

APD Decision on IAB Europe and TCF – February 2022

FREQUENTLY ASKED QUESTIONS

The Belgian Data Protection Authority (APD) handed down on 2 February 2022 a decision on IAB Europe and the Transparency & Consent Framework (TCF). What does this decision *actually* say, and what does it mean for the TCF itself, for IAB Europe, for vendors, publishers and consent management platforms (CMPs)?

Are TCF CMP consent pop-ups illegal?

No. There is nothing in the APD's decision that even remotely suggests that consent prompts are, as such, illegal or that they should not be employed by the digital advertising ecosystem to comply with legal requirements under the EU's data protection framework.

If anything, the APD appears to require the disclosure of *additional* information in consent pop-ups. This is because the APD considers user preference signals (i.e, TC Strings under TCF) as personal data that requires the establishment of a legal basis under the GDPR and also, that users cannot reasonably expect that their preferences are saved. As a result, disclosing information about such additional personal data collection and processing (in consent prompts) could be the only way to establish transparency about and user control over the creation, storage and processing of TC Strings. See the question "**What are TC Strings?**" for additional background information.

Should all data collected via the TCF be deleted?

No!

First, there remains the question of whether the TCF truly involves the processing of "personal data" - see the question "**Why are TC Strings considered personal data by the APD ?**" below.

Next, the APD says explicitly in its decision that it cannot impose the removal of all TC Strings generated until now on IAB Europe. Rather, the APD requires IAB Europe to ensure the deletion of personal data collected by means of a TC String in the context of the "global scope", a specific mechanism that was deprecated in June 2021. This mechanism helped set consent preferences in a broader, CMP-independent manner, but it is no longer in use - see the question "**What is the global-scope ?**" below.

The APD's decision only concerns IAB Europe, not any vendor, publishers or CMPs, but it does hint at the possibility of an order for a given publisher or CMP to delete TC Strings if they contain "personal data that has been collected in breach of Articles 5 and 6 GDPR". This is nothing new: if personal data is collected in breach of the GDPR, it cannot be processed. Yet no GDPR breach has been established for any vendor, publisher or CMP. For more input on what the APD's decision actually means for you as a TCF participant - see the question "**Are TCF participants at risk now towards their local Data Protection Authority?**" below.

Will the legitimate interest legal basis be removed from TCF?

The APD solely assessed and concluded that reliance on legitimate interest was inadequate for purposes that entail targeted advertising or profiling of users (excluding non-marketing

related purposes such as audience and performance measurement). It is therefore unclear if the requirement for IAB Europe to prohibit the reliance on legitimate interests as a legal ground for the processing of personal data by TCF participants shall apply to all TCF purposes or solely to purposes related to personalised advertising and profiling. Because of the lack of clarity of the APD's position on this point, IAB Europe will look at this issue in its discussions with the APD - as well as in any legal challenge, if applicable (see question "**Will IAB Europe appeal to the Market Court?**").

Why are TC Strings considered personal data by the APD ?

Although the APD considers it is not established that the TC String in itself allows for direct identification of the user due to the limited metadata and values it contains, it holds that the possibility of combining TC Strings and the IP address by CMPs means it is ultimately information about an *identifiable* user and therefore personal data. This is based on the idea that CMPs could via an Internet Service Provider link an IP address to an individual, a reasoning that is based on legal decisions in a very different context. The APD also suggests that identification is possible by linking the TC String to other data that can be used by TCF participants.

What legal basis could be used for the processing of TC Strings ?

Although the APD appears to consider neither consent nor performance of a contract are available legal basis for the processing of TC String by IAB Europe, it seems legitimate interest could constitute an adequate legal basis : the APD considers that capturing users' approval and preferences to ensure and demonstrate users have validly consented to or not objected to advertising purposes may be considered a legitimate interest, and that the information processed in a TC String is limited to data strictly necessary to achieve the intended purpose. However, it notes that users must be informed about their preferences being stored in the form of a TC String, and provided with a way to exercise the right to object to such storage/processing.

Will IAB Europe appeal to the Market Court?

The decision may be appealed before the Belgian Market Court within a period of thirty days from its notification (i.e. before March 4th 2022). IAB Europe can also ask the Market Court for the suspension of enforcement until the end of the appeal process (in other words, a request to ensure that the APD decision is put on hold entirely until a decision on appeal is handed down). We are still assessing options with respect to a legal challenge.

Will TCF be made into a code of conduct?

IAB Europe has aspired to make the TCF into a GDPR Code of Conduct since the very beginning. It could very well be that adopting the actions recommended by the APD in this case would result in a Framework that is better aligned with the expectations of the APD, which could qualify it as a potential candidate for a Code, with the APD as the leading supervisory authority.

Is OpenRTB illegal?

The scope of the decision is related to IAB Europe's controllership over TC Strings, and the sanction pertains solely to this controllership. The functioning of the OpenRTB system has

been assessed as part of the APD's analysis of the TCF and its interaction with the former, but the ruling does not directly address the legality of the OpenRTB standard.

What are the consequences for IAB Europe to be a Data controller of the TC String ?

Based on guidance from other DPAs up to now and the fact that IAB Europe does not in any way process, own, or decide on the use of specific TC Strings (nor is it involved in any "coordination" of the use of TC Strings), as well as relevant case law and its own interpretation of the GDPR, IAB Europe has not considered itself to be a data controller in the context of the TCF. In its decision, though, the APD takes a different position and says that IAB Europe is a controller regarding the processing of personal data in the form of TC Strings. Yet controllers are under additional obligations according to the GDPR.

The APD decision requires IAB Europe to work with the APD to ensure that these obligations are met going forward : this includes notably establishing a legal basis for the TC String, ensuring effective technical and organisational monitoring measures in order to guarantee the integrity and confidentiality of the TC String, carrying out a data protection impact assessment (DPIA) with regard to the processing activities under the TCF and appointing a Data Protection Officer.

Are TCF participants at risk now towards their local Data Protection Authority?

In principle, no - first for timing and procedural reasons, second for technical and legal reasons.

On **timing** and **procedure**, the APD decision (i) can be appealed (see question "**Will IAB Europe appeal to the Market Court?**") and (ii) includes a grace period, in the form of first a period of two months to present a plan to the APD to take into account the APD's conclusions and in total six months to implement them. Any investigation or complaint before the end of these follow-up procedures (appeal if relevant, and APD collaboration) could be challenged as preventing the proper course of the justice system. This notably stems from the fact that many other local Data Protection Authorities have given input to the APD before it handed down its decision, as well as general principles regarding the rights of defence.

Next, from a more **technical** and **legal** perspective, the APD decision itself does not conclude that the use of TC Strings or the TCF more broadly is illegal. While it does hint in its decision that an order for a given publisher or CMP to delete TC Strings if they contain "personal data that has been collected in breach of Articles 5 and 6 GDPR", it never concludes that vendors publishers or CMPs automatically collect personal data in breach of the GDPR. In other words, the APD decision does not make it much easier for local Data Protection Authorities to attack specific vendors, publishers or CMPs.

Will the action plan and its execution be supervised only by the APD or by other concerned authorities as well ?

The APD expects IAB Europe to submit an action plan within two months from the publication of the decision **to the Litigation Chamber of the Belgian Data Protection Authority**. Once the action plan is validated by the Belgian Data Protection Authority, the compliance measures should be completed within a maximum period of six months. This process will involve proposed changes to the TCF that **would need to be agreed by the existing TCF instances** (the Steering Group, the Policy working group as well as the Framework Signal working group).

Does IAB Europe share personal data with banks and insurance companies?

This may seem like an odd question to feature, but in a recent interview, the chairman of the APD made the astonishing claim that “*data at IAB is shared with banks and insurance companies*”. This caught even IAB Europe by surprise, as it is unclear on which basis the chairman was making this claim, and in any event the APD’s decision does not even come close to making any allegations in this respect. IAB Europe is a trade association for the digital advertising industry that develops policy guidance and compliance standards (such as the TCF). IAB Europe does not process or transfer any personal data beyond what is required for its trade association activities (i.e., data of its employees, data of member representatives, data related to the operation of its website). It certainly does not share any data whatsoever with either banks nor insurance companies beyond what is legally required for its employees and membership fees.

Additional information about the TCF

What is the TCF ?

Launched in April 2018, the TCF is an open source voluntary standard whose purpose is to assist companies from the digital advertising ecosystem in their efforts to comply with EU privacy and data protection law. It contains a minimal set of best practices seeking to ensure that when personal data is processed, users are provided with adequate transparency and choice, and that participants in the ecosystem are informed - through a digital signal - about what preferences users have expressed so that they know what they are permitted to do. Transparency and choice are provided by publishers (websites) and their Consent Management Platforms (CMPs) who then generate the digital signal and make it available to those companies that need to know whether the user has given them the necessary permissions under GDPR.

What are TC Strings ?

TC Strings are the digital signals created by Consent Management Platforms (CMPs) that work for Publishers (owners of websites and/or apps) to capture data subjects’ choices about the processing of their personal data for digital advertising, content and measurement. Vendors can receive such signals directly from CMPs or from other TCF participants to verify if they have obtained consent or legitimate interest for a purpose.

What is the global-scope ?

The TCF Policy previously allowed legal bases in the Framework to be established with “global scope”, which means a legal basis is not only applicable on the website or group of websites (service-specific and group-specific scopes) where it is obtained and managed, but all services implementing global scope preferences. Deprecation of global scope support was [announced](#) on June 22nd 2021, due to the overall negligible use of global scope by publishers, and indication by several DPAs that users should be clearly informed of the digital properties where their choices apply, for example by being provided with a list of domains.