pubvendors.json v1.0: Transparency & Consent Framework **IAB Europe | IAB Tech Lab**

Draft for Public Comment | May 2018

Table of Contents

Introduction

In February 2017, the IAB Europe assembled parties representing both the supply and demand sides of the digital advertising 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 sub-groups within the GIG was tasked with developing guidance on consent as a legal basis for processing personal data. Out of that effort, an additional working group was formed to develop a technical solution to the challenge of obtaining and disseminating consumer consent to the various parties relying on it as a legal basis of processing personal data.

This specification "pubvendors.json" is a draft for public comment. Please submit your general feedback to feedback@advertisingconsent.eu and any technical feedback to transparencyframework@iabtechlab.com by June 1, 2018.

About the Transparency & Consent Framework

The scope of the technical working group?s initiative increased to include a technical industry solution to allow website operators to:

1. Control the vendors they wish to allow to access their users? browsers (for setting and reading cookies) 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 and CMP List (commonly referred to as the List)
- The technical specification for capturing, storing and retrieving user consent in the context of digital advertising
- Policy underlying the:
    - Disclosures to be made by vendors included on the List
    - Use of the List and the reference architecture

About the Transparency & Consent Standard

Resources including policy FAQ, Global Vendor List Registration, and CMP registration can be found at advertisingconsent.eu.

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

Disclaimer

THE STANDARDS, THE SPECIFICATIONS, THE MEASUREMENT GUIDELINES, AND ANY OTHER MATERIALS OR SERVICES PROVIDED TO OR USED BY YOU HEREUNDER (THE "PRODUCTS AND SERVICES") ARE PROVIDED ?AS IS? AND ?AS AVAILABLE,? AND IAB TECHNOLOGY LABORATORY, INC. (?TECH LAB?) MAKES NO WARRANTY WITH RESPECT TO THE SAME AND HEREBY DISCLAIMS ANY AND ALL EXPRESS, IMPLIED, OR STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AVAILABILITY, ERROR-FREE OR UNINTERRUPTED OPERATION, AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE. TO THE EXTENT THAT TECH LAB MAY NOT AS A MATTER OF APPLICABLE LAW DISCLAIM ANY IMPLIED WARRANTY, THE SCOPE AND DURATION OF SUCH WARRANTY WILL BE THE MINIMUM PERMITTED UNDER SUCH LAW. THE PRODUCTS AND SERVICES DO NOT CONSTITUTE BUSINESS OR LEGAL ADVICE. TECH LAB DOES NOT WARRANT THAT THE PRODUCTS AND SERVICES PROVIDED TO OR USED BY YOU HEREUNDER SHALL CAUSE YOU AND/OR YOUR PRODUCTS OR SERVICES TO BE IN COMPLIANCE WITH ANY APPLICABLE LAWS, REGULATIONS, OR SELF-REGULATORY FRAMEWORKS, AND YOU ARE SOLELY RESPONSIBLE FOR COMPLIANCE WITH THE SAME.

About IAB Tech Lab

The IAB Technology Laboratory (?Tech Lab?) is a non-profit research and development consortium that produces and provides standards, software, and services to drive growth of an effective and sustainable global digital media ecosystem. Comprised of digital publishers and ad technology firms, as well as marketers, agencies, and other companies with interests in the interactive marketing arena, IAB Tech Lab aims to enable brand and media growth via a transparent, safe, effective supply chain, simpler and more consistent measurement, and better advertising experiences for consumers, with a focus on mobile and ?TV?/digital video channel enablement. The IAB Tech Lab portfolio includes the DigiTrust real-time standardized identity service designed to improve the digital experience for consumers, publishers, advertisers, and third-party platforms. Board members include AppNexus, ExtremeReach, Google, GroupM, Hearst Digital Media, Integral Ad Science, Index Exchange, LinkedIn, MediaMath, Microsoft, Moat, Pandora, PubMatic, Quantcast, Telaria, The Trade Desk, and Yahoo! Japan. Established in 2014, the IAB Tech Lab is headquartered in New York City with an office in San Francisco and representation in Seattle and London.

Learn more about IAB Tech Lab here: https://www.iabtechlab.com/

About IAB Europe

IAB Europe is the voice of digital business and the leading European-level industry association for the interactive advertising ecosystem. Its mission is to promote the development of this innovative sector by shaping the regulatory environment, investing in research and education, and developing and facilitating the uptake of business standards.

Learn more about IAB Europe here: https://www.iabeurope.eu/

Pubvendors.json Overview

High level goals

The high level goals of "pubvendors.json" supports the following:

1. Provide a standard for publishers to publicly declare the vendors that they are working with and their permissions/configuration
2. Allow vendors to verify publisher GDPR settings and verify andaudit CMP consent string
3. Provide a standard way for publishers to whitelist vendors
4. Enable publishers to limit purposes on a per vendor basis
5. Enable publishers to limit features on a per vendor basis

Publishers concerns about IAB?s GDPR Transparency & Consent Framework version 1.1

As understood by IAB Europe Transparency and Consent Steering Group and IAB Tech Lab GDPR Commit Group, the following are the core publisher concerns:

Liability

Transparency and consent may not be seen as valid when many vendors and purposes are indiscriminately surfaced without regard for limiting purposes per vendor

- Indiscriminate rights for vendors:
    - Surfacing thousands of vendors with broad rights to use data w/out tailoring those rights may be too many vendors/permissions
    - Concern that even if a user consents to vendors or doesn?t opt out of a vendor?s processing and broad purposes where the vendor asks a user to, a user may not fully understand what it was told/consented to and publishers may be found to have not done a good enough job limiting the further use of that data for broader arguably more privacy-intrusive uses
    - Ideally, publishers would be able to pick a small subset of vendors to which they give broader rights ("tier 1") and then limit the rights of the rest of their vendors (?tier 2?) since publishers recognize that delivering ads to their users,either through direct online deals or programmatically, requires more vendors than those in ?tier 1?
    - Publishers recognize there is no technical way to limit the way data is used after the data is received by a vendor for decisioning/bidding on/after delivery of an ad but need a way to clearly signal the restriction for permitted uses in an auditable way
    - Thus, publishers need a way to differentiate between those 2 tiers of vendors in what they surface to a user and in what they signal to vendors on page and downstream and upstream through creatives and need to have an audit trail to show this
- Control of purpose and data use by vendor. Publishers and vendors need a signal to communicate to the vendors, purposes and legal bases that have been disclosed on a publisher?s site. Publishers control the disclosures to their users and therefore which vendors can lawfully process the data of users visiting their properties
    - For example vendor 1 has permission for purposes 1, 2 and 3 but vendor 2 only has permission for purpose 3 only
    - Example uses publishers may wish to control:
        - use of a user?s data processed through the delivery, or measurement, of an advertisement or the opportunity to deliver, or measure, of an advertisement to inform future personalisation for such user based on preferences or interests known or inferred from the data collected (inferences about a user can be aggregated across sites)

Disagreement over legal basis (LI vs. consent)

A publisher may disagree with a vendor?s legal analysis on which legal basis the vendor can rely upon for a defined purpose

- Publishers can?t dictate the legal basis on which a vendor (that?s a controller) relies (that?s a legal analysis that has to be made by each controller)
- But Publishers can, based on the legal bases disclosed by a vendor for each purpose (registered in the global vendor list), either choose not to work with that vendor or allow vendors which use one or other legal basis (LI or consent)

- Given technical feasibility of publishers signalling information about the disclosures they have made on behalf of a vendor, it is further possible for publishers to choose from several available legal bases that a vendor is willing to rely on. For example, a vendor may be willing to operate on the basis of either user consent if a publisher is willing to obtain it, or justify processing under a legitimate interest in cases where a publisher is not willing obtaining consent for a given vendor.

Legitimate Interest

Framework must support vendors relying on LI and support publishers that only want to work with vendors relying on LI

- Vendors can declare legal basis per purpose
- LI status per vendor per purpose needs to be communicated to vendors downstream,so vendors know who is relying on LI

Technical implementation

- Maintain current technical specification (daisybit which communicates user consent per purpose, where a vendor needs consent)
- Add an out-of-band signal ("pubvendors.json" file a publisher places on each site) that publishers use to signal the following to vendors:
    - Limitations that a publisher places on specific vendors by purpose.
    - Disclosures made by the publisher on behalf of the vendor, i.e. whether a publisher has disclosed a specific vendor as seeking consent or relying no a legitimate interest by purpose. This would also enable a publisher to signal that a specific purpose has not been disclosed on behalf of a vendor.

Users would be able to consent/approve specific purposes and specific vendors. Publishers may provide additional information to users, such as information that the publisher has imposed additional restrictions on certain vendors and their ability to collect data about a user on its site. The publisher may also provide information to the user about which additional limitations apply to each vendor (for example: Vendor 25 may not process data for Personalization, i.e. enhancing profiles, even though the user consented to that Purpose in general)

Vendors would crawl for "pubvendors.json" periodically. In future revisions the Daisybit will signal to vendors when a new ? pubvendors.json? is available and possibly the content as well.

Publisher integration

A publisher would place a file named "pubvendors.json" at the ".well-known path" of their domain at: ? http://publisher.com/.well-known/pubvendors.json? similar to ads.txt and robots.txt (https://tools.ietf.org/html/rfc5785). The publisher should use a CMP that supports ?pubvendors.json?.

"pubvendors.json" may HTTP redirect (3xx) up to 5 hops (http://www.ietf.org/rfc/rfc1945.txt), anything beyond this may be treated as if the file is not present.

CMP integration

The CMP should check use the "pubvendors.json" as the base ruleset for what vendors to show to end clients and how to display them. The CMP should first check for the existence of the ?pubvendors.json?, if found the CMP should use the rules defined for notification to the end user, otherwise global consent or CMP specific configuration can be assumed.

SSP/DSP integration

An SSP/DSP only needs to support version 1.0 of the spec if they are interested in supporting legitimate interest. The GDPR Consent String contains a more restrictive set of information and downstream parties are compliant if they follow approved vendor/purposes in the protocol.

If an SSP/DSP does want to support vendors relying on legitimate interest they can use "pubvendors.json" as an out of band solution to augment the Consent String. The vendor needs to build a system to crawl for the existence of the file building a database mapping between the publisher?s domain and rules/content within the file. If a publisher whitelists a vendor claiming legitimate interest then Legitimate Interest can take precedence over the information in the Consent String. The SSP/DSP should regularly sync the ?pubvendors.json? rules in order to stay up to date with publisher changes.

Pubvendors.json Version 1.0This is a simplified version of the original "pubvendors.json" spec targeted for use by May 25th. Version 1.0 primary purpose to to achieve the following:

1. Provide a standard way for publishers to declare a whitelist of vendors that they are working with.
2. Enabling vendors to rely on Legitimate Interest if the vendor is listed in the whitelist.
3. Work within the confines of the existing Version 1.1 of the IAB Europe Transparency and Consent Framework specifications without modifications.

Version 1.0 requires no changes to the Global Vendor List or Version 1.1of the IAB Europe Transparency and Consent Framework. Publishers will need to use a CMP that will support version 1.0 of the specification.

Filename and location

"http://publisher.com/.well-known/pubvendors.json"

Format

```
{
    "publisherVendorsVersion": 1,         // [Required] Version of the pubvendors.json specification
"version": 1,                          // [Required] Increment on each update of this file
    "globalVendorListVersion": 1,         // [Required] The version of the GVL this was created from
    "updatedAt": "2018-05-28T00:00:00Z",  // [Required] Updated for every modification
    "vendors": [                          // [Required] Whitelist vendors
        {
            "id": 1                       // [Required] ID of vendor
        },
        {
            "id": 2
        },
        {
            "id": 3
        }
    ]
}
```

Future directions: pubvendors.json Version 1.1

Going forward, and building on the foundations of pubvendors.json Version 1.0, the proposed updates would be made to the pubvendors.json specification, creating a pubvendors.json v1.1.

pubvendors.json Updates

- disableUpstreamVendors publishers can choose to not pull in additional vendors from the global vendor list. This would make the vendor list operate as a strict whitelist.

- vendors.purposes publishers can restrict purposes by vendors

```
{


  "publisherVendorsVersion": 1,         // [Required] Version of the pubvendors.json specification
  "version": 1,                         // [Required] Increment on each update
  "globalVendorListVersion": 1,         // [Required] The version of the GVL this was created from
  "updatedAt": "2018-05-28T00:00:00Z",  // [Required] Updated for every modification
  "disableUpstreamVendors": true,       // [Optional] dont pull additional vendors from the GVL
  "vendors": [                          // [Required] Whitelist vendors
      {
          "id": 1,                      // [Required] ID of vendor
          "purposes": [1, 2, 3],        // [Optional] Publishers can restrict purposes by vendor

      },
      {
          "id": 2
      },
      {
          "id": 3
      }
  ]


}
```

Global Vendor List updates

Expanded Purposes Controls

- vendors.purposes.id - The id of the purpose. This should reference the purposes id field
- vendors.purposes.legalBasis - The legal basis for which the vendor uses the purposes. This can either be "consent" or ?legitimateInterest?.
- vendors.purposes.required - An optional field that signals to external parties if a specific purpose is required for a vendor to operate.

```
"purposes": [

{

  "id": 1,                                  // [Required] ID of purpose
  "legalBasis": "consent|legitimateInterest", // [Required] legal basis for usage of purpose
  "required": boolean,                      // [Optional] Is this purpose a requirement for the vendor to operate

},

]
```

Change to Consent String protocol

The Consent String should be modified to pass the version of the pubvendors.json used when sending the request. The value 0 would indicate that pubvendors.json is not present. The file version can be used by downstream parties to determine if they have an up to date version of the file when processing requests.

FAQ Why does this spec not address the Consent String?

We could expand the consent string to support Legitimate Interest in the future. The idea behind "pubvendors.json" goes beyond the consent protocol, as a separate signal. We are simply suggesting starting with ?pubvendors.json? as a first step, to allow for continued adoption of the Consent String v1.1 specification before May 25th.

How do publishers create a list of their vendors?

The goal of pubvendors.json is to publicly identify direct data processing relationships between publishers and ad technology providers. As such publishers should identify all DSPs, SSPs and DMPs who they have an agreement with to process data. Additionally this should include any partners who you feel comfortable gaining consent on their behalf. This list should include: programmatic partners and any third-party data providers you utilize to help build audience segments. This may exclude downstream third parties who you do not feel comfortable authorizing consent as their legal basis for data collection of your users.

As needed, Additional guidance will be created by the IAB Tech Lab GDPR working group.

```
</div>
```

```
</div>
```

```
<script crossorigin="anonymous" integrity="sha512-xx5bFEpCTis78HDM45zXGUp0XjJNgfxVJuvXT7CCXCTv1JgICExLtsUhV7HO90M3gLO0j5DA0zkAmMrsLJsFUw==" type="application/javascript" src="https://github.githubassets.com/assets/frameworks-dcdc6bbaaa9ce93ccc296c33ff1f40c3.js"></script>

<script crossorigin="anonymous" async="async" integrity="sha512-OVom1EjMVGuAhxgj+IUZGLWX+Y2YCwA5HczPO5EkywA3LpBr+opzeA2g7YZmzT0TR0w94V9UGCvzNux1BO80gw==" type="application/javascript" src="https://github.githubassets.com/assets/github-ff2a16ee220770be00aef7ab3773f297.js"></script>
```