iab. europe

Transparency
and Consent
Framework

IAB EUROPE
TCF COMPLIANCE
REPORT

iabeurope.eu

Contents

Contents

1. Introduction: What is the TCF?

Launched in 2017, the **Transparency & Consent Framework** or **TCF,** is an accountability tool that relies on standardisation to facilitate compliance with certain provisions of the GDPR[1] and ePrivacy Directive[2]. It applies principles and requirements derived from these two legislative instruments to the specific context of the digital industry, taking account of relevant EU-level guidance from the European Data Protection Board (EDPB) and national-level guidance from Data Protection Authorities.

The TCF is intended for use by three categories of stakeholders (irrespective of whether they are members of IAB Europe as a trade association – any such stakeholders are welcome to use the TCF):

1. **Publishers**: owners or operators of online content or services where personal data is collected and used by third-party companies (vendors) for digital advertising, audience measurement, or content personalisation. Many such Publishers are ad-supported content creators or service providers;
2. **Vendors**: third-party companies that do not ordinarily have direct access to end-users of Publishers. Vendors can be Ad servers, measurement providers, advertising agencies, demand-side platforms (DSPs), supply-side platforms (SSPs), and more;
3. **CMPs** (i.e. Consent Management Platforms): software or solution providers that develop notices (e.g. cookie banners) to inform users and capture their preferences with respect to the processing of their personal data.

1.1. How Does the TCF Work?

(i) Standardisation of the information that should be provided to users about Vendors

Vendors that register with the TCF must provide and maintain detailed information that, as a minimum, should also be disclosed to users to meet their transparency requirements under the GDPR. This includes their identity, the link to their privacy policies, the duration of the cookies they may rely on, whether they use non-cookie methods for accessing users' devices (e.g. mobile identifiers), the data processing purposes they pursue and associated legal bases, retention periods and categories of data collected and processed.

---

[1] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications),OJ L 201, 31.7.2002, p. 37–47, as amended by Directive 2009/136/EC.

TCF seeks to incorporate all commonly pursued purposes and categories of data processed in the online space through harmonised terminologies. Vendors should map the processing activities they already carry out and types of data they already collect or process to these standard terminologies when they register.

Once a Vendor is registered, all the information will be included in the "Global Vendor List" (GVL), a publicly available and machine-readable registry hosted by IAB Europe, and the Vendor must maintain this by providing updates. The GVL serves as a central and up-to-date information repository available to Publishers and their CMP when they select Vendors they work with and then disclose information and provide choices to users about the third-party vendors they selected.

This is further complemented by dedicated minimum practical requirements for user interfaces that stem from guidelines of Data Protection Authorities and case law. The practical requirements for user interfaces aim to align with the "layered approach" recommended by the EDPB and define specific requirements for the first layer of the CMP UI (the "cookie banner") and the secondary layers of the CMP UI (the subsequent pages of the UIs).

## (ii)   Standardisation of how users' choices should be captured

The TCF standard sets out an open-source binary format for CMPs to capture users' choices in the form of a "TC String". This common format enables CMPs to record users' choices in an auditable, machine-readable string of characters (1 for yes, and 0 for no) representing users' privacy preferences.

(iii)   Standardisation of how users' choices should be communicated and respected

The TCF provides mechanisms for Publishers and their CMPs to communicate users' choices to vendors. For websites, for example, the TCF includes a specification for CMPs to develop their own proprietary APIs that rely on the same naming conventions so that Vendors can access users' privacy choices in real-time. Similar naming conventions can be used in mobile applications. This enables Vendors to use the same code to retrieve TC Strings or part of TC Strings across multiple websites/apps that use the TCF - rather than develop different code for each website/app.

Again, this is further complemented with minimum practical requirements for technical operations performed by Vendors to ensure users' choices are respected - such as not setting any cookie when users have refused or withdrawn consent or not forwarding any personal data to another Vendor that failed to establish a legal basis for its processing.

(iv) Schema of user choices' flow using the TCF in the digital ecosystem
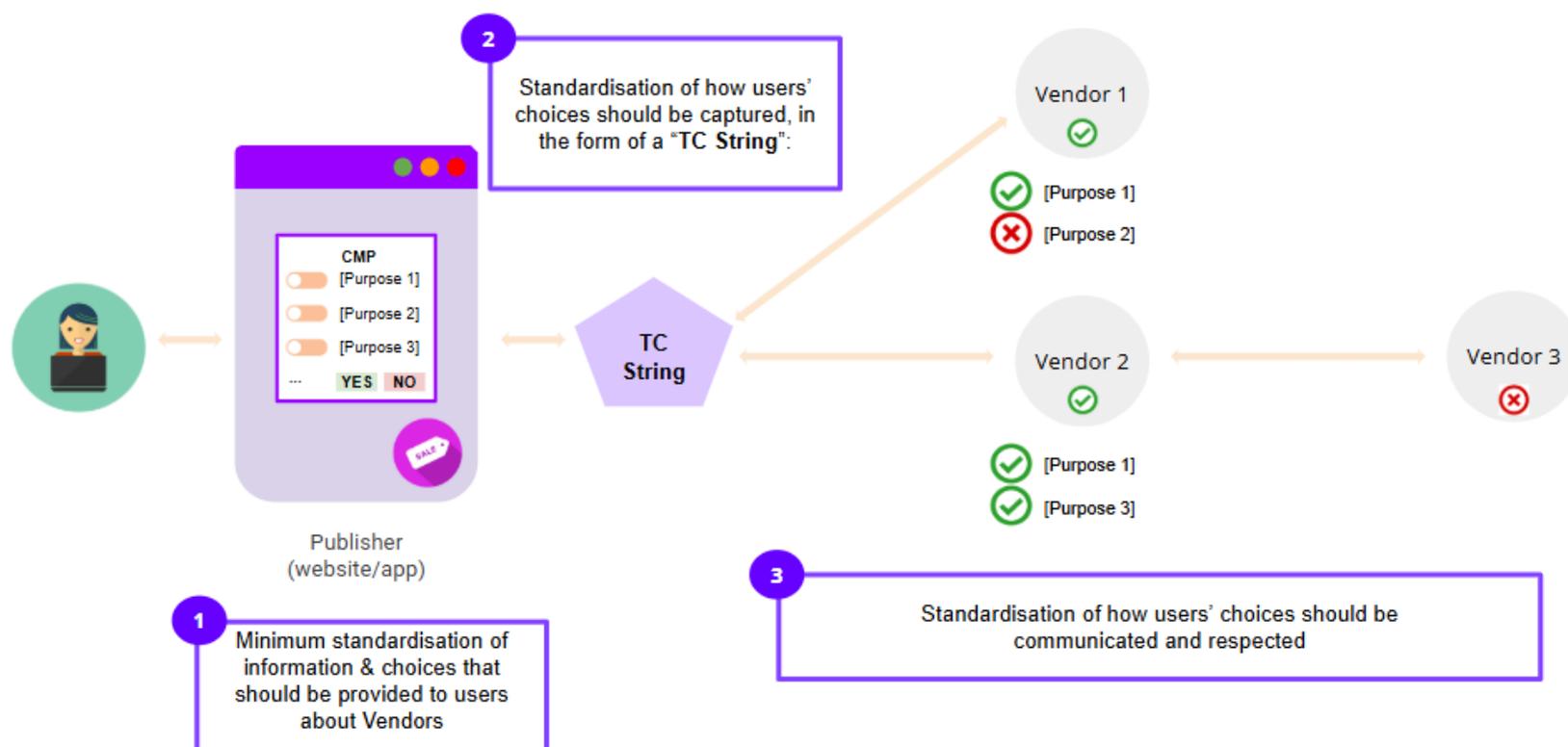
1.2. How is the TCF Adopted by Companies in the Digital Industry?

By December 31, 2025, TCF registrations increased to a **total of 953 Vendors** and **181 CMPs**: **154 new Vendors** and **19 new CMPs** registered throughout the year. When compared to the year-end 2024 figures of 885 Vendors and 177 CMPs, the framework experienced a **7.7% increase in Vendor** participation and a **2.3% rise in CMP** registrations.

Metric	2024 Total	2025 Total	Change (%)
Registered Vendors	885	953	**+7.7%**
Registered CMPs	177	181	**+2.3%**

(i) Vendors' adoption of the TCF

Vendors that register to the TCF map the processing activities they already carry out to the TCF purposes taxonomy, a menu of commonly pursued purposes in the online space expressed in a harmonised terminology:

Purpose	Description
1. Store and/or access information on a device	Purpose 1 is meant to signal whether the condition for lawful storing and/or accessing information on a user's device is met, where this is required. It is not a purpose for personal data processing in itself, unlike all other Purposes. Purpose 1 corresponds to the obligation of Article 5(3) of the ePrivacy Directive. While Purpose 1 is not a data processing purpose, it is technically treated the same way for signalling purposes. Any personal data stored and/or accessed via Purpose 1 still requires another Purpose to actually be processed.

Purpose	Description
2. Use limited data to select advertising	Purpose 2 corresponds to the use of real-time information about the context in which an ad will be shown, including information about the content and the device, such as the device type and capabilities, user agent, URL, IP address and non-precise geolocation data. It also corresponds to the use of real-time information to control the frequency and sequence or order of ads shown to a user. Real-time information about the context can also be used to prevent an ad from serving in an unsuitable editorial context.
3. Create profiles for personalised advertising	Purpose 3 corresponds to the association of the data collected with a new or existing ads profile based on user interests or personal characteristics. It includes the combination with information previously collected, subject to the latter having been collected with an appropriate legal basis.
4. Use profiles to select personalised advertising	Purpose 4 corresponds to the use of ads profile or other historical user data to enable or prevent an ad from serving. It includes the selection of ad based on retargeting criteria and/or personalised ad profile.
5. Create profiles to personalise content	Purpose 5 corresponds to the association of the data collected with a new or existing content profile based on user interests or personal characteristics.

Purpose	Description
	It includes the combination with information previously collected, subject to the latter having been collected with an appropriate legal basis. **"Content" refers to non-advertising content.**
6. Use profiles to select personalised content	Purpose 6 corresponds to the use of content profile or other historical user data to enable or prevent a content from serving. **"Content" refers to non-advertising content.**
7. Measure advertising performance	Purpose 7 corresponds to the measurement of ad performance, such as suitability and safety of the context where the ad was served, viewability rates, user engagement with the ad and nature of that engagement (click, tap, hover, scroll), ad attribution, conversions and sales lift.
8. Measure content performance	Purpose 8 corresponds to the Measurement of content performance, such as user engagement with the content, number of unique users the content was served to, user referrals. **"Content" refers to non-advertising content.**
9. Understand audiences through statistics or combinations of data from different sources	Purpose 9 corresponds to establishing aggregate reports about audiences reached by ads or content through panel-based and similarly derived insights, to be provided to publishers and/or advertisers (in the form of aggregate reports).

Purpose	Description
10. Develop and improve services	Purpose 10 corresponds to the use of information to improve existing products with new features, or to develop new products. It includes the creation of new models and algorithms through machine learning.
11. Use limited data to select content	Purpose 11 corresponds to the use of real-time information about the context in which the content will be shown, including information about the content and the device, such as the device type and capabilities, user agent, URL, IP address and non-precise geolocation data. It also corresponds to the use of real-time information to control the frequency and sequence the order of content shown to a user. **"Content" refers to non-advertising content.**

In 2025, TCF Vendors have declared the following Purposes:
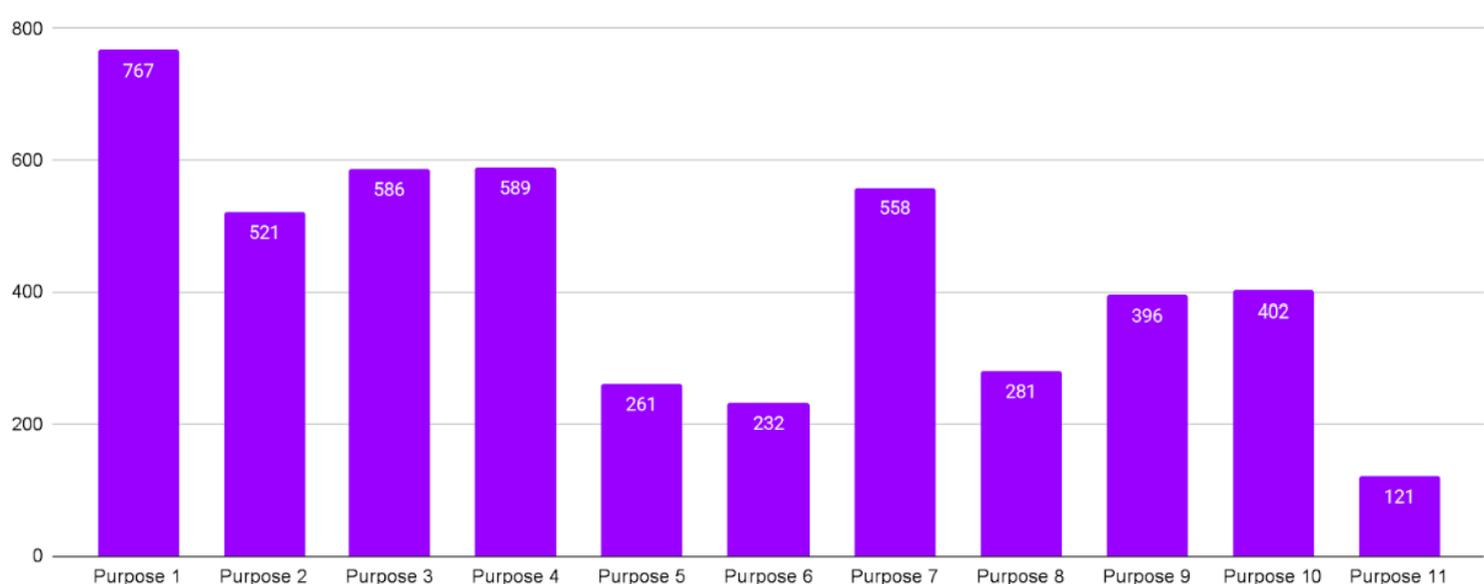
180 **Vendors have not declared any advertising relating purposes (purposes 2, 3, 4, or 7**), which indicates that they operate in industries other than digital advertising (e.g. audience measurement, fraud prevention). This represents **19%** of Vendors participating in the TCF.

(ii) CMPs' adoption of the TCF

Although the **majority (59%) of registered CMPs are commercial providers**, 41% of registered CMPs are considered private, meaning they are owned and operated by a Publisher for its own digital properties.

In connection with the technical environments supported by CMPs, a wide majority of registered companies have been certified solely for web - however the number of CMPs supporting either mobile (native app) or CTV (native app), or both has been steadily growing.
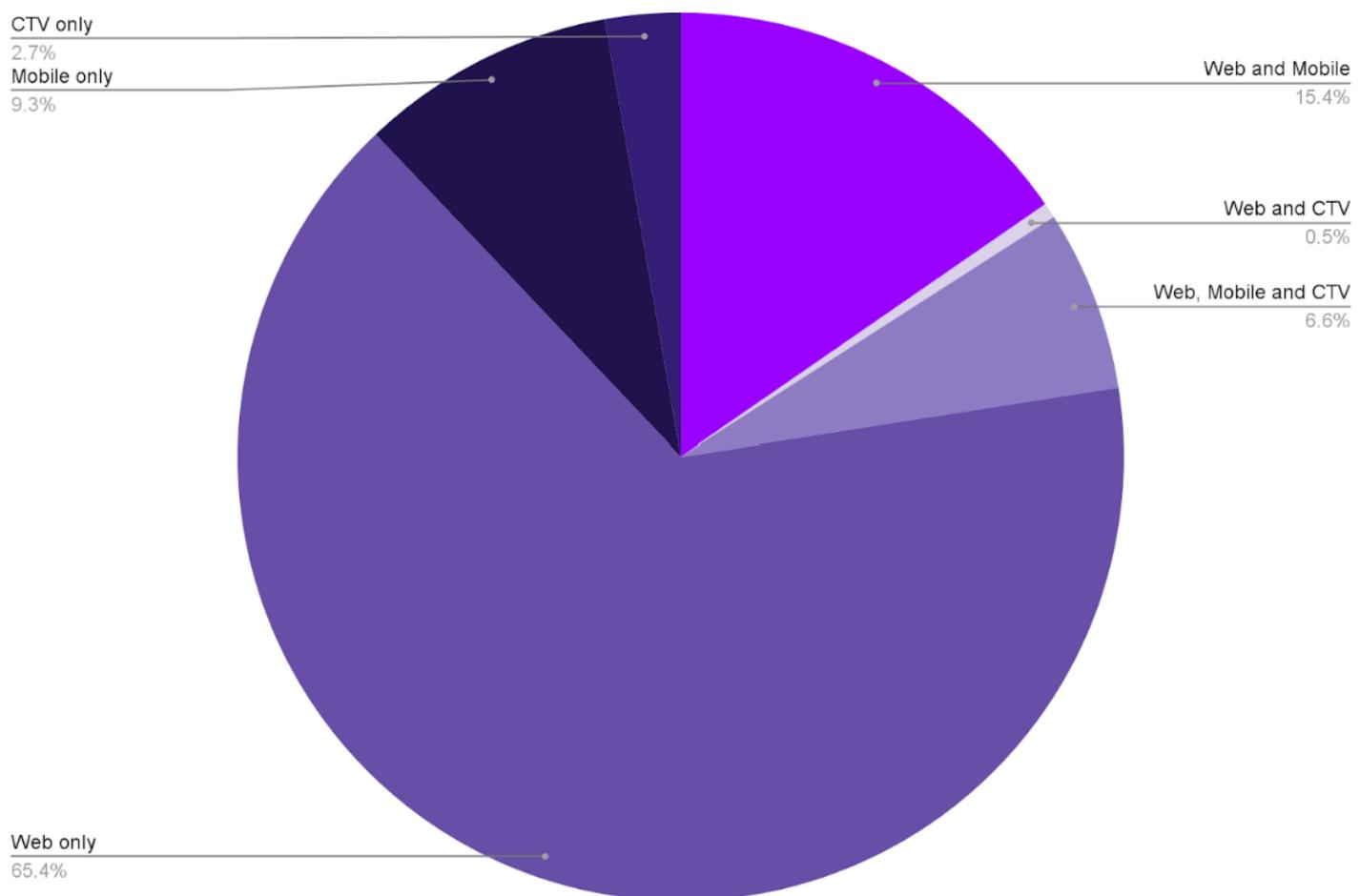
While the Web environment remains dominant, there is a clear trend toward **Cross-Environment** support.

- **Web Only:** Decreased slightly from **66.7%** in 2024 to **65.4%** in 2025.
- **Web, Mobile, and CTV:** This category grew from **4.8%** to **6.6%**.
- **Mobile Only:** Increased from **8.6%** to **9.3%**

2. The TCF Compliance Programme

IAB Europe has been operating Compliance programmes for CMPs and Vendors in order to protect the integrity of the TCF and ensure that organisations that have signed up to the TCF comply with their commitments under the TCF Policies.

Although the responsibility for the correct implementation of the TCF, and ultimately compliance with the EU's data protection framework (i.e. the General Data Protection Regulation (GDPR) and the ePrivacy Directive), lies with the businesses that are subject to it, IAB Europe provides support and develops dedicated procedures to make sure the TCF is implemented properly. As the managing organisation of the TCF, IAB Europe also imposes penalties in line with its prerogatives under the TCF Terms and Conditions to contractually sanction non-compliance. Such penalties are explained in detail under Sections 3 (for CMPs) and 4 (for Vendors) of this report.

Concomitant to the launch of TCF 2.2, the TCF Compliance Programmes have been expanded and reinforced to identify and enforce against instances of non-compliant CMP and Vendor implementations, which reduce user protection and expose TCF participants to serious legal risks.

2.1. 2025 Key Numbers

(i) CMPs

19 new CMPs have been audited and certified, and 10 already registered CMPs were audited and certified for a different technical environment.

51 enforcement procedures have been carried out following proactive monitoring of CMPs' live installations by the TCF Compliance team and/or following reports of non-compliance received from end-users or TCF participants. All enforcement issues were resolved without suspension except for one; however, after complying once again with the TCF Policies, the CMP has been reinstated.

Compared to 2024, **enforcement procedures** rose from 40 to 51, signifying a **27.5% increase**. This increase was a result of the TCF Compliance team performing more auditing across multiple digital properties compared to the years before. As for suspensions, **2024** saw **zero suspensions**, while **2025** saw **one temporary suspension**.

(ii) Vendors

180 Vendors' compliance forms were reviewed and evaluated to verify compliance with the TCF Policies and Technical Specifications.

587 enforcement procedures have been carried out following proactive monitoring of Vendors' registrations and live installations by the TCF Compliance team and/or following reports of non-compliance received from end-users or TCF participants. 41 Vendors were temporarily suspended from the TCF until they resolved their non-compliance issues.

Compared to 2024, Vendor **enforcement** activity increased significantly, with **procedures more than doubling** from 269 to 587. At the same time, **temporary suspensions grew by 78.3%**, rising from 23 to 41 instances over the same period. This increase was due to the TCF Compliance Team starting to perform additional verifications over Vendors' compliance in comparison with 2024, in order to detect inconsistencies in their implementations relating to the duration of their cookies and purposes for which they are used.

Category	Metric	2024	2025	Change (%)
CMPs	Enforcement Procedures	40	51	**+27.5%**
	Suspensions	0	1	N/A
Vendors	Enforcement Procedures	269	587	**+118.2%**
	Suspensions	23	41	**+78.3%**

2.2. TCF Compliance Resources and Tools

This section will showcase the various resources and tools made available to TCF participants to verify their compliance with the TCF.

(i) Controls Catalogue

The *Controls Catalogue* maps requirements of the Policies to auditable elements to help participants in assessing and reviewing the compliance of their practical implementations. It includes the audit checks IAB Europe performs when auditing TCF participants - and corresponding enforcement process for each.

The Controls Catalogue is regularly updated to align with the latest version of the TCF Policies. It was last updated in April 2025 in order to extend Enforcement Procedure n°3 for Vendors that have not appropriately completed their Vendor Compliance Questionnaires. Currently, Vendors are given 5 business days to remedy the issues: following the expiration of the delay, if the issues have not been resolved, the Vendor will receive a suspension notice via email and will be suspended from the GVL until the issues have been remedied.

(ii) CMP Validator

The **CMP Validator** is a Chrome extension developed by IAB Europe that helps CMPs and Publishers check their compliance with the TCF. It can also be used by Vendors to check the compliance of their Publisher-partners, and by end-users who want to verify their preferences with respect to the processing of their personal data were saved faithfully.

The Validator runs certain checks automatically, such as verifying that all CMP API required commands return a correct response, whereas other checks need to be completed manually by the user (for items where user interaction is required).

Since May 2023 the CMP Validator is publicly available for download in the Chrome Web Store here.

(iii) Device Storage & Operational Disclosures Validator

The **Device Storage & Operational Disclosures Validator** is a client-side tool for Vendors to self-test adherence of their deviceStorageDisclosureUrl to the technical specifications.

The TCF registration process requires Vendors to provide a secure URL to a JSON resource that conforms to a specific structure and contains two types of information: disclosures relating to their device storage access and corresponding duration (the Disclosures array and its attributes), as well as the web domains the Vendor uses (the Domains array and its attributes).

Vendors can verify that their URL conforms to the requirements using the Validator here prior to submitting it at registration level.

(iv) Additional Vendor Information List

The **Additional Vendor Information List** is a machine-readable file that provides extra details on TCF-registeredVendors.

This information is not intended for user disclosures but can help Publishers decide for which Vendors they wish to establish transparency and consent for on their digital properties. The list includes various details, such as:

- Full Legal Entity Address;
- B2B Contact Details;
- Territorial Scope (countries where the Vendor operates);
- Jurisdictions List;
- Environments (e.g., Web, Mobile, CTV);
- Type of Services (SSP, DSP, Verification, Ad Serving, Header Bidding, etc.);
- International Data Transfers outside the European Union (EU) or European Economic Area (EEA).

Publishers can use this resource to identify which Vendors are relevant for their own use cases. For example, it allows them to avoid requesting user consent for Vendors operating in technical environments or jurisdictions they do not support. It also helps them better understand each TCF Vendor's scope of operations, including whether or not they transfer data outside the EEA.

(v) Non-compliance report form

Through the *TCF Non-Compliance Form*, both end-users and TCF participants can report concerns about any TCF CMP or Vendor that may have failed to respect user choices or comply with TCF Policies.

Publishers can also use this tool to flag issues with Vendors that might put them at risk of non-compliance.

3. TCF CMP Compliance

The CMP Compliance programme comprises a pre-implementation validation stage and a post-implementation enforcement stage – whereby IAB Europe monitors live CMP implementations for compliance with the TCF Policies. The CMP enforcement process can result in the suspension of the participating CMP from the Framework for non-resolved breaches of TCF Policies, as it will be later shown with more detail.

3.1. Pre-Implementation Validation

After TCF registration, CMPs need to complete a validation process before they can be attributed, a CMP ID and added to the CMP List. In order to complete validation, CMPs are required to provide a URL on which it is possible to test their installation: this includes verifying the User Interfaces and the technical functioning of the CMPs for each environment (web, mobile or CTV). Validation is not a guarantee of legal compliance, but it helps establish that the CMP's User Interface and functionality seem to be in line with the TCF Policies.

In the course of 2025, **19 new CMPs have been validated and published**. Moreover, **10 already registered CMPs were validated for a different environment**.

3.2. Monitoring of Live Installations

IAB Europe regularly monitors CMPs' live installations and also investigates reports of non-compliance from end-users or TCF participants.

There are two procedures, depending on the type of breach committed by the CMP. **Procedure n°1** applies when a CMP live installation is found to be tampering with TC Strings, which represents a more serious infringement; **Procedure n°2** applies when a CMP live installation is found in breach of the TCF Policies.

Procedure n°1: Tampering of TC Strings
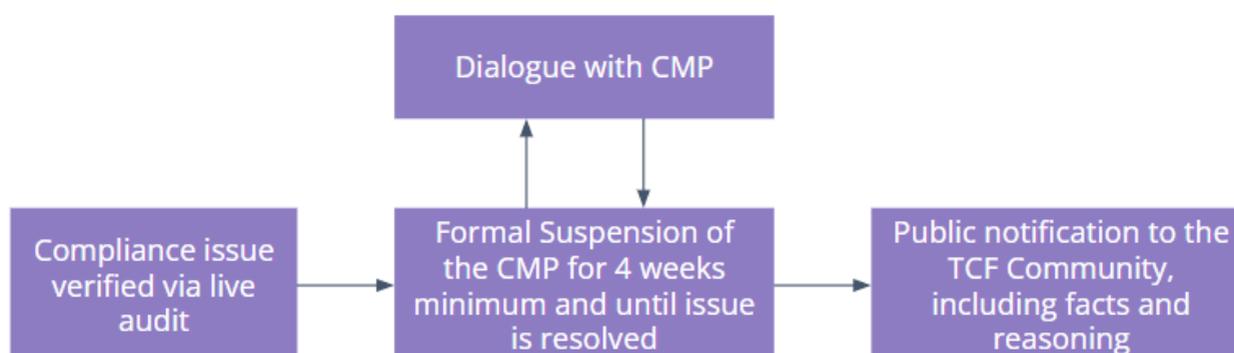
If this is the fourth time within a twelve-month period that the CMP has been found in breach of the provision targeted by Procedure n°1, it will be permanently suspended from the TCF. Throughout the course of 2025, **no Enforcement Procedure n°1** was initiated against CMPs, since all the relevant audits showed appropriate recording of users' privacy choices in the TC Strings.

Procedure n°2: Other material breach of the TCF Policies
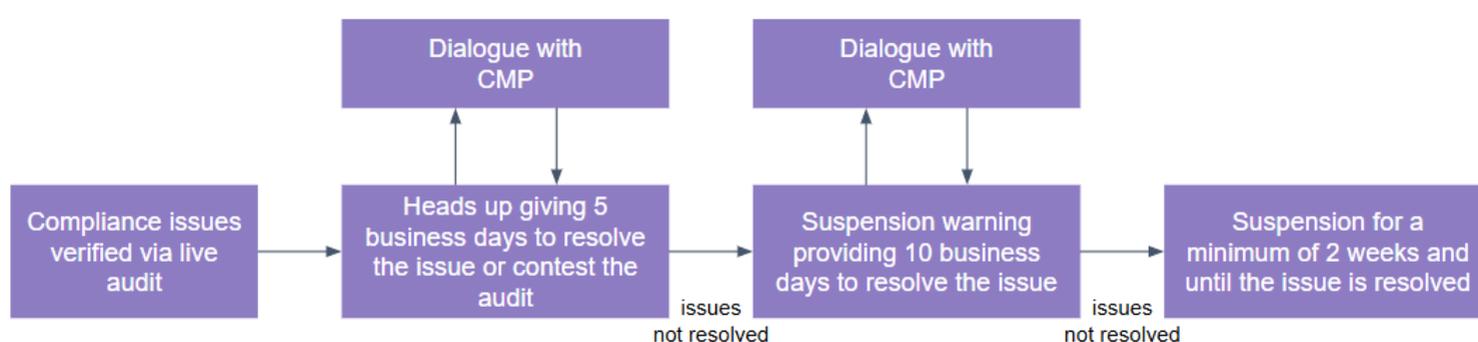
If this is the fourth time within a twelve-month period that the CMP has been found in breach of any of the provisions targeted by Procedure n°2, it will be notified via email and suspended from the GVL with immediate effect for a minimum of <u>2 weeks</u> and until all issues are resolved.

From 1st January 2025 to 31st December 2025, **36 enforcement procedures n°2 have been carried out against CMPs**. All enforcement issues were resolved without suspension except for one; however, after complying once again with the TCF Policies, the CMP has been reinstated.

3.3. Key Findings

During audit procedures, the most commonly identified issues were as follows:

❖ **Technical Checks:**

➢ '*Is the current or penultimate version of the GVL being used?* (Technical Check n°7): This check fails if the version of the GVL being used is not the current or penultimate version of the GVL. Among all the Technical Checks, this one had the highest failure rate, occurring in approximately **14% of the audits** performed.

➢ '*Are all vendor signals for deleted vendors set to 0?*' (Technical Check n°2): This check fails if there are any positive vendor consent or LI signals for vendors that are marked as deleted in the version of the GVL being used. This is the second most frequent Technical Check issue, occurring in **6% of the audits** performed.

❖ **Policy Checks:**

➢ *'Does the secondary layer of the UI disclose the storage and access information relating to the CMP's recording of signals, including the maximum device storage duration where applicable? CMPs should at a minimum disclose on the secondary layer of their UIs how the TC String is stored and for how long if it is stored on the user's device.'* Among all Policy Checks, this one had the highest failure rate, occurring **in 80% of the audits** performed. In these cases, CMPs failed to provide such information to the users.

➢ *'Is the user able to withdraw their consent as easily as they were able to give consent?'* (Policy Check n°32): This Policy Check failed **in 53% of the audits** performed, making it the second most commonly failed Policy Check. In the majority of cases, a 'Reject All' button (or similar) was missing when the user resurfaced the banner to withdraw previously given consent. The user needed to click on two (or more) calls-to-action to effectively withdraw their consent, making it less easy than it was to give consent.

➢ *'Does the 1st layer of the UI inform the user that they can withdraw their consent at any time and how to do so?'* (Policy Check n°9). This Policy Check failed **in 44% of the audits** performed, making it the third most frequent Policy Check-related issue. In most cases, CMPs' UIs only referred to the possibility for the user to change their preferences at any time, failing to explicitly explain to them the possibility to withdraw their consent later and how to do this.

Two issues improved between 2024 and 2025:
- **GVL Version Issues (Tech Check n°7):** the failure rate dropped from **20%** in 2024 to **14%** in 2025.
- **Consent Withdrawal (Policy Check n°9):** the failure to inform users how to withdraw consent dropped from **50%** to **44%**.

3.4. Non-Compliance Reports

Through the TCF Non-Compliance Form, end-users or TCF participants can submit information about any TCF CMP that they suspect may not have respected their choices or may not comply with the TCF Policies. IAB Europe does not disclose any identity information, such as the name or company name of the complainant, to the TCF CMP targeted by the non-compliance report.

There were 15 enforcement procedures initiated following reports of non-compliance in 2025. They were primarily targeted at CMPs failing to provide users with sufficient details on Vendors, such as their data retention periods and categories of data collected, or CMPs failing to provide information on how to withdraw consent. All issues reported were promptly checked by the Compliance Team, and the CMPs subsequently implemented the required changes without suspension.

4. TCF Vendor Compliance

The Vendor Compliance programme comprises a pre-implementation validation stage and a post-implementation enforcement stage - whereby IAB Europe monitors live Vendor implementations for compliance with the TCF Policies. The Vendor enforcement process can result in the suspension of the participating Vendor from the Framework for non-resolved breaches of the TCF Policies.

4.1. Pre-Implementation Validation & Verification of Vendors' Registrations

(i) Assessment of Vendors' Compliance Forms

After registration, Vendors need to complete a Vendor Compliance Form before they can be added to the GVL. This includes questions about how they intend to implement the TCF and the measures they put in place to ensure compliance with the Policies.

Because the requirement to complete a Compliance Form was introduced with TCF v2.2, the TCF Compliance Team also monitored that existing Vendors had submitted their Compliance   Form   in   time.

IAB Europe randomly selects fifteen Vendors per month to review and evaluate the answers provided in their Vendor Compliance Form. Vendors are asked to clarify their responses and submit further evidence of their compliance when the TCF Compliance Team considers the information provided is incomplete or inaccurate.

180 Vendor Compliance Forms have been reviewed from January 2025 to December 2025. During audit procedures, the most commonly identified issues were as follows:

1. Certain Vendors did not provide a non-exhaustive list of digital properties where their technologies are susceptible to be deployed (e.g. websites where their tags or pixels are present, mobile or CTV apps where their SDK is integrated - depending on the environment(s) they support). This requirement was implemented to facilitate the auditing by the TCF Compliance team of Vendors' live installations deployed on Publishers' properties.
2. Certain Vendors failed to provide the location of the attestation of their compliance with the TCF Policies that must be made public in their Privacy Policy.
3. Certain Vendors failed to provide accurate information on the mechanisms they have in place to confirm that a TC String originates from a CMP participating in the TCF, notably by verifying the corresponding CMP ID.

(ii) Vendors' Registrations verifications

IAB Europe uses an automated crawler to conduct a weekly review of all TCF registered vendors to identify any issues related to the URLs they provide at registration, ensuring that the information they provide remains accurate and compliant.

• Verification of the availability of the Device Storage Disclosure URL and its conformance with the TCF Technical Specifications
• Verification of the availability and language of the Privacy Policy and Legitimate Interest at Stake URLs

Procedure n°3 (Vendors' information required for inclusion in the GVL is incomplete or inaccurate) applies against Vendors that fail to provide available URLs or URLs that do not conform to their declarations. In April 2025, this Enforcement Procedure was also extended to Vendors that have not appropriately completed their Vendor Compliance Questionnaires.
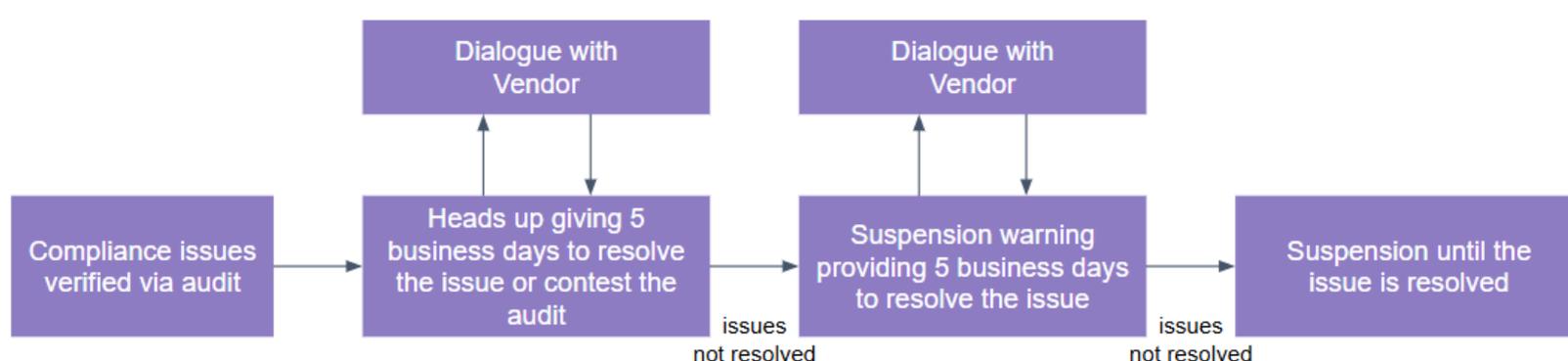
If this is the fourth time within a twelve-month period that the Vendor has been found in breach of the provisions targeted by Procedure n°3, it will be notified via email and suspended from the GVL with immediate effect for a minimum of 1 week and until all issues are resolved.

From 1st January 2025 to 31st December 2025, all Vendors have been audited weekly:

• **155 enforcement procedures n°3** have been carried out for incorrect Device Storage URLs - which led to **19 temporary suspensions**.
• **332** vendors have been audited due to mismatched information between their registration details and their device storage disclosures which led to **12 temporary suspensions**.
• **85 enforcement procedures n°3** have been carried out for incorrect Privacy Policy URLs - which led to **10 temporary suspensions**.

4.2. Monitoring of Live Installations

IAB Europe regularly monitors Vendors' live installations and also investigates reports of non-compliance from end-users or TCF participants.

There are two procedures, depending on the type of breach committed by the CMP. **Procedure n°1** applies when a Vendor's live installation is found to be tampering with TC Strings, which represents a more serious infringement; **Procedure n°2** applies when a Vendor's live installation is found in breach of the TCF Policies.
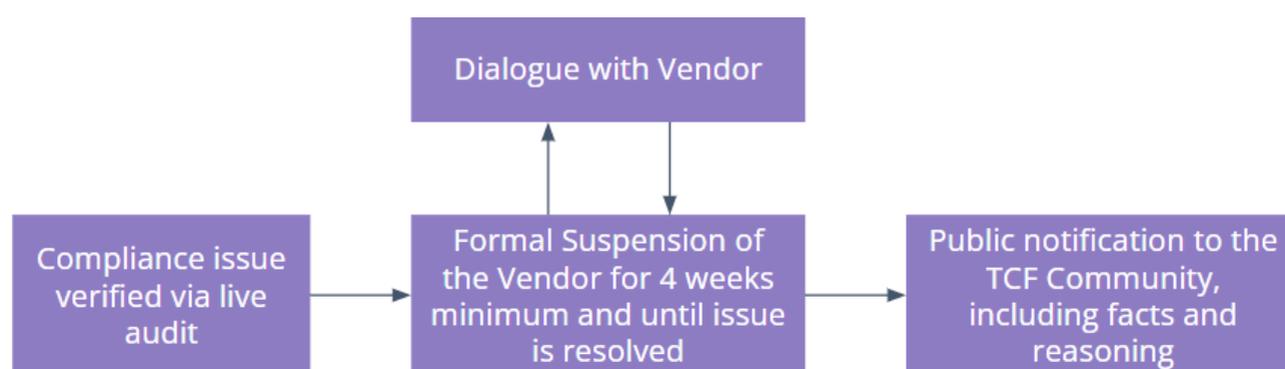
If this is the fourth time within a twelve-month period that the Vendor has been found in breach of the provision targeted by Procedure n°1, it will be permanently suspended from the TCF.

Procedure n°2: Other material breach of the TCF Policies
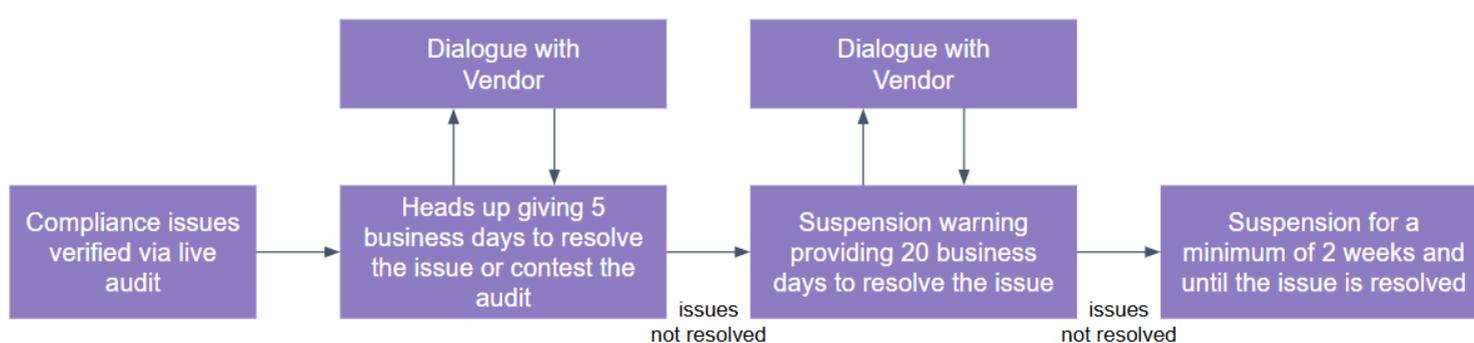
If this is the fourth time within a twelve-month period that the Vendor has been found in breach of any of the provisions targeted by Procedure n°2, it will be notified via email and suspended from the GVL with immediate effect for a minimum of 2 weeks and until all issues are resolved.

The issues that are commonly resolved during these procedures are:
- The setting of non-strictly necessary cookie prior user's consent
- Failure to use the addEventListener command of the TCF API in order to retrieve the TC String in real-time
- The setting of cookies whose duration was longer than what the Vendor has declared

4.3. Non-Compliance Reports

Through the TCF Non-Compliance Form, end-users or TCF participants can submit information about any TCF Vendor that they suspect may not have respected their choices or may not comply with the TCF Policies.

IAB Europe does not disclose any identity information, such as the name or company name of the complainant to the TCF Vendor targeted by the non-compliance report.

There were 15 enforcement procedures initiated following reports of non-compliance in 2025. They were primarily targeted at Vendors setting cookies in the absence of users' consent or using domains that were not appropriately declared. All the issues reported were promptly checked by the Compliance Team, and the Vendors subsequently implemented the required changes without suspension.

5. TCF Compliance Helpdesk

The TCF Compliance team regularly receives questions from TCF participants or companies interested in joining the TCF. All queries received are always answered to ensure implementers receive the support they need.

In 2025, IAB Europe received around **120 TCF Compliance questions**, a majority relating to the introduction of TCF 2.3, released on 19th June 2025, which made the previously optional *disclosedVendors segment* mandatory in order to resolve the ambiguity around the representation of LI in the TC string. This enhancement ensures that Vendors can always determine whether they were disclosed in the CMP UI.

The TCF Compliance team also develops and maintains supporting resources to help TCF participants in their implementation of the TCF. All resources are **accessible online**.

6. 2026 Outlook

To establish the TCF as an efficient self-regulatory standard, the TCF Compliance team will continue to scale up and automate the auditing of participating companies and corresponding enforcement procedures in 2026. This will include:

(i) **Expansion of the Device Storage Disclosure** specifications to increase end-user transparency and enhance cross-environment monitoring capabilities. Under the new specifications, Vendors are now permitted to declare cookies and other storage mechanisms used for Special Purposes, as well as those used in pursuit of non-TCF purposes (such as global opt-out). Additionally, Vendors must now declare their SDK package identifiers to support the creation of an accurate repository for monitoring, aligning with the deployment of the new auditing tool for in-app compliance. The **validator** has already been updated for Vendor to self-check their files, and as of the deadline of 31 May 2026 IAB Europe's custom crawler will verify conformance with these new declarations.

(ii) **Active monitoring of the transition to TCF v2.3** to ensure full ecosystem compliance after the February 28 deadline. To support this migration, a new version of the CMP validator was deployed together with an update of IAB Europe's auditing tools to verify the inclusion of the now mandatory *disclosedVendors* segment within the TC String.

(iii) **Finalisation of the new auditing tool for verifying the compliance of Participants' live installations within the mobile app environment**. Complementing the custom crawler currently utilised by the TCF Compliance team for the web environment, the ongoing finalisation and upcoming deployment of this dedicated tool for native apps will significantly streamline and scale the audit capabilities for non-web environments.

(iv) **Further automation of the enforcement processes** in order to increase the team's monthly threshold of companies selected for auditing. IAB Europe will launch a new Request for Proposal to appoint a contractor responsible for developing additional functionalities to the proprietary application used by the TCF Compliance Team to manage TCF participants' registrations. Building on the existing infrastructure, the selected contractor will develop new components designed to increase automation in key areas, including the completion of audits, the preparation of non-compliance notifications to TCF participants, and the tracking of enforcement phases and their associated deadlines.

Transparency and Consent Framework

Contact:
tcf.compliance@iabeurope.eu

iab europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium

𝕏 @iabeurope

in /iab-europe

iabeurope.eu