FAQs on Vendor Device Storage & Operational Disclosures

Last update: June 2026

General

Where can I find the Vendor Device & Storage Disclosure specification?

The technical specification is available in the IAB Europe GitHub repository at the location referenced in the TCF documentation.

What value does the JSON file provide?

The JSON file enhances transparency and interoperability across TCF participants.

It contains three main components:

- **Disclosures Array**
  Intended to support user-facing transparency. It is used by Consent Management Platforms (CMPs) to build UIs that allow users to view client-side storage (e.g. cookies or similar technologies) that may be written to or read from their devices, including their purposes and associated duration.

- **Domains Array (if applicable)**
  Supports vendors' technical and organisational compliance measures. It enables monitoring of technical integrations with partners and supports the TCF Vendor Compliance Programme, where vendors' live implementations are regularly reviewed against TCF Policies.

- **SDKs Array (if applicable)**
  Identifies SDKs or embedded technologies used in mobile in-app environments to support compliance review and audits.

What is in the scope of the JSON file?

All digital assets used in connection with the vendor's TCF registration must be declared.

Vendors may also voluntarily declare additional assets unrelated to their TCF participation (e.g., assets used for non-TCF purposes) to provide greater transparency. This is optional.

Disclosures array

Can wildcards be used in the identifier field?

Yes. Wildcards (e.g. "id*" or "*id") are permitted to describe multiple prefixed or suffixed identifiers.

However:

- Wildcards must not be used alone.
- Wildcards must not group identifiers that relate to different purposes.
- Each category of identifier associated with different purpose(s) must be declared separately in the disclosures array.

How should first-party storage be declared?

- If the client-side storage is linked to the **publisher domain**, the vendor must include "*" in the domains field.

- If the client-side storage is linked to the **vendor domain**, the vendor must explicitly declare that domain.

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

If no client-side storage is used, the **Disclosures array must be empty**.

Why should vendors use the domains field rather than the domain field?

The domain field (string type) allows only a single domain.

Because client-side storage is often associated with multiple domains, the domains field (array type) allows multiple domains to be declared without creating multiple duplicate records in the disclosures array.

The field domain may be removed in a future release to only use the field domains.

The use of domains is therefore recommended.

How should multiple subdomains be declared?

Wildcards are permitted.

For example:

"*.vendor.com"

indicates that the client-side storage is used across multiple subdomains of vendor.com.

How to declare non-TCF cookies?

Vendors may use client-side storage for non-TCF purposes. If a vendor uses cookies not linked to any TCF purpose, they may voluntarily declare them in their JSON file to provide greater transparency. When doing so, the purposes field must be an empty array (`"purposes": []`), and the description field must be populated to explain the cookie's function. You can find an example below.

```JSON
{
  "disclosures": [
    {
      "identifier": "cookie_name_example",
      "type": "cookie",
      "maxAgeSeconds": 2592000,
      "cookieRefresh": false,
      "purposes": [],
      "domains": ["adtech123.com"],
      "description": "Cookie used to ...",
    }
  ],
  "domains": [...]
}
```

How to declare opt-out cookies?

Opt-out cookies are a specific type of non-TCF storage used to register a user's decision to opt out of any tracking. When declaring an opt-out cookie, the purposes field must be an empty array (`"purposes": []`), the description field must be populated, and the specific `optOut` boolean flag must be set to `true`. You can find an example below.

```JSON
{
  "disclosures": [
    {
      "identifier": "optOut",
      "type": "cookie",
      "maxAgeSeconds": 63072000,
      "cookieRefresh": true,
      "purposes": [],
      "domains": ["adtech123.com/optout"],
      "description": "Cookie used to mark the user as opted out.",
      "optOut": true
    }
  ],
  "domains": [...]
}
```

Domains array

Vendors operating in the web environment must declare all domains used for collecting and processing personal data in the context of their TCF registration. Vendors must not include publishers' delegated domains or subdomains. For vendors operating in the web environment but using no domains, an empty array must be included. For Vendors that do not operate in the web environment, the array may be omitted.

Does the *use* field allow free text?

Yes. There are no strict formatting requirements for the use field.

- Free text is permitted.
- English is recommended for broader readability.
- This field is optional.

What if the vendor only uses a single endpoint?

Only that endpoint should be declared in the Domains array.

What if the vendor relies on third-party domains?

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

When must the Domains array be included?

- Vendors operating in **WEB environments** must declare the domains used.
- If no domains are used, an empty array must be included.
- If the vendor does not operate in WEB environments, the domains array may be omitted.

How should the examples in the Technical Specification be used?

The examples in the specification are illustrative only.

They:

- May contain annotations (e.g. "...")
- May omit sections not relevant to the example scenario

They must **not** be copied and pasted directly into a vendor's JSON file.

JSON files created in this way will fail validation during registration and will not be published on the Global Vendor List (GVL).

SDKs Array

Vendors operating in mobile app environments must publish and declare the SDKs used for collecting and processing personal data. This array identifies embedded technologies and supports compliance audits by helping to isolate specific technical components (for example, identifying whether an issue originates from a third-party technology provider rather than the registered vendor). For Vendors operating in mobile app environments that do not use SDKs, an empty array must be included. For Vendors that do not operate in mobile app environments, the array may be omitted.

What is the SDKs array used for?

The SDKs array identifies technologies or SDKs embedded in mobile applications.

It supports compliance audits by helping to identify specific technical components involved in a vendor's implementation. For example, an issue may originate from a third-party technology provider rather than the registered vendor itself.

When must the SDKs array be included?

- Vendors operating in **mobile in-app environments** must declare the SDKs used.
- If no SDKs are used, an empty array must be included.
- If the vendor does not operate in mobile in-app environments, the SDKs array may be omitted.

Serving the JSON Resource

Are there restrictions on the file name or path?

No. There are no specific requirements regarding the path or filename of the JSON resource.

Is using the *.json* file extension sufficient?

No.

In addition to using the *.json* extension:

- The file content must be valid JSON.
- The server must return the header:
  Content-Type: application/json

What are the CORS requirements?

To allow CMPs to access the JSON file client-side, vendors must enable Cross-Origin Resource Sharing (CORS).

The server must return:

Access-Control-Allow-Origin: *

This can be verified:

- In the browser's developer tools (Inspect → Network tab)
- Or using curl:
  curl -H "Origin: example.com" -v https://vendor.com/file.json

  Replace the URL with the actual path to your JSON resource and verify that the *Access-Control-Allow-Origin* header is present.

How can vendors ensure cross-browser accessibility?

Vendors should test access to the JSON file across multiple browsers and browser versions.

The IAB Europe compliance team uses automated crawlers with various user agents. In some cases, vendors may receive notifications referencing specific user agents (e.g. Safari).

If you receive such a notification, review server configuration and access controls.

For questions, contact: framework@iabeurope.eu

Validation of the JSON Resource

How can vendors verify that the JSON file conforms to the specification?

A publicly accessible validator is available to check compliance against the validation tests applied by the IAB Europe compliance team. All detected issues are displayed to help vendors resolve errors prior to approval.

https://iabeurope.eu/vendorjson

Suspension Notifications

Why have you received a suspension warning?

You will receive a suspension notification if you are found to be in breach of one of the three Enforcement Procedures set out in the TCF Controls Catalogue. These include:

- **Tampering with TC Strings** by CMPs or Vendors' live installations (procedure n°1)
- **Other material breaches of the TCF Policies** by CMPs or Vendors' live installations (procedure n°2)
- **Incomplete or inaccurate information** required for inclusion in the Global Vendor List (GVL) (procedure n°3)

The availability and conformance of the device storage and operational disclosures JSON file is covered by procedure n°3.

What should you do if you receive a suspension warning?

If you receive a suspension warning about the availability and/or conformance of your device storage and operational disclosure JSON file,, you will be given 5 business days to remedy the issues.

You should review the issues found by the compliance team and modify your JSON file accordingly. It is recommended to use the Vendor JSON validation tool here to verify the conformance of your file.

If, following the expiration of the delay, the issues have not been resolved, you will receive a suspension notice via email and will be suspended from the GVL until the issues have been remedied:

1. Review your TCF registration and ensure that all mandatory fields are complete and accurate.
2. Review your TCF implementation to confirm that you are not in breach of any Enforcement Procedure listed in the Controls Catalogue.
3. Implement the necessary corrective actions within the timeframe specified for the relevant procedure.

A suspended Vendor may request reinstatement once all identified issues have been fully addressed and compliance has been restored.

Who should be contacted for support?

For any questions or assistance, contact: framework@iabeurope.eu.