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

Dated: 14 May 2020

Subject: **Updated CMP enforcement process - TCF v2.0, May 2020**

Background

In 2019, the Managing Organisation (MO) identified the need to develop a process to assess CMP compliance with the Transparency & Consent Framework (TCF) v1.1. This process was implemented through the launch of a validation tool (Validator), under which 134 CMPs were certified, complemented by a resource-intensive enforcement programme to ensure market compliance.

With the roll-out of TCF v2.0, the MO has identified the need to strengthen the enforcement process by improving its effectiveness and associated deterrence mechanisms. This follows the observation of certain non-compliant CMP UI implementations, mere weeks after completing the TCF v2.0 validation procedures.

Non-compliant CMP implementations undermine the reputation of the TCF and expose participating organisations to serious legal risks. As the only visible point of contact with the user and authorities, CMPs have a responsibility and obligation under TCF policies to ensure that the market implements compliant versions of the UI.

New measures

To protect the Framework and ensure its success for the whole industry CMPs are expected to control the deployment of compliant versions of their software. All live installations must be compliant.

We are therefore updating the compliance measures. Currently warning of suspension are issued by the MO when one or more infringements of the TCF policies are found on one or more sites, followed by suspension if issues are not resolved in 14 days. However, there is no limit to the number of suspension warnings. This creates the risk of investment of scarce resources in repeated enforcement cycles that may or may not “definitively” solve the problem.

Going forward CMPs will be **immediately suspended** from the TCF for a minimum of 14 days if breaches are found and the MO has already issued three suspension warnings in a 12-month period. If the issues have not been resolved after 14 days the CMP will remain suspended until all outstanding breaches have been remedied.

From the date of this communication May 19th 2020 the enforcement process will be as follows:

- CMP installations in breach of the TCF policies will be identified in the following ways:

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

  - The MO will regularly monitor the top 100 sites in key markets
  - The MO may also act on TCF community reports of issues found in market

- If a live CMP installation is found to be in breach of the policies:

  - If this is the first, second or third time a breach has been identified in each instance the CMP will be given 14 days to remedy the issues. After 14 days if the issues are not resolved the CMP will be suspended from the Framework until the issues are fixed, in line with the current compliance process.
  - **NEW**: If this is the fourth time within twelve months that a breach has been identified, the CMP will be suspended with immediate effect for a minimum of 14 days, as described above.

CMP customisation

It should be clear that in order to comply with the TCF policies, CMPs must not allow their software to be configurable by publishers in a way that would breach the TCF policies. CMPs must therefore limit customisation to changes that do not impact compliance with the policies.

Publishers

It is understood that even if a CMP does not proactively provide a means of customisation that can invalidate the TCF policies, publishers may still be able to override the style components on the page (CSS) and remove or modify elements using JavaScript - including in ways that could lead to breaches of the policies.

It should therefore be clear that it is the responsibility of CMPs to ensure that all live implementations of their software comply with the TCF policies. These requirements need to be clearly communicated to publishers, especially where free tools are made available, to ensure that publishers understand that overriding the configuration and making changes in this way would be a breach of contract with clear consequences. CMPs must therefore be able to remove their software from a publisher site in these cases.

The MO will continue to communicate to all publishers that overriding CMP configurations in the way described above is not compliant with the TCF Policies.

Important note: if a breach is identified on a publisher site, and the CMP can prove that the breach has been caused by a publisher overriding the CMP configuration, for example by documenting or otherwise demonstrating the CSS and/or JavaScript used by the publisher to override the configuration and provide the MO with copy of a contract showing that this behaviour is forbidden, then this type of breach will not count towards the limit of three suspension warnings described above. Nonetheless, the CMP must resolve the breach as per the compliance procedure within 14 days.

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

IAB Europe

Address:
Rond-Point Schuman 11
B-1040 Belgium
T +32 225 675 33
W www.iabeurope.eu