

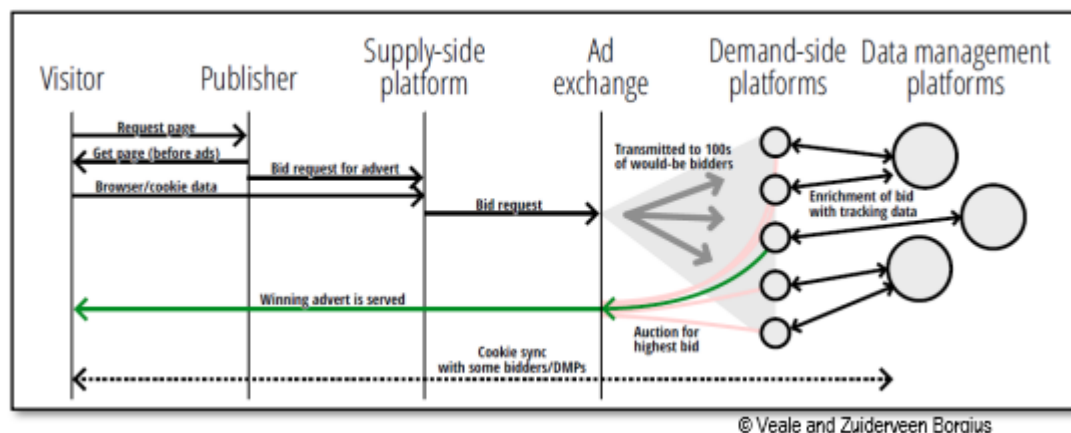
## **IAB Europe's Transparency and Consent Framework (TCF) Infringes GDPR – Belgian DPA Imposes Fine of 250,000 EUR**

The Transparency and Consent Framework (**TCF**), developed by Interactive Advertising Bureau Europe (**IAB Europe**), is a widespread mechanism facilitating the management of users' preferences for online personalised advertising. On 2 February 2022, the Litigation Chamber (*Geschillenkamer / Chambre Contentieuse* – the **Litigation Chamber**) of the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit / Autorité de protection des données* – the **DPA**) imposed a fine of 250,000 EUR on IAB Europe for the TCF's breach of the General Data Protection Regulation 679/2016 (the **GDPR**). The DPA's decision may have an important impact in the digital advertising industry, which relies on the TCF mechanism in the context of the real time bidding process (**RTB**) for online advertisements.

### **Background and Functioning of the TCF Mechanism and RTB**

IAB Europe is a digital marketing trade association – representing corporate members as well as national associations - which indirectly represents 5,000 companies. IAB Europe developed the TCF as a consent solution for digital advertisers to comply with Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the **e-Privacy Directive**). The TCF also aims to ensure compliance with the GDPR for organisations relying on the OpenRTB protocol. The latter was developed by IAB Tech Lab which is based in New York. The TCF mechanism and the OpenRTB protocol are connected, and, together with Google's AdBuyers protocol, the OpenRTB protocol is the most widely used RTB protocol worldwide.

The OpenRTB protocol is a standard protocol that aims to simplify the interconnection between ad space providers, publishers, and competing buyers of ad space. The overall aim is to establish a common language for communication between buyers and vendors of advertising space. RTB as such refers to the use of an instantaneous automated online auction for the sale and purchase of online advertising space. How this works in practice is: when users access a website or application that contains an advertising space, technology companies representing thousands of advertisers can instantly (*i.e.*, 'in real time') bid behind the scenes for that advertising space through an automated auction system using algorithms, in order to display targeted advertising specifically tailored to that individual's profile. Through RTB, billions of advertisement spaces are auctioned every day. The DPA refers to a schematic representation of the RTB process:



When users visit a website or application for the first time, an interface (*i.e.*, a Consent Management Platform or **CMP**) will pop up where they may consent to the collection and sharing of their personal data, or object to various types of processing based on the legitimate interests of ad tech vendors. This is where the TCF plays a role: it facilitates the capture and storage of the users' preferences through the CMP. These preferences are then coded and stored in a unique Transparency and Consent string (**TC string**), which will be shared with the organisations participating in the OpenRTB mechanism in order for them to know what the user has consented or objected to. The author of the preferences is identifiable due to the CMP placing a cookie on the user's device. This means that the IP address of the user is identifiable after the TC string and that cookie have been combined.

The DPA investigated the TCF following a series of complaints filed against IAB Europe in 2019. The complaints mainly claimed that users were insufficiently aware that their profiles are sold a number of times a day to a large number of potential advertisers in order to offer them personal advertising.

### **DPA Decision**

In its decision, the DPA found that IAB Europe acts as a (joint) controller for the TCF system and therefore could be held responsible for the system's infringement of the GDPR. Below, we discuss the main findings in each section of the decision: (i) the finding that IAB acts as controller for the TCF; (ii) the assessment of the infringements of the GDPR; and (iii) the determination of the sanctions imposed on IAB Europe.

#### *IAB Europe is Responsible as Controller of the TCF*

First, the DPA held that IAB Europe acts as controller with respect to the registration of individual users' consent signals, objections and users' preferences by means of a TC string. The DPA considered that the TC string is linked to an identifiable user and IAB Europe is the entity that determines the purposes and means of the processing of that personal data (*i.e.*, it determines the means of generating, storing and sharing the TC string).

In its defence, IAB Europe argued that identification codes assigned to users cannot be considered personal data. IAB Europe also raised the point that, since it did not process, own or make decisions on the data, it should not be considered a controller. The DPA disagreed. First, it explained that information should be

considered personal data as long as that information, due to its content, purpose or effect, can be linked to an identified or identifiable data subject by such means that can reasonably be used, regardless of whether the information from which the data subject can be identified is held entirely by the same controller. Second, since publishers and adtech vendors would not be able to achieve the goals set by IAB Europe without the TCF, IAB Europe has responsibility as controller over the users' personal data. It considered that IAB Europe acts as "managing organisation" for the TCF by determining the policies and technical specifications of the TCF.

IAB Europe's framework thus plays a decisive role in determining the means and purposes of processing users' preferences, consents and objections, regardless of whether IAB Europe handles the personal data itself. The DPA referred to the broad scope of the concept of a "controller" as set out in the Court of Justice of the European Union's (**CJEU**) decisions including *Wirtschaftsakademie* (Case C-210/16; [See our Newsletter, VBB on Belgian Business Law, Volume 2018, No. 6, at p. 9](#)).

In addition, the DPA referred to the CJEU's decision and Advocate General's opinion in the *Fashion ID* case (Case C-40/17; [See our Newsletter VBB on Belgian Business Law, Volume 2019, No. 8, at p. 6](#)) which found that if two parties have converging decisions relating to a processing operation, both can be regarded as joint controllers. On this basis, the DPA considered that IAB Europe provides an ecosystem within which the consent, objections, and preferences of users are collected and exchanged not for its own purposes or self-preservation. IAB Europe collects and exchanges these in order to facilitate further processing by third parties (*i.e.*, publishers and adtech vendors). Therefore, the DPA held that IAB Europe acts as joint controller together with online advertising firms when the personal data are used in the advertising system in the context of the CMP.

#### *IAB Europe's TCF Infringes Several Provisions of the GDPR*

As a data controller, IAB Europe must abide by several provisions of the GDPR, which have clearly not been complied with in the case at issue. The DPA found that IAB Europe had breached several provisions of the GDPR, relating to the following:

- Lawfulness. The DPA found that IAB Europe had failed to establish a legal basis for the processing of user personal data through the TCF and RTB platform. Furthermore, no adequate legal grounds were offered by the TCF for the subsequent processing by adtech vendors. Users were unable to properly consent to the processing of their personal data due to the lack of information (*see infra*). Furthermore, the legitimate interest of online advertising firms cannot constitute a legal basis for processing in the context of direct marketing and behavioural advertising, *i.e.*, the DPA found that the legitimate interest of the organisations participating both in the TCF and the OpenRTB protocol does not outweigh the protection of the fundamental rights and freedoms of the data subjects.
- Transparency and information of the users. The information provided through IAB Europe's TCF system does not comply with the GDPR. In this regard, the DPA argued it is difficult for users to maintain control over their personal data under the mechanism, as the information provided through the CMP interface is "*too generic and vague to allow users to understand the nature and scope of the processing, especially given the complexity of the TCF*". Also, users are not informed about the specific purposes for which adtech vendors will process their data.

- Accountability, security and data protection by design and by default. The DPA furthermore found that IAB Europe had failed to guarantee the integrity of processing users' preferences, consents and objections and failed to monitor vendors for compliance with their TCF rules (*i.e.*, adtech vendors would receive a consent signal without any technical or organisational measure to ensure that this consent signal is valid or that a vendor has actually received it (rather than generated it)). The DPA held that in the absence of organisational and technical measures in accordance with the principle of data protection by design and by default, including to ensure the effective exercise of data subject rights as well as to monitor the validity and integrity of the users' choices, the conformity of the TCF with the GDPR is not adequately warranted nor demonstrated.
- Other obligations pertaining to a controller processing personal data on a large scale. The DPA also found that IAB Europe has failed to keep a register of processing activities, to appoint a DPO and to conduct a data protection impact assessment (**DPIA**). Indeed, the DPA considered that a DPIA should have been conducted given the large number of data subjects that come into contact with websites that implement the TCF and given the impact of the TCF on large-scale processing of personal data in the context of the RTB platform.

#### *Sanctions Imposed by the DPA*

In addition to a fine of 250,000 EUR, the DPA imposed an order on IAB Europe to submit a plan for corrective measures within two months after the date of the decision and issued a daily penalty of 5,000 EUR if IAB Europe fails to execute the plan within six months after the plan has been approved. Also, IAB Europe was ordered to permanently delete all TC strings and other personal data already processed in the TCF *“from all its IT systems, files and data carriers, and from the IT systems, files and data carriers of processors contracted by IAB Europe”*.

IAB Europe can appeal against the DPA's decision before the Belgian Market Court (*Marktenhof / Cour des Marchés*).

The DPA's decision is available in [Dutch](#), [French](#) and [English](#).