IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

FAQs on Vendor Device Storage & Operational Disclosures

Last update : January 2023.
This document is also available here.

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

General

What value does the JSON file provide?

The json file provides additional transparency to users and enhances interoperability between TCF participants. The first part (Disclosures Array) is intended for users' disclosures, and is used by Consent Management Platforms (CMP) to build UIs that allow users to access the list of client-side storages susceptible to be written and read on their devices, their purposes and associated duration. The second part (Domains Array) aims to support TCF participants' own technical and organisational measures at company level, to monitor and ensure compliance of their technical integrations with Vendor partners. It also supports the TCF Vendor Compliance programme whereby Vendors' live installations are regularly checked against the TCF Policy.

What is in scope of the JSON file?

The digital assets used in the context of the Vendor's TCF registration must be declared in the file. In addition Vendors can add assets unrelated to their TCF participation if they wish to provide additional transparency, such as digital assets that are used for non-TCF purposes, but this is not required.

Disclosures array

Can wildcards be used in the identifier field?

Yes. Wildcards are permitted (for example, "id*" or "*id" to describe multiple prefixed or suffixed identifiers) but not alone. Wildcards should not be used to group different categories of identifiers with different purpose(s) : Each category of identifiers must be recorded separately in the disclosures array.

How to manage first party storage?

If the client-side storage is linked to the publisher domain, then the vendor must add a wildcard ("*") as a value in the `domain(s)` field (spec). Otherwise, if the client-side storage is linked to the vendor domain, then the vendor has to put the domain as a value.

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

How should vendors declare that they do not use any client-side storage?

Vendors should leave the Disclosures array empty in such cases.

Why is it better to use the “domains” field rather than the “domain” field?

The type of `domain` field is a string, and therefore only allows for one domain to be declared. Because client-side storage is often associated with multiple domains, the `domains` field, whose type is an array, allows for multiple domains to be declared and avoids having to create several records for the same client-side storage in the `disclosures` array.

How can you declare multiple subdomains associated with client-side storage?

Wildcards ‘*’ are permitted to allow any vendor to declare multiple subdomains. For example, declaring "*.vendor.com" means that the client-side storage is used across multiple subdomains of vendor.com.

Domains array

Does the field ‘use’ allow free text or should it contain specific strings?

There are no specified requirements on the explanatory text contained in the “use” field - free text can be used. It is recommended to use English for widest readability. Note scope of the field is optional.

What if the vendor only uses a single endpoint client-side?

Only this endpoint should be declared in the `domains` array.

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

What if the vendor does not operate on its own domain and rely on partners' domains for their data processing operations?

Vendors must declare all domains used for collecting and processing personal data in the context of their TCF registration (as a data controller), including domains they do not own or operate themselves.

How to use the examples provided in the Technical Specification?

The examples in the specification represent sections of the JSON file for illustration only and have been annotated (e.g. they can contain "..." to remove certain sections that are not relevant in the scenario being explained). They should not be copied and pasted by vendors to create their own JSON file. JSON files that have been created in such a manner will return an error after being submitted at registration and will not be published on the GVL.

Serving the JSON resource

Do any restrictions apply when naming the JSON file?

No. There is no requirement on the path or filename of the JSON resource.

Is adding ".json" as a filename extension enough to identify a JSON file?

No. In addition to the filename extension, which must be .json, the content of the file has to be in JSON format, and the response header `content-type` must be `application/json` to properly indicate the type of the resource..

What should be done to enable Cross-Origin Resource Sharing (CORS)?

To allow CMPs to request and load the JSON client side, the vendor must enable Cross-Origin Resource Sharing (CORS). When accessing the JSON resource, the server should return a `Access-Control-Allow-Origin` header with `Access-Control-Allow-Origin: *`. This can be verified when loading the JSON resource from a browser by selecting the inspect option to ensure the appropriate header is included in the response. Alternatively, the following command can be used with a terminal : `curl -H "Origin: example.com" -v`

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

"https://vendor.com/file.json" (changing "https://vendor.com/file.json" with the path to your JSON resource) and verify the Access-Control-Allow-Origin.

How to make sure that the JSON file is accessible from different browsers?

To make sure that any visitor gets access to the JSON file, it's important to test it from different browsers (also testing from latest browser versions can be helpful). The IAB Europe compliance team uses a crawler with many different user agents for running the tests. For example, as a vendor, you could get a notification like this one if we find an issue related to Safari browser "*Url not accessible: The format of value 'Version/15.6,2 Safari/605.1.15' is invalid*". Of course, if you have any questions, you can write or reply to framework@iabeurope.eu.

How to get the list of all the tests done by the IAB Europe compliance team and the methods to fix a JSON file?

Currently, several tests are applied to every JSON file which means different issues can be found and at the end, a vendor can receive different notifications. As this list evolves over the time and to better help the vendors to understand the issues, the IAB Europe compliance team gathers every test, every definition and the methods to fix them in this public file.

Validation of the JSON resource

How to verify that the JSON file conforms to the content and structure of the technical specifications?

When you update your TCF registration and add the path to the JSON file, the IAB Europe compliance team will notify you if there is an error, so that you can update the file prior to its publication on the Global Vendor List.

Does IAB Europe provide a validator publicly accessible by any vendor to check a JSON file anytime?

Yes. The JSON validator checks the JSON file according to the tests done by the IAB Europe compliance team. Every issue is displayed in order to help the vendor to fix the JSON file until approved. You can use it here.

IAB Europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium
iabeurope.eu

Why have you received a suspension notification?

You have received the suspension notification for one of or both of the reasons detailed below as per the TCF notification here from March 14, 2022 :

1. You have not provided the additional B2B information that can be used by publishers for determining which vendors they wish to establish transparency and consent for on their digital properties
2. You have not provided a secure URL to a JSON resource containing disclosures related to purpose-specific storage and access information and web domains used by your company for collecting and processing personal data in the context of your implementation of the TCF.

If you receive a suspension notification then please check your registration here and ensure that all mandatory fields that relate to the requirements described above are completed.

If you fail to update the required fields then notifications will be sent every 7 days, reverting to daily for the last 5 working days prior to the suspension deadline.

Who should you contact if you are unable to complete the requested fields in the registration?

If you have any questions, you can write to framework@iabeurope.eu.