - List of Vendors with corresponding purposes and links to their privacy policies
  - User can change its choices and revoke consent (where it is requested) at any time.
- Proposed example text presented to the consumer through the consent UI
  - "[Site] and our partners set cookies and collect information from your [browser] [device] to provide you with [website] content, deliver relevant advertising and understand [web] audiences. [View partner info]"
  - "We use technology such as cookies on our site to collect and use personal data to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our partners who also use technologies such as cookies to collect and use personal data to personalise content and ads, to provide social media features and to analyse our traffic on our site and across the internet. View info on our partners and their use of this data. You can always change your mind and revisit your choices." OK or Manage use of your Data
- If user clicks into "Manage use of your Data", the text presented to the consumer (based on a site owner's choice) that would allow users to select all or consent on a purposes-by-purpose basis.
  - Choose the purposes for which we and vendors approved by us can set cookies and/or share and use your [personal data]
    - Select:
      - ALL or
      - List of purposes

- The text presented to the consumer on the screen (based on a site owner's choice of vendors) should allow users to select all or consent on a vendor-by-vendor basis.
    - Choose the vendors we can share your personal data with
        - Select:
            - ALL or
            - List: Vendor; purposes; link to privacy policy

Section Five: **CONSENT MANAGEMENT PROVIDERS (CMPs) AND THE FRAMEWORK**

Where necessary, a user's consent status is stored, read and passed throughout the online advertising ecosystem through a CMP

1. What is a CMP?

- A CMP is a name for a company that captures and stores a publisher's preferred vendors and purposes and the consent status of a user (either service-specific (through a first-party cookie) or global (through a third-party cookie) per purpose (where necessary) and transmits that information throughout the online advertising ecosystem
- It is not the same as the company that surfaces the UI to a user (although it can be the same)

2. What requirements need to be met to become a CMP?

- Must apply to and be approved by a central entity so they can obtain an ID that can be used within the Framework – all signals of preferred vendors and user consent need to include a CMP ID
- Must agree to adhere to the standards set forth by the entity, including:
  - Can't refuse to work with any vendors if those vendors are on a publisher's approved vendor list. However, remember that publishers may decide not to surface certain CMPs on their sites and may decide not to work with certain vendors and CMPs can refuse to work with certain vendors on their own platforms (unrelated to reading and disseminating preferred vendor and consent status)
  - Must agree to follow the technical specifications for the Framework
  - Set 13 months as maximum validity of consent
  - In future, there may be a recommended best practice or code of conduct adopted for CMPs

3. What if a CMP violates the rules?

The central entity determines whether to allow the CMP to continue to integrate with the domain following a predetermined procedure adopted and maintained by the central entity

4. Does the CMP need consent from the consumer to be a CMP?

No, the CMP will not need to have consent to set a cookie to capture and store consent state. This falls under a necessity exception.

Section Six: **USER CONSENT STATUS**

Once a CMP has read and stored a user's consent status it is important to understand how the consent status is handled

1. Are there other consent states that will not be transmitted as part of the Framework?

- Possible consent states that will not be signalled include:
  - **Revoked** - this can be determined based on audit trail held by the vendor. NOTE: Revocation is NOT the same as a user requesting right to access / deletion of data.
  - **New User** - this can be determined by the absence of a cookie.

2. What are the consent states that are available?

- There are two consent states in the protocol:
  - **No Consent** (0) which could include new users, users who have said no, or users who have revoked consent
  - **Consent** (1)

3. Will a central entity host common revocation pages and what functionality would that revocation need to have?

- Initially, CMPs and Publishers will host revocation pages and when revocation occurs will update consent status in the cookie from 1 to 0
- The central entity may in future manage one page where a consumer can come and execute choices but this is currently beyond the scope of the Framework

4. How long is consent valid once it is granted?

The lifespan of consent differs from case to case. Consistent with what CNIL has interpreted to be reasonable life of a cookie under the ePrivacy Directive, as guidance consent may be valid for 13 months, before a refresh or reminder is recommended

5. Should vendors report to the CMP if it receives a consent or revocation signal directly?

- Yes. Vendors must report global consent changes to the CMP, vendors should also report service- specific consent changes to the CMP if possible

6. What is the standard logic to reconcile conflicting signals?

- See 'Should vendor be required to report back into CMP if it receives a consent or revocation signal directly?' for an example of why we might need to reconcile
- Service-specific consent status overrules global consent status for that service. For example user gives global consent on Site A. User then visits Site B and is prompted

for service-specific consent and says no. Result: Vendor has global consent except on Site B

- When comparing two like signals for example both regarding service-specific the most recent timestamp overrules
- CMPs must resolve conflicts before transmitting the appropriate consent status through the DaisyBit mechanism to avoid conflicts.

7. Where is service-specific consent stored?

- Server specific consent can be stored in any storage medium to which a digital service requiring has access too which could be a first party cookie

Section Seven: **OTHER IMPORTANT POLICY CONSIDERATIONS**

1. What is the definition of service-specific and global consent?

- Service-specific consent is given by the consumer to a publisher or vendor to access their device and/or perform the requested processing purposes where a publisher or vendor requires consent for their site
    - If a vendor receives service-specific consent from a consumer for multiple services, the vendor may combine information about that consumer across those consented sites
    - If legitimate interests exist, the controller may use the data collected for purposes outside of that specific site
- Global consent is given by the consumer to access their device and/or perform the requested processing purposes across the internet.

2. **If a Publisher has to get consent for itself and other parties on its site(s) how can it minimise the impact on the consumer?**

- While the Framework supports service-specific consent, the Framework's support of global consent is intended to minimise repeated solicitations for the same parties who may be present on multiple sites
- The publisher may be able to present a lighter-weight consent request for itself (not listing third parties) in instances where those third parties have already obtained global consent, which might increase chances of obtaining such consent. If such consent isn't revenue critical, it could also be presented in less intrusive manners.
- It is important to emphasise that we are not introducing new requirements for consent but responding to EU legal requirements to obtain consent

2. When a user revokes consent does this trigger the invocation of other data subject rights, such as the right to be forgotten?

Not necessarily. The party that controls the UI receiving the revocation signal is under no obligation to directly trigger any other data subject rights

3. How are common purposes and supporting features defined?

- Proposed **purpose** list:
    - **Accessing a device** allow storing or accessing information on a user's device.
    - **Advertising personalisation** allow processing of a user's data to provide and inform personalised advertising (including delivery, measurement, and reporting) based on a user's preferences or interests known or inferred from data collected across multiple sites, apps, or devices; and/or accessing or storing information on devices for that purpose
    - **Analytics** allow processing of a user's data to deliver content or advertisements and measure the delivery of such content or advertisements, extract insights and generate reports to understand service usage; and/or accessing or storing information on devices for that purpose

    - **Content personalisation** allow processing of a user's data to provide and inform personalised content (including delivery, measurement, and reporting) based on a user's preferences or interests known or inferred from data collected across multiple sites, apps, or devices; and/or accessing or storing information on devices for that purpose.

- Proposed **feature** list:
    - **Matching data to offline sources** combining data from offline sources that were initially collected in other contexts
    - **Linking devices** allow processing of a user's data to connect such user across multiple devices.
    - **Precise geographic location data** allow processing of a user's precise geographic location data in support of a purpose for which that certain third party has consent.

- Distinction between **Purpose** and **Feature**:
    - **Purpose** is a data use that drives a specific business model and produces specific outcomes for consumers and businesses. Purposes must be itemised at the point of collection, either individually or combined
    - **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.

Section Eight: **CENTRAL CONTROL**

1. **What industry entity will maintain the Framework and global vendor list?**

IAB Europe will continue to drive the interpretation and communication of Framework and will manage the GVL. The IAB Tech Lab will manage the technical specifications and on-going updates to the framework.

2. How will the different aspect of the Framework be managed?

- **The technical specifications will be managed Tech Lab**

    - Set and maintain standardised consent cookie (and other storage) formats - both global and service specific

    - Set and maintain standardised JS API functions documentation and spec to be used by CMPs developing transparency and consent UX and JS APIs.

    - Set and maintain any additions to the OpenRTB specification

- **The GVL will be managed by IAB Europe**

- IAB Europe will manage the registration of vendors on the GVL and hosting

- **Non-technical procedures will also be managed by IAB Europe:**
  - Approve CMPs and managed specification
  - Establish and standardise requirements for language presented to users when providing transparency and asking for consent related to: service-specific versus global, purpose and collection/use of data.

3. What standards do industry vendors, publishers and consent management platforms need to adhere to in order to participate in the Framework?

- Standardized disclosures on the GVL
- Disclosure language: service-specific versus global, purpose and collection/use of data
- Central subdomain, consent storage cookie formats
- Consent JS API definitions implemented by CMPs, and used by publishers, SSPs, and DSPs
- When and how often to re-provide transparency disclosures and re-request consent (where necessary) from a user who has previously not provided consent for a vendor, and how long consent is valid once given
- CMPs: To not give preferential treatment to any DSP, SSP or other vendor when developing their solution
- Vendors: updating their code to not set cookies or record, collect, or process other personal data unless their transparency disclosures have been surfaced in the UX to a publisher's end users and they have an applicable legal ground for processing such as legitimate interest or receiving consent from the CMP JS API or the bid request

APPENDIX:

TECHNICAL DETAILS

1. How does the Framework work?

- A central industry entity maintains a portal at a domain name (e.g. mgr.consensu.org) that hosts a list of participating vendors (a Global Vendor List) which is used by Publishers to make the necessary disclosures to provide dynamic transparency disclosures with the help of the GVL through which participating companies provide relevant information about their data processing practices and keep these disclosures up to date and Publishers (in coordination with Consent Manager Providers (CMPs)) to obtain consent, where necessary. In future this portal may also house a central consumer-facing information site and a central subject access request UX, that would point consumers to the appropriate place for each vendor where they can exercise their data subject rights
- The industry entity allocates subdomains (i.e. cmp1.mgr.consensu.org) to approved CMPs. This enables CMPs to read and write third-party global browser cookies with a domain of ".mgr.consensu.org", and to host their code at those subdomains. Multiple CMPs competing for publisher's approved vendors and "consent business" allows faster time-to-market for solutions, better feature customizability to publisher's needs, and allows large publishers to write and host their own standards-compliant custom solutions if they want.

- CMPs host JavaScript code at their delegated subdomain which implements a transparency and consent UX and a standardised CMP JavaScript API, and manages the approved vendor and consent cookies and other standardized formats.

- A publisher's approved vendors and a user's consent choices are stored in browser cookies. Global vendor consents are stored in a global third-party cookie. Publisher's approved vendors, purposes and consents (and per-site vendor consents, if so configured) are stored in first-party cookies, under the domain of that publisher.

- The industry entity would establish standards that all CMPs must follow for UX, the JS API, data storage formats, and behaviours.

- Publishers would load a CMP of their choosing on their site. Publishers, DSPs, and SSPs query the JS API for approved vendors, purposes and consent values. Depending on approved vendors, purposes and consents, tracking cookies can be set, or other information can be gathered. Purposes and consent values for all vendors are passed to subsystems by parties that can read the information.

2. What types of transparency and consent does the Framework support?

Support will be dependent on the individual CMPs and what they choose to offer as part of their solution. Any options would adhere to the agreed industry standard, so that all parties can communicate standardised status.

The standard supports global- (web-wide), service- (site-wide), and group-wide transparency and consent. Each option has its own data storage format so approved vendors, purposes and consent can be understood. They are defined as follows:

- Global: Preferred vendors are chosen by a publisher, disclosures are made about those vendors and consent is requested and granted by the consumer (where necessary) to perform the requested processing purposes (such as the setting and reading of cookies by that entity) across the internet.
- Service: Preferred vendors are chosen by a publisher, disclosures are made about those vendors and consent is requested and granted by the consumer (where necessary) to perform the requested processing purposes (such as for the setting and reading of a cookie by that entity) on the service (website or app) where the disclosures were made and consent (where necessary) is given.
- Group: Preferred vendors are chosen by a publisher, disclosures are made about those vendors and consent is requested and granted by the consumer (where necessary) to perform the requested processing purposes (such as the setting and reading of cookies by that entity) across a group of sites.

3. Does this solution support per-company consent? Per-purpose? Per-company AND per-purpose?

This solution supports all per-purpose and per-vendor, but due to concerns of payload size and negatively impacting the consumer experience, a per-vendor AND per-purpose option is not available. Options are being discussed and a per-vendor, per-purpose option is being discussed and will likely be handled through an ads.txt-type solution.

Vendors (SSPs, DSPs) get a single consent value with possible values of:

- No Consent (0)
- Consent (1)

4. Does the solution work in cookie-less browsers?

The issue of cookie-less browsers and browsers that block third-party cookies via default settings (Safari) is a separate issue from the immediate European regulatory compliance need. As an industry, we will have to deal with this issue, regardless of ePrivacy and GDPR. This can be addressed as a separate work stream as a fast follow-on to the immediate work towards a solution for browsers where we are currently able to set third-party cookies.

5. What are the preferred vendor, purposes and consent storage requirements for the Framework?

Storage of preferred vendor, purpose and user consent is distributed and maintained in the browser via a third-party cookie (or first party cookie), with a maximum expected size of approximately 700 bytes. Unlike the registry solution, this does not require a central, expensive storage solution.

6. How are preferred vendors, purposes and user consent per vendor communicated by the Framework?

Each CMP will be responsible for providing preferred vendors, purposes and consent state to each vendor or SSP on a given site. This will be done with a call to one or more of the

standardised JS API functions. Each vendor or SSP will need to update their own code to use the API to check preferred vendors, purposes and consent when their system receives a call.

For SSPs, they will need to do additional work to propagate this information for multiple vendors up the chain to ad networks and exchanges to determine which ads can be served. See IMPLEMENTATION section below for more details.

7. Can we provide this solution without needing vendors to change their tags?

This cannot be easily done and is not part of the specification. However individual CMPs can come up with a mechanism to add the necessary cookie value to all the tags on the page. The vendors will still need to make modifications on their servers to read and interpret the cookie value and take appropriate action to not set, set, update, or delete their third-party cookies. As policy dictates, vendors will need to agree to certain policies in order to be included on the vendor list. It is up to the vendor to take the appropriate action based on the data signal, not the publisher or CMP.

8. How does the audit trail work?

Each company (DSP, SSP, vendor, publisher) will log consent data received in the ad and vendor tag calls. The industry should adopt a standard for what consent parameters must be logged (e.g. timestamp, url where consent was obtained, CMP by which consent was obtained)

9. Does the Transparency & Consent Framework allow one party to know whether another party has been approved by a publisher and has obtained consent (where necessary)?

Yes - through APIs provided by the Consent Manager, or through the “DaisyBit” data structure passed through the Ad calls, anyone can determine whether a vendor is an approved vendor of a publisher and its consent status. Publishers’ approvals and consents will be stored in a first-party cookie and will only be available to that publisher unless they choose to pass it to other vendors via cookies, parameters, or other means.

The global consent cookie, being stored in the.mgr.consensu.org domain can be read by Consent Managers that are approved to have a subdomain under “.mgr.consensu.org”. Consent Managers are free to read and set cookie values through APIs of their own design. Nothing in this proposal indicates how exactly a consent manager should interact with the subdomain, the standard would simply be the format of the cookie.

10. Can the Framework communicate approved vendors, purposes and consent in server-to-server scenarios?

Yes - by passing the data through the server to server calls in the compressed data format used for these calls and the cookie.

11. Does the Framework require calls mid-ad call?

No. The SSP queries the CMP JS API for all vendor consent values, passes those values down the chain, waits for an ad to be returned, then returns that ad to the page. No additional calls within the chain are required. For vendors who have not been approved by a publisher and/or have not been given consent (due to site-wide consent restrictions or a user who has manually given consent for a subset of vendors), consent will be passed to them as "No Consent (0)."

12. Does lag time impact of the Framework for ad serving?

The most significant lag time would be in waiting for users to view transparency disclosures and provide consent, where necessary, when the UX needs to be shown (on first visit to publisher if publisher disclosures and consent is required, or occasionally if only global vendor consent is required). If the global vendor consent cookie has been set, ad serving can proceed.

The CMP JavaScript would most likely be cached, and if not, would be small (10-50k) and load quickly (<100-200ms typically). Vendor lists (<100k) would also need to be loaded once, but typically be cached. One asynchronous request of <700 bytes to retrieve the browser-side 3rd-party consent cookie (<10ms typically) is the only uncacheable request. A more advanced implementation with third-party cacheable JavaScript in an iframe and interframe communication could be implemented to eliminate this uncacheable request. All these requests are non-blocking until ad or DSP code requests consent values. After that, all API requests to get consent data by the SSPs and DSPs are sub-millisecond, as the code to lookup consent is a simple in-memory lookup.

13. Does this solution add meaningful data cost? LOE/cost to establish and maintain?

No. Concerns with the approach related to the size of the cookie containing approved vendors, purposes and consent values for each vendor have been resolved via a compression scheme that would result in a maximum cookie size of ~700 bytes, and much smaller (~20 bytes) for the likely common cases of "all consents given" and "no consents given". Vendor lists are highly-cacheable static content typically <100k. CMPs would be responsible for hosting highly-cacheable, mostly-static JavaScript content (likely 10-50k) and associated cookie-getting/setting APIs.

13. Are there single points of failure with this solution?

Yes, but all are low-risk and mitigatable:

- Central DNS server must be up and serving addresses for the common domain and CMPs' subdomains, but DNS is notably reliable and risks can be mitigated through proper use of redundant DNS servers and long TTLs (time-to-live) values.
- Central domain vulnerable to ad blockers. Working with major ad-blocker add-on providers to not be placed on blacklists under the justification that this code does not show ads but collects legally-required consent might be a mitigation, but would be dependent on ad-blockers' policies and authors' opinions. In cases where only the third-party cookie is dropped but CMP code is loadable, consent managers could fall back to first-party cookies (and re-request consent from consumers). Detection of CMP ad-blocking in-tag could load CMP code from a different location, but it wouldn't be able to set the global cookie, and could be subject to further blocking of the new location in the ad-blocker.

- Third-party cookie loss or blocking can occur but this is present in all proposed solutions, as a cookie is needed to store consent preferences or a linking ID (for registry).
- Successful retrieval of the hosted vendor lists is a requirement for a CMP to present the (per-vendor drilldown) UI, and to properly set the global vendor cookie. Risks can be mitigated with proper use of caching content delivery networks, and by providing mirrors of these lists at CMP-specific DNS names, or other public locations, as well.

14. How will vendors know if they need to wait for consent state before firing cookie?

CMP will need to return a message of “you do not need consent for this user” since the CMP will be detecting user IP, not the vendors and vendors globally will need to know if they need consent or not.

15. Is the solution vulnerable to cookie clearing?

Yes. Preferred vendor, purposes and consent preferences are stored in a cookie, and disclosures will need to be re-made and consent will need to be re-obtained if cookies are cleared. Alternative storage methods could be developed in future.

16. How many bits per vendor are intended to be stored in the third-party cookie?

In addition to approved purposes, current thinking is to only have one bit per approved vendor. It is either 0 (no consent) or 1 (consent). All parties that read the bit only need to know whether consent given or not (if required).

17. Does the Transparency & Consent Framework work in mobile apps?

The current solution works for web-based apps, but not native apps. An SDK is being discussed and is required as an add-on to this solution and will be made available to app builders by individual CMPs.

USER EXPERIENCE AND THE FRAMEWORK

1. What might the user experience look like?

- UI created by the publisher explaining the vendors used, the purposes for which they are using data, if they need consent or not and options to accept or reject
- Standard minimum language, customisable within parameters (legal) by publishers
- Yes / No buttons
- Access to a level that allows management by purposes.
    - User could toggle on/off consent for all vendors for a given purpose, if consent needed by vendors
- Access to a level (à la carte) that allows management by vendor.
    - Page generated from master vendor list that would display all vendors selected by a publisher.
    - May display toggles next to each vendor name, the vendor's use of data purpose, link to privacy policy, etc.
    - May provider the option to click a select all button to select/deselect all vendors and apply consent or individually turn on/off consent.
- How the publisher handles the user experience after they get status from the CMP is up to the publisher within the confines of the regulation.

2. What UX requirements are there relating to transparency, consent update, and change/revocation?

The user will need to be informed that the change is applicable only for current browser/device and that it may take some time to replicate across consent management solutions

3. Will the Framework slow down the user experience?

The solution works using asynchronous calls. The one instance of a perceived user slowdown might be if the user has not given consent and sees the consent request modal (popup) asking to provide disclosures and requesting consent. It will take time for them to read, understand and respond, but calls are happening in the background waiting for the disclosures to be made and consent to be set so that cookies can be set, scripts run and ads served.

4. Does the Framework rely on first- or third-party cookies and what are the impacts or potential risks?

One possible implementation is the use of both third-party cookies and first-party cookies for publisher and service-specific consents but other storage mechanisms may be used as well. Third-party cookie loss or blocking can occur, but this is present in all proposed solutions, as a cookie is needed to store consent preferences or a linking ID (for registry).

5. Is it possible to use a first-party cookie instead of a third-party cookie with this solution?

- This solution will not work in exactly the same way without the use of a third-party cookie, but it will still function.

- First-party cookies would not enable the reading/writing of cookies by anyone not on the domain where the cookie is stored (domain1t.com cannot read/write a cookie on domain2n.com without domain or subdomain delegation and it's unlikely a publisher would delegate DNS for 2K+ vendors). Using a first-party cookie results in a solution that is service-specific only.

- For browsers that block third-party cookies by default, the solution will set a first-party cookie and treat it as a service-specific consent cookie.

- The issue of cookie-less browsers and browsers that block third-party cookies via default settings (Safari), is a separate issue from the immediate GDPR compliance need. As an industry, we will have to deal with this issue, regardless of GDPR. This can be addressed as a separate stream as a fast follow to the immediate work towards a GDPR transparency and consent solution.

6. What happens if a user does not give consent for the data processing required for ads to be served (if required by a vendor)? Would this mean that no ads are shown or can a public service announcement be shown?

This would be up to the publisher to determine in conjunction with their SSP. The framework focuses on transparency, and the collection and propagation of consent, not the resulting consumer experience.

IMPLEMENTATION

1. What is required of CMPs to integrate with the solution?

- Implement a JS API based on the industry standard that can be used by publishers, SSPs and other vendors
- Develop a consumer-facing transparency and consent collection UX per industry standards and guidelines
- Host said services on sub-domain delegated by central entity

2. What is required of SSPs to integrate with the solution?

Update their tag to query for preferred vendors, purposes and consent and propagate that information down to the vendors through the bid requests via OpenRTB. Set or update their cookies, depending on the data received.

3. What is required of DSPs / vendors to integrate with the solution?

Update their own proprietary code to query for whether they are allowed on a publisher's page as a vendor or to process the vendors' users' personal data and consent status. Set, update or delete their cookies and personal data collected depending on the signal and act accordingly per the GDPR requirements.

Vendors will also be required to maintain an audit trail by logging all unique user consent signals provided, the date consent was obtained and the URL of the site consent was obtained on.

4. What is required of Publishers to integrate with the solution?

- Integrate with their CMP of choice. Will vary by CMP, but likely to involve installing JavaScript tags and functions to call the CMP JS API.
- Determine their preferred vendors.
- Determine user experience desired after user choices made are received from CMP and send user to appropriate experience.

5. What is required of ad networks and ad exchanges to integrate with the solution?

This depends on how they are integrated with a publisher's page. If they get the approved vendor, purpose and consent information from an SSP (or any other entities), Ad networks and exchanges and RTB participants will need to decode the information and act accordingly.

If their tag is placed on the page making a request, then they too can access the CMP JS API just like the SSP or DSP.