Litigation Chamber

Decision on the merits 21/2022 of 2 February 2022

Unofficial translation from Dutch

Case number: DOS-2019-01377

Concerning: Complaint relating to Transparency & Consent Framework

The Litigation Chamber of the Data Protection Authority, composed of Mr Hielke Hijmans, chairman, and Mr Yves Poullet and Mr Frank De Smet;

Having regard to 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), hereinafter referred to as the GDPR;

Having regard to the Act of 3 December 2017 establishing the Data Protection Authority, hereinafter referred to as DPA Act;

Having regard to the Internal Rules of Procedure, as approved by the House of Representatives on 20 December 2018 and published in the *Official Gazette* on 15 January 2019;

Having regard to the documents in the file;

has taken the following decision on:

The complainants: Mr Johnny Ryan; Mr Pierre Dewitte and Mr Jeff Ausloos, as well as Mrs Katarzyna Szymielewicz, who designated the NGO Panoptykon Foundation to act on her behalf, and the NGOs Bits of Freedom and La Ligue des Droits de l'Homme, all represented by Mr Frederic Debusseré and Mr Ruben Roex, and Mr Bruno Bidon, hereinafter 'the complainants';

The defendant: IAB Europe, having its registered office at [...] 1040 Brussels, with company number [...], represented by Mr Frank Judo and Mr Kristof Van Quathem, hereinafter 'the defendant'.

Table of contents

Case number: DOS-2019-01377 1

A. Facts and procedure 4

A.1. - Complaints against Interactive Advertising Bureau Europe 4

A.2. - The language of the procedure: Interim Decision 01/2021 as amended by the Interim Decision 26/2021 of 23 February 2021 6

A.3. - RTB and TCF 6

A.3.1. - Definitions and operation of the Real-Time Bidding system 6

A.3.2. - IAB Europe's Transparency & Consent Framework 12

A.4. - Reports of the Inspection Service 15

A.4.1 - IAB Europe acts as data controller in respect of the Transparency and Consent Framework and the personal data processing operations relating thereto 15

A.4.2. - Identified infringements of the GDPR 15

A.4.3. - Additional considerations that the Inspection Service considers relevant to the assessment of the gravity of the facts 19

A.5. - Summary of the defendant's response dd. 11 February 2021 19

A.5.1. - IAB Europe is not a data controller with regard to the processing of personal data in connection with the TCF 19

A.5.2. - The TCF complies with the GDPR 22

A.5.3. - IAB Europe is not subject to the obligation to keep a register of processing operations 23

A.5.4. - IAB Europe is not required to appoint a data protection officer 24

A.5.5. - IAB Europe did cooperate with the Inspection Service 24

A.5.6. - There are no aggravating circumstances to the detriment of IAB Europe 24

A.6. - Summary of the complainants' reply submissions dd. 18 February 2021 25

A.6.1. – IAB Europe is data controller for the TCF 25

A.6.2. - The processing operations carried out in the TCF violate the GDPR at various levels 26

A.7. - Summary of the defendant's rejoinder dd. 25 March 2021 34

A.7.1. - Organisations that process personal data within the RTB system are responsible for complying with the GDPR and the ePrivacy Directive 34

A.7.2. - IAB Europe cannot be held responsible for the alleged illegal practices of RTB participants, as the TCF is completely separate from RTB 35

A.8. - Hearing and reopening of debates 36

A.9. - Procedural objections raised by the defendant 41

A.9.1. - Infringements of procedural rules applicable to the inspection report and of fundamental rights and freedoms of IAB Europe 41

A.9.2. - Infringements of the fundamental rights and freedoms of IAB Europe with regard to the general nature of the procedure for the DPA 47

A.10. - Sanction form, European cooperation procedure and publication of the decision 58

B. Reasoning 62

B.1. – Processing of personal data in the context of the Transparency and Consent Framework 62

B.1.1. – Presence of personal data within the TCF 62

B.1.2. - Processing of personal data within the TCF 67

B.2. - Responsibility of IAB Europe for the processing operations within the Transparency and Consent Framework 68

B.2.1. - Broad interpretation of the concept of data controller by the Court of Justice and the EDPB 69

B.2.2. - Determining the purposes of the processing of personal data within the TCF 71

B.2.3. - Determining the means for processing personal data within a TCF 74

B.3. - Joint controllership of publishers, CMPs and adtech vendors with regard to the means and purposes of the processing of personal data within the context of the TCF and of the OpenRTB 79

B.3.1. - Joint processing responsibility 80

B.4. On the alleged breaches of the General Data Protection Regulation 87

B.4.1 - Lawfulness and fairness of processing (Art. 5.1.a and 6 GDPR) 87

B.4.2. - Duty of transparency towards data subjects (Art. 12, 13 and 14 GDPR) 99

B.4.3. - Accountability (art. 24 GDPR), data protection by design and by default (Art. 25 GDPR), integrity and confidentiality (Art. 5.1.f GDPR), as well as security of processing (Art. 32 GDPR) 101

B.4.4. - Additional alleged breaches of the GDPR 105

C. Sanctions 111

C.1. - Breaches 115

C.2. - Sanctions 118

A. Facts and procedure

A.1. - Complaints against Interactive Advertising Bureau Europe

1. In the course of 2019, a series of complaints were filed against Interactive Advertising Bureau Europe (hereinafter IAB Europe), for breaching various provisions of the GDPR in relation to large-scale processing of personal data. The complaints related, in particular, to the principles of legality, appropriateness, transparency, purpose limitation, storage restriction and security, as well as to accountability.

2. Nine identical or very similar complaints were filed, four directly with the Data Protection Authority (hereinafter 'DPA') and five via the IMI system with supervisory authorities in other EU countries.

3. The Inspection Service also carried out investigations on its own initiative, pursuant to Article 63(6) DPA Act. Since the complaints related to the same subject matter and were directed against the same party (IAB Europe), on the basis of the principles of proportionality and necessity in the conduct of investigations (Article 64 DPA Act), the Inspection Service merged the above files into one case under file number DOS-2019-01377.

4. The complainants have agreed to this merger, as well as to the request by the Litigation Chamber to merge their submission and submit them as a joint package, in the interests of economy and efficient proceedings.

5. In this international case, four complainants, including the NGO Ligue des Droits Humains, are domiciled in Belgium, one in Ireland, four in different EU states, represented by the Polish-based NGO Panoptykon, and one complainant is represented by the Dutch-based NGO Bits of Freedom.

6. Pursuant to Article 4(1) DPA Act, the Data Protection Authority is responsible for monitoring the data protection principles contained in the GDPR and in other laws containing provisions on the protection of the processing of personal data.

7. Pursuant to Article 32 DPA Act, the Litigation Chamber is the administrative dispute resolution body of the DPA[1].

8. Pursuant to Articles 51 et seq. GDPR and Article 4(1) of the DPA Act, it is the task of the Litigation Chamber, as the administrative dispute resolution body of the DPA, to exercise effective control over the application of the GDPR and to protect the fundamental rights

[1] The administrative nature of the disputes before the Litigation Chamber has been confirmed by the Market Court. See in particular the judgment of 12 June 2019, published on the website of the DPA, as well as decision 17/2020 of the Litigation Chamber.

and freedoms of natural persons with regard to the processing of their personal data and to facilitate the free flow of personal data within the European Union. These tasks are further explained in the Strategic Plan and the management plans of the DPA, drawn up pursuant to Article 17(2) DPA Act.

9. Moreover, as regards the one-stop-shop mechanism, Article 56 GDPR states: "*Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.*"

10. Article 4.23 GDPR clarifies the notion of cross-border processing in the following terms: "*processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;*"

11. The defendant has its only registered office in Belgium, but its activities have a significant impact on stakeholders in several Member States, including the plaintiffs in Ireland, Poland and the Netherlands, as well as in Belgium. The Litigation Chamber draws its jurisdiction from a combined reading of Articles 56 and 4(23)(b) of the GDPR. The DPA was seized by the Polish, Dutch and Irish data protection authorities following a complaint made to them by the complainants in accordance with Article 77.1 of the GDPR. It declares that it is the lead supervisory authority (Article 60 of the GDPR).

12. The following supervisors have indicated their willingness to act as concerned supervisory authorities (CSA): the Netherlands, Latvia, Italy, Sweden, Slovenia, Norway, Hungary, Poland, Portugal, Denmark, France, Finland, Greece, Spain, Luxemburg, Czech Republic, Austria, Croatia, Cyprus, and Germany (Berlin, Rhineland-Palatinate, North Rhine-Westphalia, Saarland, Lower Saxony, Brandenburg, Mecklenburg-Western Pomerania, Bavaria).

13. In the course of the proceedings, additional complaints with a very similar focus to the ones on which the present case is based were sent to the Belgian DPA, by the Maltese, Romanian, Croatian, Greek, Portuguese, Swedish, Cypriot and Italian DPAs. These complaints are not part of the present proceedings.

A.2. - The language of the procedure: Interim Decision 01/2021 as amended by the Interim Decision 26/2021 of 23 February 2021

14. On 13 October 2020, the Litigation Chamber sent a letter to the parties, in accordance with Article 98 DPA Act, informing the parties of the language of the procedure (French), and inviting them to present their written submissions.

15. In response to a request by the complainants dd. 27 November 2020, and in view of the international nature of this case, the Litigation Chamber issued Interim Decision 01/2021 on 8 January 2021 regarding the language of the proceedings. Following an appeal by the complainants to the Market Court, this Interim Decision was amended on 23 February 2021 (Interim Decision 26/2021).

16. Pursuant to the latter Interim Decision, which is based on an agreement with the parties, the DPA's correspondence with the parties is conducted in Dutch and the preliminary and final decisions of the Litigation Chamber are in Dutch. However, the Litigation Chamber shall provide the parties with a French and an English translation of the final decision.

17. Moreover, the parties are free to use the language of their choice (Dutch, French or English) in the proceedings before the Litigation Chamber, either in writing or orally. In the case of IAB Europe, it is French or English. The DPA is not responsible for translations of procedural documents submitted by one party on behalf of the other.

18. Finally, the Litigation Chamber points out that it sometimes uses English language terminology in this decision, in cases where translation into Dutch would reduce the comprehensibility of the decision.

A.3. - RTB and TCF

19. In essence, this case concerns, on the one hand, the conformity of the Transparency & Consent Framework (hereinafter, 'TCF') with the GDPR and, more specifically, the responsibility of IAB Europe, the defendant in these proceedings, and other various actors involved. In addition, it also pertains to the impact of the TCF on the so-called Real-Time Bidding (RTB). Given the complexity of the latter, it is introduced here.

A.3.1. - Definitions and operation of the Real-Time Bidding system

20. In contrast to "traditional" advertising, where the parties involved manually and contractually determine the modalities of information exchange, online advertising is

usually done primarily automatically and behind the scenes, through "*Programmatic advertising*" methods of which real-time bidding (RTB) is the leading system[2].

21. Real-time bidding is defined in legal literature as "a network of partners that enables big data applications within the organisational field of marketing to improve sales of pre-determined advertising space through real-time data-driven marketing and personalised (behavioural) advertising"[3].

22. Real-time bidding refers to the use of an instantaneous automated online auction for the sale and purchase of online advertising space. Specifically, it means that when an individual accesses a website or application that contains an advertising space, behind the scenes through an automated online *auction* system and algorithms, technology companies representing thousands of advertisers can instantly (in *real time*) *bid* for that advertising space to display targeted advertising specifically tailored to that individual's profile.

23. Real-time bidding works behind the scenes on most commercial websites and mobile apps. Thousands of companies are involved that receive information about the person visiting the website. In this way, billions of advertisements are auctioned every day.

24. In a real-time bidding system, several parties are involved[4]:

    A. The companies or organisations that have created and manage the relevant real-time bidding system, including by setting its *policies/governance* and technical protocols. The main ones are:

        a. the "*OpenRTB*" system and the associated "*Advertising Common Object Model*" (AdCOM), created by IAB Technology Laboratory, Inc. (abbreviated as "IAB Tech Lab") and Interactive Advertising Bureau, Inc. (abbreviated as "IAB"), both based in New York;

        b. the "*Authorised Buyers*" system created by Google.

    The OpenRTB is a standard protocol that aims to simplify the interconnection between ad space providers, publishers (ad exchanges, *Sell-Side Platforms*, or networks working with publishers), and competing buyers of ad space (bidders, *Demand-Side Platforms*, or

---

[2] M. VEALE, FR. ZUIDERVEEN BORGESIUS, "Adtech and Real-Time Bidding under European Data Protection Law", German Law Journal*, 31 July 2021,* p. 8-10.

R. VAN EIJK, "Web Privacy Measurement in Real-Time Bidding Systems - A Graph-Based Approach to RTB system classification", 2019, p. 140: "*a network of partners enabling big data applications within the organizational field of marketing to improve sales by real-time data-driven marketing and personalized (behavioural) advertising*", available at https://ssrn.com/abstract=3319284; [3] M. VEALE, FR. ZUIDERVEEN BORGESIUS, *ibidem*, p. 3.

[4] *Ibidem.*

networks working with advertisers). The overall objective of OpenRTB is to establish a common language for communication between buyers and vendors of advertising space[5].

B. On the "supply side" there are:

   a. Companies that own a website or app with advertising space. In RTB jargon, these companies are called "*publishers*".

   b. Companies operating an automated online platform through which *publishers* can optimise the value and volume of their ad space sales by signalling the availability of their ad space to be displayed to a data subject and requesting that one or more *bid requests* be made for that ad space. In RTB jargon, these companies are called "*Sell-Side Platforms*" ("SSPs"). SSPs provide the available inventory of their publishers to the various ad exchanges in the market and possibly to ad networks and other DSPs. The most advanced SSPs work in real time. As soon as an ad space is called up when a page is viewed on a publisher's site, the SSP searches for the best offer on that type of ad space according to the detected visitor profile, and automatically delivers the corresponding ad[6].

C. On the "demand side" there are:

   a. Companies that want to display advertising for their products or services in a targeted manner to visitors to websites and users of apps (the advertisers).

   b. Companies operating an online platform that enables advertisers and media agencies to carry out and optimise their purchases of advertising space, and in which advertisers' ads are offered[7]. In RTB jargon, these companies are called "*Demand-Side Platforms*" ("DSPs").

D. Acting as intermediaries between them are companies, so-called "*Ad Exchanges*", which bring the supply and demand side organisations together and allow them to communicate with each other automatically so that the DSPs can bid on *bid requests* from SSPs.

E. In addition, there are so-called *"Data Management Platforms"* ("DMPs") that extract huge amounts and types of personal data from multiple sources (such as from devices, cookies, mobile identifiers, pixels, online surfing behaviour analysis, social media, offline data, but also from third parties such as data brokers, etc.), then centralise this data, and finally analyse and categorise it by means of algorithms and artificial intelligence. By

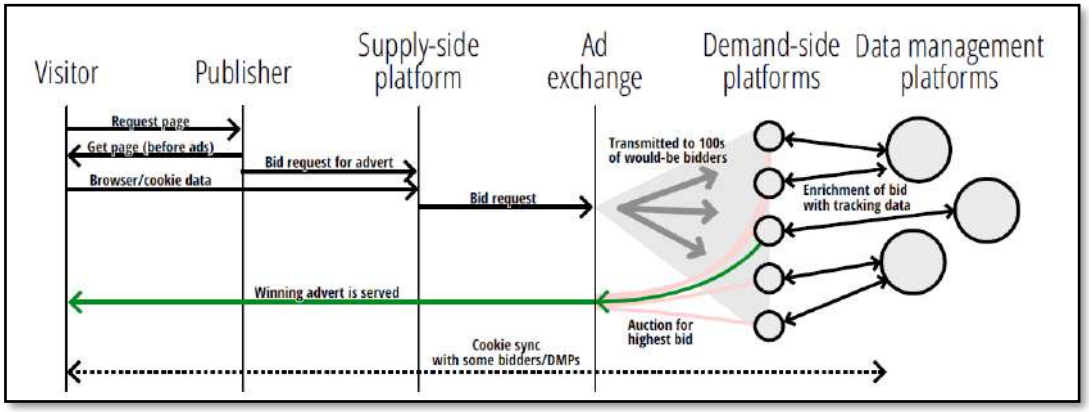
[5] Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 11.
[6] Technical Analysis Report of the Inspection Service, 4 June 2019 (Exhibit 24), p. 5-6.
[7] Technical Analysis Report of the Inspection Service, 4 June 2019 (Exhibit 24), p. 5.

using a DMP, an advertiser can enrich and combine data that it himself has about (potential) customers with data that it can get from a central DMP. Thus, one of the main functions of a DMP is to create detailed consumer profiles through data enrichment in order to optimise the targeting and effectiveness of marketing and advertising campaigns and to provide personalised offers on websites and in applications[8].

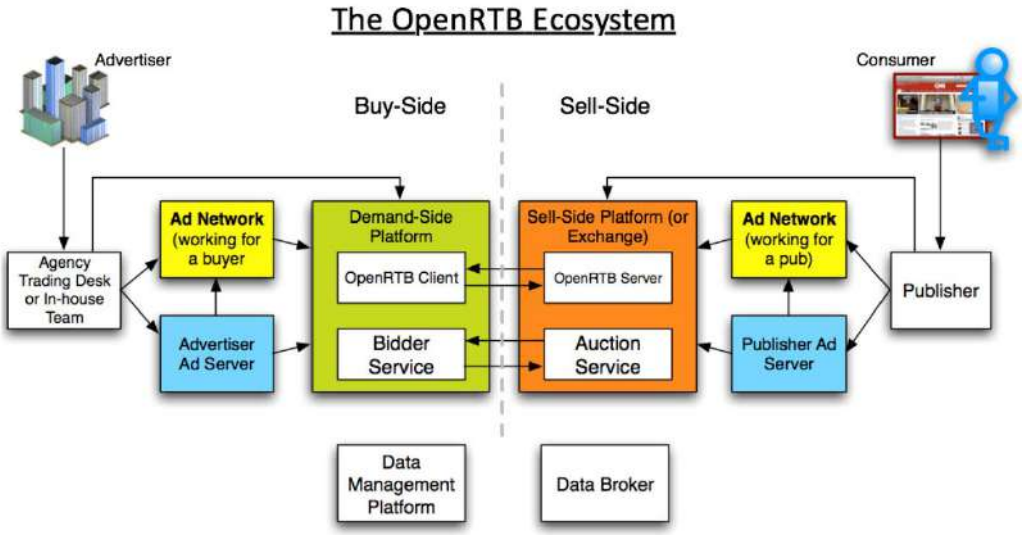
25. After an advertiser has drawn up detailed consumer profiles via a DMP, it bids via its DSP for *bid requests* from *publishers/SSPs* offering advertising space that matches those consumer profiles.

26. In RTB jargon, SSPs, DSPs, Ad Exchanges, advertisers and DMPs are collectively referred to as "*Vendors*".

27. Schematically this can be presented as follows[9]:



28. This can also be represented as follows[10]:



[8] Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 7.

[9] M. VEALE, FR. ZUIDERVEEN BORGESIUS, "Adtech and Real-Time Bidding under European Data Protection Law", German Law Journal, *31 July 2021, p.* 9.

[10] Technical Analysis Report of the Inspection Service, 4 June 2019 (Exhibit 24), p. 6.

29. The content of a *bid request*, which contains data about online users, their device and the websites visited, is captured by the OpenRTB system or the Authorised Buyers system. Generally, the following categories of personal data can be communicated in a *bid request* with advertisers[11]:

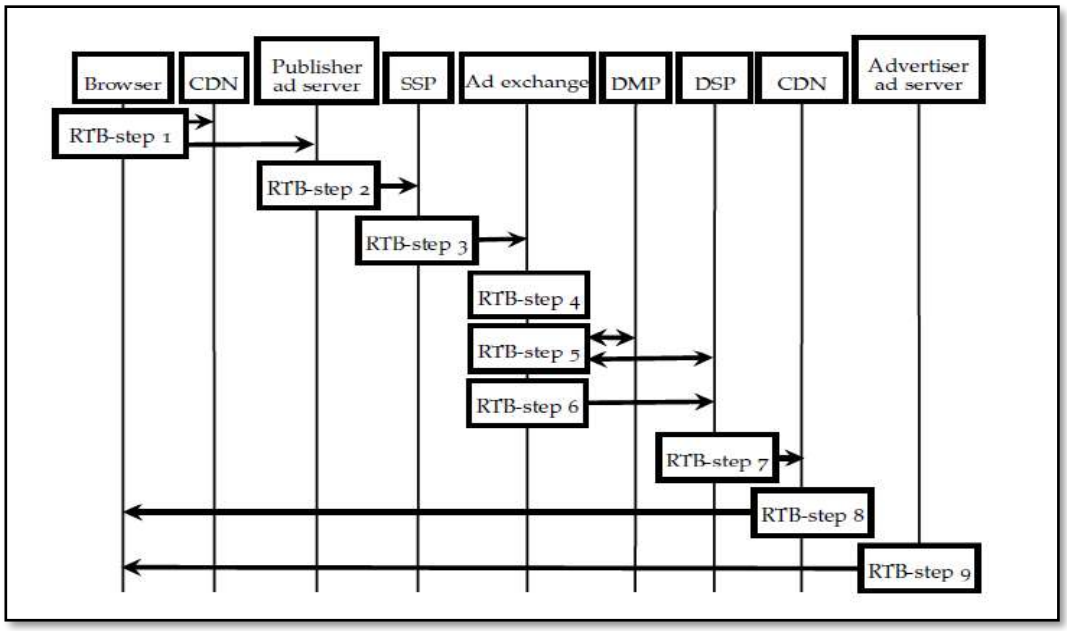
- URL of the visited site
- Category or subject of the site
- Operating system of the device
- Browser software and version
- Manufacturer and model of the device
- Mobile operator
- Screen dimensions
- Unique user identification set by vendor and/or buyer.
- Unique person identifier from the Ad Exchange, often derived from the Ad Exchange's cookie.
- The user identification of a DSP, often derived from the Ad Exchange's cookie that is synchronised with a cookie from the DSP's domain.
- Year of birth
- Gender
- Interests
- Metadata reporting on consent given
- Geography
- Longitude and latitude
- Post code

30. As a result, it is beyond doubt that the GDPR applies *ratione materiae* to the RTB system, of which the OpenRTB protocol and, to some extent, the Transparency & Consent Framework (TCF) discussed below are essential components, as RTB operations by means of *bid requests* inherently entail the processing of personal data.

31. The different steps and interactions between the SSPs, DSPs and DMPs that take place in the RTB system can be summarised as follows[12]:

[11] *Ibidem*, p. 10.

[12] R. VAN EIJK, "Web Privacy Measurement in Real-Time Bidding Systems- A Graph-Based Approach to RTB system classification", 2019, p. 150-151, available at https://ssrn.com/abstract=3319284.



i. An end user requests a web page;

ii. The *publisher*'s ad server on the web page selects an SSP;

iii. The SSP then selects an *Ad exchange*;

iv. The *Ad Exchange* sends *bid requests* to hundreds of network partners and offers them the opportunity to generate a *bid response*;

v. The *Ad Exchange* allows privileged DMPs and/or DSPs to synchronise http cookies;

vi. The *Ad exchange* places the winning bid;

vii. The DSP serves the advertiser's ad;

viii. The ad is loaded from a *CDN* (Content Delivery Network, or network provider);

ix. The advertiser's server loads a Javascript for verification;

32. *Real-time bidding* poses a number of risks that stem from the nature of the ecosystem and the way personal data is processed within it. These risks include[13]:

- profiling and automated decision-making;
- large-scale processing (including special categories of personal data);
- innovative use or application of new technological or organisational solutions;
- matching or merging of datasets;
- analysis or prediction of behaviour, location or movements of natural persons;
- invisible processing of personal data.

[13] Information Commissioner's Office, "Update report into adtech and real time bidding", 20 June 2019, p. 9 - https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

33. In addition, a large number of organisations — such as data controllers, joint data controllers, processors or other data subjects — are part of the ecosystem. This has a potentially significant impact on data protection. Moreover, most data subjects have a limited understanding of how the ecosystem processes their personal data.

34. As a result, the GDPR applies to the processing operations carried out within the framework of RTB, which are of such a nature that they can create a significant risk to the rights and freedoms of individuals.

A.3.2. - IAB Europe's Transparency & Consent Framework

35. IAB Tech Lab has developed the OpenRTB protocol, which together with Google's AdBuyers protocol, is the most widely used RTB protocol worldwide. IAB Tech Lab, based in New York in the United States of America, acts as a provider of the OpenRTB standard and should be distinguished from IAB Europe, which developed the Transparency and Consent Framework (TCF).

36. IAB Europe is a federation representing the digital advertisement and marketing industry on the European level. It comprises corporate members as well as national associations, with their own corporate members. Indirectly, IAB Europe represents approximately 5.000 companies, including both large corporations and national members[14].

37. According to IAB Europe, the defendant in these proceedings, the TCF provides *accountability* and *transparency* to the OpenRTB. The TCF constitutes a separate set of policies, technical specifications, terms and conditions, created, managed and administered by IAB Europe, and, according to the defendant, should be capable of informing users of the legitimate interests pursued by advertisers, as well as obtaining the valid consent of those users with regard to the processing of their personal data in a real-time bidding system (such as OpenRTB).

38. Although the OpenRTB should be distinguished from the TCF, the two systems are connected. After all, IAB Europe claims that the TCF provides an operational framework in which the data processing operations that take place on the basis of the OpenRTB protocol can be brought in line with the GDPR (and the ePrivacy Directive).

39. In relation to the TCF, IAB Europe states the following:

> "*In its current form, the TCF is a cross-industry best practice standard that facilitates the digital advertising industry's compliance with certain EU privacy and data protection rules and seeks to bring improved transparency and control to individuals over their personal data. Specifically, it is a 'framework" within which businesses operate independently and which*

[14] As indicated by the CEO of the defendant during the hearing before the Litigation Chamber, on 11 June 2021.

helps them satisfy the requirement to have a GDPR legal basis for any processing of personal data and the requirement for user consent for the storing and accessing of information on a user device under the ePrivacy Directive."[15]

40. Moreover, the main players within the TCF correspond to a large extent to the parties participating in the OpenRTB (with the exception of the Consent Management Platforms, *i.e.* 'CMPs'):

    i. *Publishers*— Parties who make advertising space available on their website or in their application and who are in direct contact with users whose personal data are collected and processed. A *publisher* may provide a CMP (see below) on its website or in its app to enable it to seek and manage the consent of visitors/users to the processing of their personal data and to facilitate the operation of TCF[16]. *Publishers* decide which *adtech vendors* may collect data through their website and process their users' personal data (and/or access their devices) and for what purposes[17].

    ii. *Adtech vendors* — Companies that receive personal data from *publishers* in order to fill advertising spaces on *publisher* websites or in publisher apps, such as advertisers, *SSPs*, *DSPs*, *Ad Exchanges*, and *DMPs*.

    iii. *Consent Management Platforms*— Specifically for TCF, there are also companies that offer so-called "*Consent Management Platforms*" (CMPs). Specifically, a CMP takes the form of a pop-up that appears during the first connection to a website to collect the Internet user's consent to the placement of cookies and other identifying information[18].

41. An essential part of the intervention of a CMP is the generation of a character string consisting of a combination of letters, numbers and other characters. This string is called the "*TC String*" by IAB Europe, which stands for the "*Transparency and Consent String*". The TC String is meant to capture in a structured and automated way the preferences of a user when he visits a website or app of a *publisher* that has integrated the CMP. This concerns in particular the capturing of consent (or not) to the processing of personal data for marketing and other purposes, whether or not to share personal data with third parties *(adtech vendors*) and the exercise or not of the right to object.

42. Vendors decipher the TC String to determine whether they have the necessary legal basis to process a user's personal data for the specified purposes. Thanks to its concise data

[15]Conclusions of the defendant's reply dated 25 March 2021, para. 32.

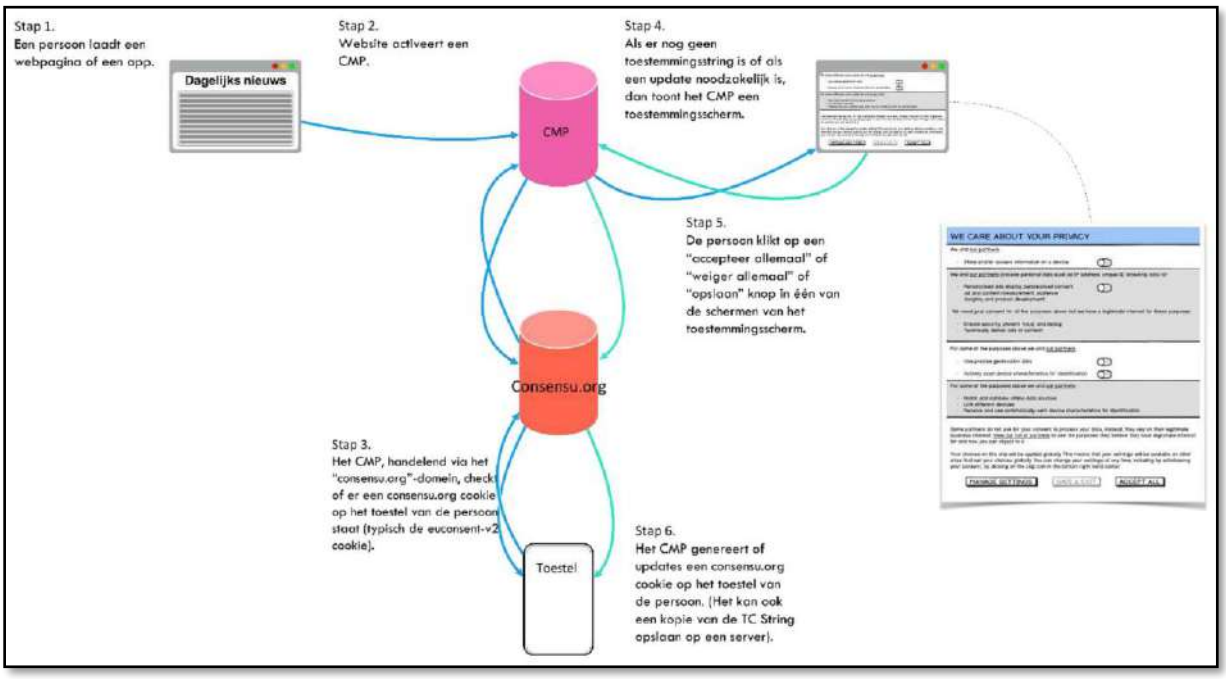
[16] Information Commissioner's Office, "*Update report into adtech and real time bidding*", 20 June 2019, p. 11-12, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.

[17]Conclusions of the defendant's reply dated. 25 March 2021, para. 36.

[18] Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 59.

format, the CMP can store and retrieve a user's preferred data at any time and pass this information on to adtech vendors who need it[19].

43. This can be represented schematically as follows[20]:



i. An Internet user browses the website of a *publisher*, for example a news website.

ii. The *publisher* ensures that a CMP is activated on its website or in its app when the user arrives.

iii. The CMP checks whether a TC String already exists for this user or not. If a "globally stored" TC String[21] is chosen, the CMP will contact the IAB Europe-managed consensu.org internet domain to verify from there whether there is already a so-called "consensu" cookie on the user's device. In particular, this relates to the *euconsent-v2* cookie.

iv. If the third step shows that the TC String does not yet exist or is not up to date, in a fourth step the CMP will show the user a user interface where he can consent to the collection and sharing of his personal data.

v. The Internet user makes a choice in the user interface.

vi. The CMP generates the *TC String* and places a *euconsent-v2* cookie on the user's device or updates the existing cookie.

[19] Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 75.
[20] Conclusions of the complainant dated. 18 February 2021, para. 18.
[21] Also referred to as “globally scoped consents”.

A.4. - Reports of the Inspection Service

A.4.1 - IAB Europe acts as data controller in respect of the Transparency and Consent Framework and the personal data processing operations relating thereto

44. In these proceedings, the Inspection Service focused its investigation exclusively on IAB Europe, which the Inspection Service identified as the data controller for the TCF. The Inspection Service supports this initial finding with the fact that IAB Europe developed the TCF, with which IAB Europe imposes binding rules on participating organisations. According to the Inspection Service, these binding rules relate in particular to the processing of personal data in the context of the collection and processing of consent, as well as the preferences of online users, regarding processing purposes and authorised *adtech vendors*.

45. The Inspection Service bases its report on two technical analyses related to the *Open Realtime Bidding API Specification* of IAB Europe, as well as the different mechanisms under the *OpenMedia* specification of IAB Tech Lab, including the *Transparency and Consent Framework* developed by IAB Europe jointly with IAB Tech Lab[22].

46. With regard to the OpenRTB protocol, the Inspection Service concludes that IAB Tech Lab, which developed this open technical standard and is based in New York (USA), merely acts as a provider of the system with respect to participating organisations and therefore cannot be considered a data controller. In contrast to the TCF, the OpenRTB allows the processing of personal data in accordance with means and purposes entirely determined by the participating organisations, but not by IAB Tech Lab.

47. Finally, the Inspection Service states that the Belgian DPA is not competent for the *Authorised Buyers* protocol, which was developed by Google as an alternative to the OpenRTB standard.

A.4.2. - Identified infringements of the GDPR

48. The Inspection Service finds that IAB Europe is in breach of the following legal provisions and principles of the GDPR with its *Transparency and Consent Framework*:

- Articles 5.1.*a* and 5.2 (principles of fairness, transparency and accountability)
- Article 6.1 (lawfulness of processing);
- Article 9.1 and 9.2 (processing of special categories of personal data);
- Article 12.1 (transparency of information, communications and modalities for exercising data subjects' rights);

[22] Technical Analysis Reports of the Inspection Service, 4 June 2019 (Exhibit 24) and 6 January 2020 (Exhibit 53). Whereas IAB Europe drafted the TCF Policies, IAB Tech Lab developed the technical specifications in accordance with said Policies.

- Article 13 (information to be provided when personal data have been obtained from the data subject);
- Article 14 (information to be provided when personal data have not been obtained from the data subject);
- Article 24.1 (responsibility of the data controller);
- Articles 32.1 and 32.2 (security of processing).

49. Outside the scope of the complaints, the Inspection Service also finds additional infringements of the following provisions of the GDPR:

- Article 30 (register of processing activities);
- Article 31 (cooperation with the supervisory authorities);
- Article 24.1 (responsibility of the data controller);
- Article 37 (appointment of a data protection officer.

Finding 1 - IAB Europe wrongly uses legitimate interest as a basis for processing personal data under the TCF, whereby special categories of personal data may also be processed in certain cases.

50. Based on the two versions of the *IAB Europe Transparency & Consent Framework Policies*[23], the Inspection Service notes that IAB Europe places the responsibility for compliance with the principles of transparency and fairness on the CMPs and/or *publishers*. Moreover, IAB Europe takes the position that the legitimate interest of participating organisations is an appropriate basis for processing personal data within the framework of the TCF in order to create an advertising profile of the data subjects and to display personalised advertising to them. However, according to the Inspection Service, IAB Europe fails to provide evidence that the interests, in particular the fundamental rights and freedoms, of data subjects were adequately considered in the process.

51. Incidentally, the Inspection Service notes that in certain circumstances, special categories of personal data may also be collected and processed by the participating organisations. For example, participating organisations could learn about the websites previously visited by a data subject, whereby the political opinions, religious or philosophical convictions, sexual orientation, health data or even trade union memberships of the data subjects could be inferred or revealed.

52. The Inspection Service considers that IAB Europe has thus failed to comply adequately with the principles of transparency and fairness in relation to the persons concerned.

[23] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32); IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38).

Finding 2 - The information provided does not comply with Articles 12.1, 13 and 14 of the GDPR

53. The Inspection Service also finds that the privacy policy that IAB Europe makes available to data subjects is not always transparent or understandable, which constitutes a breach of the obligations arising from Articles 12.1, 13 and 14 of the GDPR.

54. The privacy policy of IAB Europe[24] is available only in English. In addition, the privacy policy contains several terms that, without further explanation, are unclear to those involved. By way of example, the Inspection Service mentions "*services*" and "*other means*".

55. Moreover, according to the Inspection Service, the information provided is incomplete and inadequate. Firstly, data subjects are not informed of the exact legitimate interests pursued by IAB Europe. Secondly, it is not easy for data subjects to distinguish between the different recipients or categories of recipients of their personal data; the terms "*third parties*" and "*partners*" are not understandable without further explanation. Thirdly, data subjects are not informed, on the one hand, about the reference to appropriate or sufficient safeguards for the international transfer of their personal data outside the EEA or, on the other hand, about how to obtain a copy or where it is made available. Fourthly, based on the privacy policy of IAB Europe, it is not clear to data subjects that their personal data can be obtained by IAB Europe via its TCF[25]. Fifthly, the conditions under which data subjects must provide their personal data, in particular whether this collection is organised on the basis of a legal, pre-contractual or contractual obligation, are not clearly set out. Nor are the data subjects informed of the possible consequences of not providing their data.

56. Therefore, the privacy policy does not comply with the obligations enshrined in Articles 13 and 14 of the GDPR.

Finding 3 - IAB Europe does not foresee any compliance control under the TCF policy rules

57. On the basis of the two versions of the *IAB Europe Transparency and Consent Framework* Policies[26], the Inspection Service is of the opinion that IAB Europe does not sufficiently monitor compliance with the rules it has developed with regard to participating organisations. In particular, it would be possible for a CMP to continue exchanging personal data with a publisher even if it reasonably considers that this Publisher does not comply with the rules imposed by IAB Europe in the context of its TCF or the rules imposed by the legislation[27].

[24] Exhibit 41.

[25] Terms and Conditions for the IAB Europe Transparency & Consent Framework ("Terms and Conditions") (Exhibit 33), p. 7.

[26] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32); IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38).

[27] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 11 ; IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38), p. 6.

58. Given the role that IAB Europe assigns to itself, namely that of *Managing Organisation*, this disregard for the risks to the rights and freedoms of data subjects would indicate a breach of Article 24.1 GDPR as well as of the obligation to provide appropriate security for the processing of personal data, pursuant to Articles 32.1 and 32.2 GDPR.

Finding 4 - IAB Europe failed to keep a register of processing operations

59. The Inspection Service also notes that IAB Europe does not consider itself obliged to keep a register of processing activities, based on the exception provided in Article 30.5 GDPR for organisations with fewer than 250 persons[28]. The Inspection Service also points out that IAB Europe did not initially provide a copy of its register of processing activities to the Inspection Service.

60. Only in a second reply[29] did IAB Europe decide, for the sake of completeness, to provide a register of processing activities, although the organisation still does not consider itself subject to the obligation under Article 30.5 GDPR.

Finding 5 - IAB Europe did not cooperate sufficiently with the investigation by the Inspection Service

61. Based on finding 4, and with reference to the delay with which IAB Europe responded to the Inspection Service's requests for additional information, the Inspection Service concludes that the conduct of IAB Europe in the context of its investigation is in breach of the duty to cooperate under Article 31 of the GDPR.

Finding 6 - IAB Europe failed to appoint a data protection officer, although as Managing Organisation it reserves the right to access the (personal) data that organisations participating in the TCF collect and process

62. IAB Europe asserts[30] that it does not fulfil the conditions referred to in Article 37.1.*b* of the GDPR, as "*IAB Europe is a professional association whose main activities are to provide information and tools to stakeholders (in particular, companies) operating in the digital advertising sector, as well as to provide information to the general public in order to improve their knowledge and to inform them of the value that digital advertising brings to the market*". For these reasons, IAB Europe has not appointed a data protection officer.

63. According to the Inspection Service, the approach of IAB Europe set out above is not supported by the facts. IAB Europe developed and manages the TCF in its capacity as *Managing Organisation* and as such, as well as under the terms and conditions of the IAB

[28] IAB Europe - Response to Belgium DPA, 26 June 2019 (Exhibit 22), p. 2-3.
[29] IAB Europe response to the Inspection Report, 10 February 2020 (Exhibit 57).
[30] In its reply to the Inspection Service dated 26/06/2019 and 20/08/2019, Exhibits 22 and 29.

Europe Transparency & Consent Framework[31], has a right to access and to store and process all information provided by participating organisations.

A.4.3. - Additional considerations that the Inspection Service considers relevant to the assessment of the gravity of the facts

64. The Inspection Service refers to the judgment of the Court of Justice of the European Union (hereinafter "the Court of Justice") in Case C-25/17 (Jehovah's Witnesses)[32], in which the Court clarified that the definition of data controller must be interpreted broadly in order to ensure effective and complete protection of data subjects. In this regard, the Inspection Service argues that IAB Europe is trying to evade its responsibility under the GDPR.

65. The Inspection Service refers to clauses included under Title 10 "*Liability*" of the General Terms and Conditions for the TCF[33], with which IAB Europe places the responsibility for the processing of personal data collected by the parties of the digital advertising sector entirely on the CMPs, publishers and other adtech vendors[34]. Indeed, these clauses expressly state that IAB Europe does not guarantee in any way that:

- the consent given by CMPs or *publishers* to authorised partners (*global adtech vendors*) has been collected and processed in accordance with, inter alia, the GDPR;
- any data processing carried out in connection with, or on account of, the TCF shall comply with all relevant laws and regulations, including the GDPR.

A.5. - Summary of the defendant's response dd. 11 February 2021

A.5.1. - IAB Europe is not a data controller with regard to the processing of personal data in connection with the TCF

66. The defendant refutes the Inspection Service's view that it acts, in its capacity as *Managing Organisation*, as a data controller in respect of the personal data processed by participants in the Transparency and Consent Framework.

67. According to the defendant, the TCF in no way obliges the participating organisations to pursue certain objectives, but merely aims to provide the information, which must be provided to data subjects in accordance with Articles 12 and 13 of the GDPR, in a

[31] Terms and Conditions for the IAB Europe Transparency & Consent Framework ("Terms and Conditions") (Exhibit 33).
[32] CJEU judgment of 10 July 2018, C-25/17, Jehovah's Witnesses, ECLI:EU:C:2018:551.
[33] Terms and Conditions for the IAB Europe Transparency & Consent Framework ("Terms and Conditions") (Exhibit 33).
[34] In particular, the *Supply-Side Platforms*, *Demand-Side Platforms*, *Ad Exchanges*, Advertisers and *Data Management Platforms*.

streamlined and standardised manner by means of the CMPs. In contrast, the actual processing purposes are determined by the participating organisations, without the intervention of the defendant.

68. Firstly, the defendant addresses the lack of legal capacity *(ratione personae*) on the part of the DPA, and more specifically the Inspection Service, to conduct an investigation and to challenge the TCF. The defendant also refers to the DPA's capacity to hold the actual data controllers, i.e. the participants in the TCF, accountable for possible infringements of the GDPR, where necessary.

69. According to the defendant, the TCF as such does not entail any processing of personal data and the Inspection Report does not show for which processing activities IAB Europe should be regarded as the data controller.

70. Secondly, it argues that a broad definition of the concept of a data controller, as proposed by the Inspection Service, is not justified in the context of the TCF, since there are already clearly identified data controllers, on the one hand, and in view of the fact that the TCF has no influence on the processing of personal data that takes place in the context of the OpenRTB protocol, on the other. More specifically, the defendant refers to the lack of any influence on both the means and ends of processing within the RTB system.

71. The defendant also considers that the Jehovah's Witnesses judgment cited above does not apply to the situation of IAB Europe, for the following reasons:

    - Unlike the Jehovah's Witness Community, IAB Europe does not "organise, coordinate or promote" in any way the processing of personal data by TCF participants.
    - The processing of personal data by TCF participants for RTB purposes is not in the interest of IAB Europe.
    - TCF participants have no common purpose in processing personal data and only participate in the TCF with the aim of achieving their individual objectives in a manner that is compliant with the GDPR.

72. The defendant is of the opinion that the *Wirtschaftsakademie*[35] ruling does not apply to IAB Europe either, as the defendant never disseminates information (i.e. advertising) on behalf of or at the behest of advertisers; does not choose an advertising platform or other communication channel; and does not set any parameters or processing purposes, unlike the participants in the TCF who do decide on these matters. According to the defendant, IAB Europe is not actively involved in any RTB processing and it does not initiate such

[35] CJEU judgment of 5 June 2018, C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388.

processing in any way or form. The data processing associated with the OpenRTB system is carried out exclusively by TCF participants and therefore takes place independently of IAB Europe or the TCF.

73. Thirdly, it discusses the definition of a data controller as explained in guidelines issued by the European Data Protection Board (EDPB).[36] The defendant claims that it does not exercise any discretion as to the purposes or means of the processing of personal data within the framework of the TCF. Furthermore, IAB Europe does not process personal data in a way that could be regarded as "inseparable" from, or "inextricably linked" to, the processing of personal data by participants in the TCF. Also, the fact that participating organisations pay a financial fee to IAB Europe does not constitute, according to the defendant, a "mutual benefit" that would lead to a joint processing responsibility.

74. Moreover, the defendant emphasises the lack of decisions or guidelines from other supervisory authorities which could support the Inspection Service's view. In particular, the Belgian, German, French and UK supervisory authorities failed to identify IAB Europe as a (joint) data controller. Specifically, the Conference of Independent Data Protection Authorities of the German Federation and the Länder decided in September 2019 that IAB Europe was acting purely as a representative organisation in the sector of programmatic *advertising*. In addition, the German supervisory authorities confirmed their position in November 2019, when they announced that any enforcement proceedings related to complaints against online advertising should be initiated against TCF participants, but not against IAB Europe. According to the defendant, the French supervisory authority (CNIL) also indirectly accepted the view that IAB Europe was not responsible for the processing operations carried out by participants in the TCF. Also, the UK ICO has allegedly never identified IAB Europe as a potential data controller within the RTB ecosystem at any point.

75. Finally, the defendant refers to the possible consequences for other organisations subject to the GDPR if the Litigation Chamber were to rule that IAB Europe is indeed (co-)responsible for the processing of personal data within the framework of the TCF. In particular, according to the defendant, such a decision would mean that any umbrella organisation which develops and adopts a code of conduct would, merely by virtue of its supervisory role, be deemed to be co-responsible with regard to the processing operations carried out by other organisations in accordance with that code of conduct.

[36] EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021.

A.5.2. - The TCF complies with the GDPR

a. Legality and legal basis

76. First of all, the defendant argues that IAB Europe, unlike the participating organisations, is not at all obliged to explain to the Inspection Service the existence of a legitimate interest, including a balancing of the interests of participating organisations against the rights and freedoms of data subjects, since IAB Europe does not participate in the TCF nor does it act as a data controller.

77. Moreover, the defendant claims that the DPA is not authorised to prohibit participants in the TCF from processing personal data of data subjects on the basis of a legitimate interest. On the contrary, the assessment of the merits of the legitimate interests asserted by the participants must be made on a case-by-case basis, and therefore cannot be prohibited in advance and in absolute terms by the DPA.

78. As regards the allegations that IAB Europe processes special categories of personal data within the framework of the TCF, or is allegedly jointly responsible for the processing of such personal data by the participating organisations, the defendant points out that such categories of personal data may, if necessary, only be processed within the framework of the OpenRTB, as opposed to the TCF. The defendant refers in this regard to the TCF Policies, which expressly prohibit the use of the TCF to process special categories of personal data.

b. Transparency

79. In view of the fact that IAB Europe does not act as a data controller in respect of personal data processed for RTB purposes, the defendant argues that it cannot be expected to inform data subjects in accordance with Articles 12 and 13 of the GDPR either.

80. Moreover, the defendant claims that the privacy policy which the Inspection Service invokes as evidence of possible infringements of the principle of transparency is applicable exclusively to the processing of personal data collected on the various websites operated by the defendant, as well as to the personal data collected in connection with the participating organisations (in particular, the contact details of representatives of those organisations). In other words, the privacy policy to which the Inspection Service refers has no connection whatsoever, according to the defendant, with the processing activities in the context of the OpenRTB system.

81. The defendant also disputes any allegation that IAB Europe, in its capacity as Managing Organisation, reserves the right to access the personal data collected and exchanged by the participating organisations within the framework of the TCF and the OpenRTB system. IAB Europe claims that this assumption is not based on any evidence and is due to an

incorrect interpretation of the possibility offered to the defendant to process personal data of representatives of participating organisations.

82. Moreover, the defendant considers that it is entitled to offer the privacy policy exclusively in English, since the target audience is mainly professional, B2B actors. The defendant points out that Belgian law does not provide for any obligation to make a privacy policy available in French or Dutch and that, moreover, Belgium has failed to make use of the possibility of adopting additional requirements concerning the use of language within the framework of the European Directive on consumer rights[37].

c. Security

83. The defendant claims that the charges concerning the lack of technical and organisational measures to protect personal data in connection with the TCF are unfounded.

84. First of all, the defendant takes the view that IAB Europe is not subject to Articles 24 and 32 of the GDPR in respect of the data processing operations carried out within the TCF, as the organisation is not a data controller.

85. Secondly, the Transparency & Consent Framework Policies provide that participants in the TCF must report infringements of TCF rules to IAB Europe. Again, the defendant claims that the Inspection Service is misinterpreting the TCF Policies, in particular by granting CMPs the right to terminate the cooperation if they consider that a publisher does not comply with the rules, without suffering any contractual disadvantage. In addition, the defendant notes that infringements of the rules provided for in the TCF can always be reported to the supervisory authorities, which will then take action if they deem it necessary.

d. International transfer of personal data

86. IAB Europe refutes the complainants' allegations concerning the international transfer of personal data within the framework of the TCF. The defendant notes in this regard that these allegations are only relevant in the context of the OpenRTB system, which is not at issue in this case. Incidentally, IAB Europe cannot be held responsible for the transfer within the framework of the OpenRTB System.

A.5.3. - IAB Europe is not subject to the obligation to keep a register of processing operations

87. The defendant emphasises that it can invoke the exception provided for in Article 30.5, in particular that the organisation does not have to keep a register of processing activities, as

[37] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304/64.

IAB Europe is not a data controller in respect of the processing activities carried out within the TCF and, moreover, the organisation has fewer than 250 employees. Nevertheless, the defendant emphasises its own initiative in drawing up a register and submitting it to the Inspection Service, as well as the fact that this register does not relate to processing activities relating to the TCF.

A.5.4. - IAB Europe is not required to appoint a data protection officer

88. Having regard to the nature and scope of the processing activities carried out by the organisation, the defendant states that IAB Europe is not required to appoint a data protection officer, since the criteria laid down in Article 37 of the GDPR are not met.

A.5.5. - IAB Europe did cooperate with the Inspection Service

89. The defendant refutes the allegations of insufficient cooperation with the investigation, noting that the time limits imposed by the Inspection Service on parties to an investigation are in no way determined by law, but must be the result of reasonable assessment and must take into account the specific circumstances of the case. *In the present case*, the defendant takes the view that IAB Europe has always cooperated in good faith and provided information and replies in an attempt to clarify its status in relation to the TCF and to demonstrate its compliance with the GDPR, in so far as it applies to IAB Europe.

90. In addition, the defendant observes that the duty of cooperation under Article 31 of the GDPR cannot in any way be construed as an obligation to provide documentation in accordance with provisions of the GDPR which the defendant does not consider to be required.

A.5.6. - There are no aggravating circumstances to the detriment of IAB Europe

91. Finally, IAB Europe disputes the Inspection Service's finding that the defendant's denial that IAB Europe is acting as a data controller, as well as the large volume of both personal data processed and of participating organisations, may be regarded as aggravating circumstances.

92. The defendant refers to the lack of clear evidence in the investigation report that these circumstances are aggravating and concludes that the allegations are due to insufficient knowledge of the operation of the TCF. Consequently, the defendant requests the Litigation Chamber to disregard the opinion of the Inspection Service.

A.6. - Summary of the complainants' reply submissions dd. 18 February 2021

A.6.1. – IAB Europe is data controller for the TCF

a. Processing of personal data within the framework of the TCF

93. The complainants argue that a unique identification number, such as the TC String generated and stored in a cookie, is personal data within the meaning of Article 4(1) of the GDPR, a position which has also been expressly confirmed in case law prior to the GDPR.

94. Moreover, according to the complainants, the TC String is more than just a unique identifier, as IAB Europe allegedly also uses the TC String to collect information regarding which applications a data subject uses and which websites he visits. This could also reveal sensitive data on data subjects within the meaning of Article 9 of the GDPR.

95. Furthermore, the generation of the TC String in itself constitutes, without any doubt, processing of personal data. The issue at hand is the automated creation, by a CMP registered with the TCF, of a unique and linked set of characters intended to capture a specific user's preferences regarding permitted data exchanges with advertisers.

96. The sharing of the TC String with CMPs takes place, according to the complainants, in two ways:

    a. storing the TC String in a shared *globally scoped consent* cookie on the IAB Europe *consensu.org internet domain*; or

    b. storing the TC String in a storage system chosen by the CMP if it is a service-specific permission.

97. According to the complainants, in both cases IAB Europe is the data controller of those processing operations. The intervention of IAB Europe is, moreover, all the more drastic in the hypothesis of the shared *global consent* cookie. Indeed, that shared *globally scoped consent* cookie that stores the TC String points to the "*consensu.org*" domain, managed by IAB Europe, from where CMPs can access and update the shared TC String.

b. IAB acts as data controller for the processing operations within the TCF

98. First of all, the complainants believe that IAB Europe, in its "*Frequently Asked Questions*" about the TCF, explicitly states that it is responsible for the *TCF Policies*.

99. According to the complainants, it goes without saying that the organisation that manages and operates the TCF is also the data controller of this system, including any processing of personal data imposed and organised by the TCF. After all, IAB Europe imposes these personal data processing operations on the other participants in an enforceable manner.

100. Furthermore, IAB Europe requires CMPs to implement the TCF strictly according to its *Technical Specifications*. In the TCF *Technical Specifications*, IAB Europe explains in detail

which personal data must be processed by the participants, for what purposes and by what means.

101. IAB Europe also requires CMPs, in the case of a global consent, to store the character string in a shared *global consent* cookie on the "*consensu.org*" domain. Since this internet domain is registered and managed by IAB Europe, the defendant also has access to the personal data processed in the TCF.

102. Moreover, according to the complainants, IAB Europe determines the so-called "essential means" for the processing of personal data within the TCF. On the one hand, IAB Europe specifies in detail which elements must be included in the TC String. And, on the other hand, IAB Europe determines the categories of recipients of that personal data, as the defendant is responsible, in its own words, for the management of the *Global Vendor List* and the management of the CMPs participating in the TCF.

103. The complainants also believe that TCF does not provide an effective mechanism to enforce certain policies[38], although a code of conduct is intended to be an effective system for compelling its members to comply, as stipulated in Article 41 GDPR.

A.6.2. - The processing operations carried out in the TCF violate the GDPR at various levels

a. Infringement of the principles of purpose, proportionality and necessity

104. According to the complainants, IAB Europe collects users' preferences in the TCF via the TC String for a vague, inaccessible and abusive purpose, while the personal data processed is insufficient and irrelevant for this purpose.

105. Moreover, the processing in itself is alleged to be anything but proportionate, which means that IAB Europe is in breach of Articles 5(1)*(b)* and 5(1)*(c)* of the GDPR, as well as its duty of responsibility as the data controller, laid down in Article 5(2) of the GDPR. Furthermore, the complainants consider that, with the design of the TCF, IAB Europe does not provide the necessary guarantees for compliance with the requirements of the GDPR and for the protection of the rights of data subjects; consequently, the defendant infringes Article 25 GDPR.

The purpose of processing the TC String is neither specified nor explicitly defined for data subjects, nor is it justified

106. According to the complainants, IAB Europe does not provide information to data subjects concerning the processing of their personal data in the TCF.

[38] See para. 133 *et seq*. of this decision.

107. The purpose of the TC String within the overall purpose of the TCF is to capture the information provided to users and their processing preferences. In other words, IAB Europe does process personal data (in particular the TC String) within the TCF because it claims this could bring the underlying marketing-related processing in line with the GDPR. According to the complainants, it is therefore this purpose that must be assessed in terms of its lawfulness, and in the light of this purpose, the proportionality and necessity of the TC String's processing within the TCF must be assessed.

The TC String is inadequate and not relevant for the intended purpose

108. The complainants further argue that the TC String's processing operations within the TCF are insufficient and not relevant to ensure compliance with the GDPR when personal data are processed through the OpenRTB system.

109. The OpenRTB system contains an inherent security problem that makes it impossible for a system such as the TCF to guarantee, among other things, the necessary transparency and accountability with regard to personal data, including special categories of personal data, processed in a bid request after the bid request has been sent out.

110. The central idea behind the TCF is that participants collect user preferences and transmit them in the form of the TC String, so that other participants take note of the content (i.e. read the TCF signal) and can therefore respect the user preferences. However, according to the complainants, there is nothing in the TCF, or in any related system or mechanism, that actually ensures that participants in the OpenRTB system are bound by the TCF signal. The TCF signal is therefore no more than a mere notification.

111. Given the inherently unlawful nature of processing personal data in the OpenRTB system, on the one hand, and the inherently imperfect nature of a purely signal-based system such as the TCF without effective control, on the other, the use of the TCF, including the processing of the TC String, can never give participants the assurance of being in compliance with the GDPR. After all, the TCF offers no guarantee whatsoever that TCF participants will comply with their accountability obligations (Article 5.2 of the GDPR). Nor can it provide adequate protection for the personal data shared through the OpenRTB system (Article 5.1.*f* GDPR).

IAB Europe set up the TCF in such a way that data protection by design is not guaranteed

112. The complainants argue that the design of the TCF, due to its disproportionate nature, cannot guarantee the level of data protection required under Article 25 GDPR, in particular in view of the obligation arising from Article 25 GDPR to implement appropriate technical and organisational measures to ensure that, in principle, only personal data that are necessary for each specific purpose of the processing are processed.

113. The processing of personal data within the TCF, in particular the TC String, is therefore not necessary for the specific purpose as, according to the complainants, that purpose cannot and will not be achieved in any case.

114. Moreover, the complainants argue that the TC String, as an independent personal data that uniquely identifies users, is shared with numerous participants through various mechanisms, including through IAB Europe's own mechanism of the shared *global consent* cookie on its "*consensu.org*" internet domain.

b. Infringement of the principles of fair, lawful and transparent processing (Articles 5, 6, 12, 13 and 14 GDPR)

115. The complainants allege that data subjects are not informed in any way of the fact that their personal data (including the TC String) are systematically and widely processed by IAB Europe within the TCF.

116. According to the complainants, the processing of the personal data of the complainants and other data subjects by IAB in the TCF is after all:

- anything but lawful as there is no legal basis;
- neither proper nor transparent, as it takes place entirely "behind the backs" of those affected, without any form of notification.

IAB Europe's processing operations lack a legal basis and are therefore unlawful

117. IAB Europe cannot rely on the consent of data subjects (Article 6.1.*a* GDPR), according to the complainants, as it never sought or obtained such consent. Also nowhere in the *TCF Policies*, *Technical Specifications* or General Terms and Conditions is a mechanism cited whereby IAB Europe would ask data subjects for permission to generate a unique identifying string of characters that shares their privacy preferences with a mass of recipients, even in cases where those data subjects indicate in a CMP that they do not wish to share personal data with anyone.

118. According to the complainants, IAB Europe also cannot invoke the necessity of the processing of the TC String within the TCF for the performance of a contract with the complainants and other data subjects (Article 6.1.*b*), as there is no contract between data subjects and IAB Europe.

119. Furthermore, the complainants argue that the defendant may also not rely on the necessity of the processing of the TC String within the TCF to serve its legitimate interests, or those of a third party (Article 6.1.*f* GDPR). The required balancing of interests would always be in favour of those affected.

120. First of all, the processing of the TC String does not benefit the data subjects in any way as the TCF is not able to guarantee security, accountability or transparency. Moreover, there

is no legitimate interest, as this interest is not sufficiently clearly articulated anywhere, and it is not possible to balance it against the interests and fundamental rights of the data subjects.

121. Secondly, in balancing the interests, the data controller must in principle take into account several factors: the effects of the processing on the data subject, the nature of the personal data processed, the way in which these personal data are processed, the data subject's reasonable expectations, and the status of the data controller and the data subject.

122. According to the complainants, the consequences of the processing of the TC String are particularly far-reaching for those involved. IAB Europe's processing operations would lead TCF participants to assume that they are correctly informing data subjects about the processing of personal data through the OpenRTB system, but this is not the case. This would then lead to the unlawful sharing and distribution of personal data, even sensitive personal data, on an immense scale via the OpenRTB system.

123. IAB Europe's processing of the TC String would result in a unique online identifier being shared with untold numbers of parties, similar to what happens with unique identifiers in advertising cookies from large advertising companies. It would therefore allow easy tracking of users across the web and across devices ("*web and cross-device tracking*"). Moreover, the complainants argue that the TC String can be combined with the data distributed via the OpenRTB system, because the TC String is integrated in a *bid request*.

124. Given the lack of information for data subjects about the processing operations within the TCF and the unrestricted sharing of the TC String with an almost unlimited group of recipients, it is clear to the complainants that these processing operations are beyond the scope of the data subjects' reasonable expectations. Furthermore, data subjects such as the complainants do not expect that the processing of personal data within the TCF will result in their, sometimes sensitive, personal data and detailed profiles being shared with numerous companies through the OpenRTB system without any real and effective control over what those companies will do with the personal data obtained.

125. The complainants in this case are natural persons and interest groups representing the data protection interests of natural persons. They have no control over the processing of personal data within a TCF (which happens anyway, regardless of whether consent is given or refused in a CMP). Nor do they have control over what happens to their personal data shared through the OpenRTB system. According to the complainants, those involved cannot verify whether participants in OpenRTB actually comply with the rules of the TCF.

IAB Europe processes personal data in the TCF covertly without any form of notification and the processing is therefore neither proper nor transparent

126. Despite the extensive documentation that IAB Europe makes available to TCF participants on its website, nowhere does it state that the TCF itself also involves the processing of personal data, according to the complainants. Moreover, the documentation expressly disregards, with regard to TCF participants, that the TCF itself involves the processing of personal data.

127. The TCF Implementation Guidelines seems to suggest that there are hypotheses in which participation in a TCF does not involve the processing of personal data. After all, advertisers and DSPs, who already participate in the TCF, are told that they should register as *vendors* if they process personal data. According to the complainants, this implies that they would not have to do so if they were not processing personal data. However, the latter situation is entirely impossible, according to the complainants, as the TCF inherently requires the processing of personal data.

128. According to the complainants, the statements in the IAB Europe guidelines are misleading for the hundreds of *adtech vendors* who use TCF. Because IAB Europe does not inform TCF participants about the processing of personal data necessarily entailed by the implementation of a TCF, none of these participants knows or realises that they have a transparency obligation. In this way, data subjects - such as the complainants - are not informed by any participant of the processing of personal data within TCF.

129. IAB Europe does also not comply with its own transparency obligation. Neither on its own website nor in other sources does the defendant communicate the information required by Articles 13 and 14 to those concerned, such as the complainants. This would include the following information: that IAB Europe is the data controller of the TCF and its contact details; the contact details of its data protection officer; what its processing purposes are and the legal basis for the processing; which categories of personal data it processes (in particular the TC String); who receives the personal data (these are already at least all participants in the TCF who receive the TC String); that IAB Europe intends to transfer the personal data to recipients in third countries; how long the personal data are retained; what its legitimate interests for processing are; what the rights of the data subjects are; that data subjects may lodge a complaint with the DPA; that data subjects may withdraw their given consents; and finally, what the source of the personal data is.

130. At the same time, IAB Europe cannot invoke any of the exceptions provided for in Article 14.5 of the GDPR in order not to have to provide this information, as:

    a. the data subjects are not yet in possession of the information, since the processing in respect of them has so far been carried out in secret (Article 14.5.*a* GDPR);

b. it is not impossible nor does it require a disproportionate effort to make this information known to the data subjects, given the influence that IAB Europe exercises over the operation of the TCF (Article 14.5.*b* GDPR);

c. the acquisition of these data is not prescribed by law (Article 14.5.*c of* the GDPR); and

d. the personal data need not remain confidential for reasons of professional secrecy (Article 14.5.*d* GDPR).

IAB Europe's reference to the Vectaury case in France does not hold water

131. According to the complainants, IAB Europe wrongly believes that it can rely on the decision of the French supervisory authority CNIL in the Vectaury case. Indeed, IAB Europe wrongly claims that it would be strange for the Inspection Service to find infringements related to the processing of personal data in the TCF, while the CNIL is alleged to have no problems with the legitimacy of these processing operations. The complainants argue that IAB Europe is making assumptions here and reaching conclusions that cannot be deduced from the Vectaury case at all:

- Firstly, the Vectaury case was about the specific implementation of a CMP by Vectaury whereby the TCF would have been implemented. The role of IAB Europe was not the subject of those proceedings and CNIL therefore did not rule on, nor investigate, the role of IAB Europe in providing the TCF.
- Secondly, that case specifically concerned whether Vectaury's implementation of the TCF could bring the underlying processing of real-time bidding systems in line with the GDPR. The CNIL's verdict was clearly negative, as shown by the fact Vectaury itself states on its website that it has created a completely new method in dialogue with the CNIL. According to the complainants, it is therefore misleading of IAB Europe to claim that the CNIL has legitimised the TCF in itself as being sufficient to bring real-time bidding systems into compliance with the GDPR.
- Thirdly, the complainants argue that the CNIL investigation did not focus on the legitimacy of the processing of personal data within the TCF. The CNIL did not look at the generation and distribution of the TC String as a stand-alone processing and therefore did not make any statement about it.

132. According to the complainants, the CNIL's decisions in the Vectaury case are therefore irrelevant, as it was a clearly different case, directed against a different party, involving different processing operations and under legislation that has since been replaced. The Litigation Chamber follows the position of the complainants and does not discuss the Vectaury case, which concerns a different case than the present one.

c. Infringement of the principles of integrity and confidentiality (Articles 5.1.*f* and 32 of the GDPR)

133. According to the complainants, IAB Europe violates the integrity and confidentiality obligations of the GDPR because it facilitates the exchange of personal data in the TCF, in particular the exchange of the TC String, with numerous parties, without verifying whether all recipients of this personal data comply with the rules of the GDPR.

134. It is certain that the TC String is shared with thousands of companies. The TC String must therefore be protected by appropriate measures in accordance with Articles 5.1.*f* et 32 GDPR. However, IAB Europe has not built in an appropriate protection mechanism: As with all other processing in the OpenRTB system, there is no way to verify that recipients are effectively processing the TC String in accordance with the GDPR. Indeed, none of the mechanisms presented by IAB Europe is based on real, proactive control of TCF compliance, the complainants argue.

135. The complainants dispute IAB Europe's argument that it has no obligation to enforce the TCF, and in particular the agreements made within the TCF. The complainants argue that it is indeed its obligation as a data controller to enforce the agreements within the TCF and, at least in this way, to provide certain guarantees for the secure processing of the TC String.

136. Secondly, the complainants point to claims by IAB Europe that, as a management organisation, it makes "substantial efforts" to enforce the agreements within the TCF. According to the complainants, there is no evidence of these alleged "substantial efforts". They further argue that IAB Europe would have to verify each registered TCF participant's compliance with all agreements, which given the scale of data processing would imply a huge investigation. Moreover, the complainants refer to the answer given by IAB Europe itself to the Inspection Service: "*The reporting obligation itself is not currently monitored. Moreover, it is difficult to monitor it because it would be difficult for IAB Europe to establish whether or not or when a CMP had (or should have had) a "reasonable belief" that another party was not complying*" [39].

137. Thirdly, the complainants believe that IAB Europe is wrong to try to hide behind the contractual arrangements. According to the complainants, the defendant claims that it is sufficient that participants are contractually obliged to report any non-conformity to IAB Europe.

138. The complainants also argue that IAB Europe, as the data controller of the TCF, is bound by Articles 5.1.*f* and 32 of the GDPR, although it is practically impossible to guarantee the security of the processed TC String when it is shared with thousands of recipient

[39] Letter from IAB Europe to the Inspection Service of 10 February 2020, p. 8.

companies. According to the complainants, the latter would mean that IAB Europe actively checks that all recipients of the TC String always comply with the obligations of the GDPR so that the processing of the received TC String would not be unlawful.

139. Moreover, according to the complainants, practice proves that almost all participants in the TCF unlawfully process the TC String, as not one CMP, not one publisher and not one vendor provide information on the processing of the TC String, its purpose, legal basis or the categories of recipients. This would imply, according to the complainants, that the transfer of the TC String to these parties is inherently a personal data breach which, given its immense scale, gives rise to an obligation to report to the supervisory authorities.

140. The practical impossibility of providing the necessary safeguards for the protection of the personal data (in particular the TC String) of data subjects, when shared with thousands of recipients within the OpenRTB system, shows, according to the complainants, that IAB Europe is in breach of its obligations under Articles 5.1.*f* and 32 GDPR.

d. The systematic transfer of the TC String to third countries without adequate protection (breach of Article 44 of the GDPR)

141. The complainants argue that IAB Europe has set up the TCF in such a way that personal data — including the TC String, because it is integrated into the *bid requests* — is structurally transferred in the context of OpenRTB to numerous companies outside the European Economic Area (EEA), without adequate protection being provided for these transfers.

142. The complainants refer to the Ad Exchange Xandr (based in the USA), which is affiliated to IAB Europe's TCF and therefore receives at least the TC String from EEA users, including the complainants. As data controller for the processing of personal data in the TCF, IAB Europe should provide a mechanism for the transfer of personal data so that Ad Exchanges established outside the EEA may receive the TC String.

143. Exchanges of the TC String via real-time bidding systems such as OpenRTB are structural in nature and repeat themselves continuously in fractions of seconds. After all, the TC String is sent along with the *bid requests*. This would make it impossible for IAB Europe, according to the complainants, to invoke any of the exceptions in Article 49 GDPR.

144. Appropriate safeguards would be the only way for IAB Europe to organise transfers of personal data in the TCF. However, at present IAB Europe does not provide any form of appropriate safeguards for the transfer of the TC String through real-time bidding systems such as OpenRTB.

145. In line with the Schrems II judgment, IAB Europe,[40] in addition to selecting a form of adequate safeguards, should also have taken additional measures to prevent personal data from being processed in a non-compliant manner in third countries. However, these additional measures are just as lacking as appropriate safeguards. The TC String is shared in a blind manner with an indefinite number of participants in the OpenRTB system, wherever in the world they may be located.

A.7. - Summary of the defendant's rejoinder dd. 25 March 2021

A.7.1. - Organisations that process personal data within the RTB system are responsible for complying with the GDPR and the ePrivacy Directive

146. The defendant first argues that any party participating in RTB and using the OpenRTB specification can intervene in the technical storage and/or access operations on a user's device (e.g. the placing of website cookies) under the ePrivacy Directive, and/or act as a data controller or processor of personal data (e.g. for digital advertising purposes) under the GDPR. Where appropriate, all of these parties are responsible for complying with their obligations under the GDPR and the ePrivacy Directive when engaging in RTB.

147. In addition, according to the defendant, there are thousands of companies engaged in RTB and using the OpenRTB specification, which, however, do not participate in the TCF. Similarly, parties may use the TCF for purposes other than RTB. IAB Europe also stresses that publishers can use the TCF for a range of online advertising scenarios other than the OpenRTB specification - including other types of RTB protocols, but also online advertising that does not involve RTB at all, such as the direct sale of advertising inventory.

148. The defendant also refutes the complainants' allegations that RTB is inherently illegal by referring to the UK supervisory authority's (ICO) report which merely stated that RTB "requires organisations to take responsibility for their own data processing, and that the industry is collectively reforming RTB". The ICO is also said to have highlighted the good faith efforts of stakeholders such as IAB UK to contribute to this reform process in a more recent publication[41].

149. Furthermore, the defendant states that several supervisory authorities have called for ways to increase transparency for data subjects by clearly identifying the data controllers with whom personal data will be shared, by specifying the processing purposes and by enabling

[40] CJEU judgment of 16 July 2020, C-311/18, *Facebook Ireland and Schrems*, ECLI:EU:C:2020:559.

[41] Information Commissioner's Office – Adtech - the reform of real time bidding has started and will continue, 17 January 2020, https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/.

data subjects to exercise control over their personal data. It is precisely this kind of transparency measure that IAB Europe and the TCF aim to support.

150. Within the framework of the TCF, data subjects are given the opportunity to give their prior approval to a number of identified third parties *(adtech vendors*) and processing purposes. According to IAB Europe, this transparency and prior checking is an appropriate substitute, from a legal compliance perspective, for *real-time*, *on-the-fly*, one-by-one consent for access, storage and data processing by data controllers.

A.7.2. - IAB Europe cannot be held responsible for the alleged illegal practices of RTB participants, as the TCF is completely separate from RTB

151. The defendant emphasises that the TCF is only one of many optional approaches that data controllers may choose to help ensure compliance with transparency and consent requirements when processing personal data for RTB or other advertising purposes. Consequently, the responsibility for compliance and for the actual decisions on the purposes and means of these personal data processing operations lies entirely with the parties engaged in RTB, and not with IAB Europe.

152. The defendant also states that IAB Europe had contact with several supervisory authorities after the roll-out of the first version of the TCF, as well as with several *publishers*. Following these discussions, the second version of the TCF was developed, in which several processing purposes were bundled under one title in so-called "stacks", and the legitimate interest was introduced as a possible legal basis. Furthermore, the TCF v2 introduces additional purposes and "*publisher controls*" that allow publishers to restrict access to a particular purpose to a subset of *adtech vendors*.

153. Finally, the defendant clarifies that IAB Europe has always intended to have the TCF adopted as a transnational code of conduct.

154. In its initial submission, the defendant puts forward procedural arguments concerning the competence of the DPA and the way in which the complaints and the investigation were handled. These defences are set out below in Section A.9.

155. In its summary submission, the defendant also claims that the manner in which the DPA conducted the proceedings does not comply with Article 57 of the GDPR. However, since the complainants were unable to respond, the debates were reopened at the request of the Litigation Chamber.

A.8. - Hearing and reopening of debates

156. In accordance with Article 51 of the Rules of Procedure of the Data Protection Authority, a hearing was organised, to which all parties shall be invited. The hearing took place on 11 June 2021.

157. An official report of the hearing was drawn up in order to give details and additional information which were made during the hearing, without repeating the elements set out in the submission. The parties were also given the opportunity to submit their written comments on the record. A number of elements mentioned below are relevant to the present decision.

158. In the context of the hearing, the Inspection Service first confirmed its position that IAB Europe acts as a data controller for the processing of personal data under the Transparency and Consent Framework (hereinafter "TCF"), but not for OpenRTB.

159. The Inspection Service also clarified that personal data is collected as provided for in the *TCF Policies*, in the *Terms and Conditions*[42] and in the privacy policy, as well as in the context of the TC String values stored in a *euconsent-v2* cookie, the latter as an expression of a user's preferences must also be regarded as personal data. The Inspection Service also emphasises that the TC String as such does not contain any information relating directly or indirectly to the taxonomy of the website to which the TC String refers. This last aspect concerns an essential distinction between the preferences of the user that are collected in the context of the TCF, and the personal data of that same user that are collected and distributed within the OpenRTB system. In conclusion, the Inspection Service states that the TC String values and the *euconsent-v2* cookie do not in themselves allow the identification of an individual user. Although both elements contain personal data, in the sense that the information relates to one natural person, the Inspection Service also confirms that it is not possible to identify the specific data subject on the basis of that information alone.

160. During the hearing, the defendant raised a procedural point, namely that the Litigation Chamber is not permitted to rule on the complainants' submission before an analysis has been carried out on the consistency of their written submissions in comparison with the complaints. The defendant also requests that the Litigation Chamber rule on the necessity of requesting a supplementary investigation by the Inspection Service, as allegedly required by Article 57.1.*f* GDPR. The Litigation Chamber will decide on this procedural point in the present decision[43].

---

[42] Terms and Conditions for the IAB Europe Transparency & Consent Framework ("Terms and Conditions") (Exhibit 33), p. 7.
[43] See para. 174 *et seq*. of this decision.

161. The complainants responded orally to the defendant's procedural arguments during the hearing.

162. With regard to the timing of the TC String generation, the defendant emphasises that the capture of the exact creation time cannot lead to the uniqueness of a TC String, as there is a chance that two unidentified users may give the same preferences at the same time. Moreover, this timestamp alone is not sufficient to speak of a unique string, since the values of the TC String are not persistent and may vary over time or according to the visited websites.

163. The defendant also states that the *global consent* cookies scenario, in which the preferences stored in one TC String apply across several websites, is not relevant in view of the limited scope at the time of the hearing[44], as well as the intention of IAB Europe, as a result of the finding that a global consent does not meet the requirement of a specific consent[45], to stop supporting this functionality and to phase it out in the weeks following the hearing.

164. As regards the question whether the allocation of a subdomain of *consensu.org* to CMP by means of a DNS delegation can be regarded as a determination of the means of processing, the defendant submits that, as a result of the DNS delegation, each subdomain refers to servers of the CMPs, which are moreover the only ones able to read the TC Strings from the users' devices. In addition, the defendant submits that the registration of a subdomain of *consensu.org* is purely optional and, as such, does not constitute an essential means of processing.

165. The complainants emphasise, on the other hand, that a DNS delegation can always be reversed by the defendant, and that it is irrelevant that the defendant does not have access to the *euconsent-v2* cookies. The complainants also point out that the DNS delegation can be regarded as an essential means of processing, since the DNS delegation is used to distribute the TC String further through the TCF ecosystem.

166. Concerning the existence of interfaces between the TCF and OpenRTB, the complainants stress that both systems are inherently intertwined because of the link between, on the one hand, the TC String that the CMPs generate according to the instructions of the TCF and, on the other hand, *bid requests*, which are regulated by the OpenRTB. In other words, the latter are used as vehicles to spread the TC String throughout the OpenRTB ecosystem.

---

[44] According to the defendant, the number of globally scoped consents was at most 0.5% of all consent and preferences collected worldwide.

[45] Article 4.11 GDPR: "consent" of the data subject means any freely given specific, informed and unambiguous expression of will by which the data subject accepts, by declaration or unambiguous active act, the processing of personal data relating to him or her.

167. The defendant states that both systems can function independently and that the TCF was developed with OpenRTB as a starting point and could be used in that context, as OpenRTB is the most widely used standard in the industry. According to the defendant, this does not mean that the TCF is an essential means of using OpenRTB.

168. The defendant argues that the elaboration by the defendant of a future Code of Conduct in relation to the TCF cannot be regarded as proof of its (shared) responsibility for the processing of personal data in the context of the TCF. Complainants add that it is impossible to verify compliance with the GDPR by participating organisations, even if the rules are clearly defined in an enforcement policy.

169. In this regard, the defendant refers to the development and gradual implementation of automated compliance programmes to monitor the extent to which CMPs and advertisers (as well as other *adtech vendors*) comply with the TCF Policies, including future internal audits of the processes at the aforementioned parties. The defendant also emphasises that the TCF already provides for sanctioning measures against *adtech vendors* that do not adhere to the framework, such as temporary suspensions of their participation in the TCF.

170. With regard to the link between the TC String and the individual user, the defendant takes the view that the TCF does not determine how this is done, nor how the TC String is subsequently communicated to the *adtech vendors*, as these elements are entirely subject to the OpenRTB specification.

171. The defendant clarifies that the use of the *consensu.org* domain is purely optional, and moreover, this domain was not developed for the purpose of processing or storing logs related to the TC Strings.

172. Finally, the defendant emphasises its position that the TC String only constitutes personal data after it has been linked in the context of the OpenRTB to a *bid request* which already contains personal data.

173. On 9 August 2021, after deliberation, the Litigation Chamber decides to reopen the debates on specific procedural arguments of IAB Europe.

174. On 23 August 2021, the Litigation Chamber received the first submissions from the defendant. The defendant states that the DPA infringed Article 57.1.*a* and 57.1.*f* GDPR and Article 94(3) DPA Act. The DPA also allegedly failed to comply with the principle of sound administration and the defendant's rights of defence.

175. With regard to Article 57.1.*f* GDPR, the defendant first of all claims that the complainants have submitted new allegations in their submission, which are thus more extensive than the original complaints. Moreover, according to the defendant, the DPA did not proactively investigate these new allegations by charging the Inspection Service with a new or

supplementary investigation. As a result, the defendant considers that the DPA has failed to fulfil its duties under Article 57.1.*f* GDPR.

176. Furthermore, the defendant claims that, by requesting an initial investigation from the Inspection Service, the Litigation Chamber has *de facto* bound itself to a procedure in which every allegation or defence must be investigated by the Inspection Service. According to the defendant, the decision of the Litigation Chamber not to request a supplementary investigation after an initial investigation and the submission of the defences led to an infringement of Article 94(3) DPA Act.

177. The defendant also states that, in the absence of an investigation by the Inspection Service into supposed new allegations in the complainants' defences and a legal classification of those allegations, it was unable to defend itself adequately against the complaints made against IAB Europe. Thus, the procedure before the Litigation Chamber could be considered to have evolved from an *inquisitorial* to an *adversarial* procedure in which the Litigation Chamber would no longer have acted as an administrative dispute resolution body, taking mainly into account the claims and documents of the complainants, with the result that the rights of defence of IAB Europe have been violated, according to the defendant.

178. On 6 September 2021, the Litigation Chamber received the complainants' submission. The complainants consider, first of all, that the defendant's new pleas exceeded the limited scope of the reopened debates.

179. Secondly, the complainants argue that the nature of the proceedings has not changed in any way, as the proceedings were started because of complaints made to the DPA, in other words, as an *adversarial* procedure, and have remained so throughout.

180. Thirdly, the complainants refer to Articles 63(2) and 94 DPA Act, as a counter-argument to the assertion that the Litigation Chamber should have had the Inspection Service examine each of the pleas raised by the complainants. After all, these provisions provide the Litigation Chamber with a discretionary power to decide whether or not an (additional) investigation by the Inspection Service is necessary.

181. Furthermore, the complainants argue that it is impossible for the Litigation Chamber to have an investigation or supplementary investigation carried out by the Inspection Service after the parties' submissions and exhibits, taking into account the time limit of 30 days after, respectively, the referral to the Litigation Chamber by the First Line Service following the lodging of the complaint, or the Litigation Chamber's reception of the Inspection Service's initial investigation report, under Article 96 of the DPA Law.

182. With regard to the defendant's argument that the way the Litigation Chamber handled the case violates Article 57.1.*f* GDPR, the complainants point out that, first of all, this provision has no direct effect in the sense that the defendant can derive rights from it. The complainants also argue that this provision cannot affect the internal structure and

functioning of the supervisory authorities, which, with regard to the DPA and, more specifically, the division of powers between its Inspection Service and its Litigation Chamber, are subject to Belgian administrative (procedural) law.

183. Furthermore, the complainants state that Article 57.1.*f* GDPR does not refer to an obligation on the part of the Litigation Chamber to request an investigation by the Inspection Service into the complaints, but to the power of the supervisory authorities to close the case.

184. In addition, the complainants argue that the decision of the Litigation Chamber to request an investigation from the Inspection Service in no way prevents it from relying on the submissions and exhibits submitted by the parties, contrary to the defendant's position.

185. As regards the defendant's alleged failure to comply with the principle of due care, the complainants submit that the Litigation Chamber is required under that principle to study properly all the exhibits in the file so that its decision is based on a correct and complete presentation of the facts. However, this principle again does not imply in any way that the Litigation Chamber must have a (supplementary) investigation carried out by the Inspection Service for every exhibit.

186. As regards the defendant's rights of defence, the complainants maintain that, on the basis of the Inspection Service's various investigative reports and the submissions and exhibits submitted by the complainants, the defendant was adequately informed of the alleged facts and infringements of law. Also, according to the complainants, the defendant was given sufficient opportunity to defend itself in writing against the legal and factual allegations made by the complainants, given that the defendant was offered two rounds of submissions.

187. Finally, the complainants refer to the lack of concrete examples, in the defendant's latest submissions, of alleged new allegations on which the defendant was unable to conclude or which were not investigated by the Inspection Service.

188. On 13 September 2021, the Litigation Chamber received the defendant's response.

189. According to the defendant, only the inspection report determines the extent of the allegations, provided that the inspection report is meaningful and based on a comprehensive examination of the facts. Furthermore, the defendant submits that the decision of the Litigation Chamber to request an investigation by the Inspection Service has resulted in the procedure as a whole becoming an "*inquisitorial*" procedure, irrespective of whether the procedure has its origin in the complaints filed with the DPA. According to the defendant, the decision of the Litigation Chamber not to subsequently request a supplementary investigation and to base the further proceedings solely on the parties' submissions and exhibits amounts to a breach of its rights of defence.

190. In addition, the defendant is of the opinion that the period of thirty days provided for in Article 96(1) DPA Act does not apply to the request by the Litigation Chamber to have a supplementary investigation carried out by the Inspection Service.

191. The defendant bases that reasoning on the distinction made in general administrative law between expiry periods and periods of order. In particular, the defendant takes the view that, in the absence of formal provisions in the DPA Act to the effect that exceeding the 30-day time limit results in a loss of jurisdiction for the Litigation Chamber, the time limits provided for in Article 96 must be complied with, although not on pain of invalidity of the decision rendered too late. According to the defendant, the Litigation Chamber therefore remains competent to make a decision for supplementary investigation even after the expiry of the 30-day period of order. That interpretation, the defendant argues, is in fact the result of the greater importance of the right to a defence over the right to expeditious proceedings before the Litigation Chamber.

192. As regards the direct effect of Article 57.1.*f* GDPR, the defendant submits that the existence of a margin of appreciation for the Member States does not exclude the direct effect of a provision, but implies an examination of whether that provision is intended to provide a guarantee for the parties. The defendant takes the view that Article 57.1.*f* GDPR fulfils this requirement and clarifies that its argument for requesting an supplementary investigation is furthermore limited to an assessment in fact and in law of the supporting points in the proceedings.

193. In conclusion, the defendant states that it has not received a clear statement of the nature and scope of the charges, except for the allegations made in the complainants' defences. In that regard, the defendant submits that the technical inspection reports contain merely technical descriptions, in which, moreover, the TC String is not mentioned anywhere. In Section A.9. - Procedural objections raised by the defendant, the Litigation Chamber will demonstrate why the procedural rights, including those relating to the specificity of the charges, were sufficiently respected.

A.9. - Procedural objections raised by the defendant

A.9.1. - Infringements of procedural rules applicable to the inspection report and of fundamental rights and freedoms of IAB Europe

a. Inadmissibility of the complaints

194. The defendant first of all argues that some of the complaints were filed in English and therefore do not meet the formal admissibility requirements set out in Article 60 DPA Act.

195. In addition, the defendant takes the view that some of those filing the complaints cannot be regarded either as "complainants" or as "parties" within the meaning of Articles 93, 95, 98 and 99 DPA Act, with the result that their submissions must be excluded from the debates and cannot be taken into account.

196. Finally, the defendant asserts that the measures that the DPA can impose under Article 100 of the DPA Act do not provide any benefit to these complainants.

197. IAB Europe thus considers that the case was unlawfully initiated - in particular on the basis of several inadmissible complaints - with the result that the claims against IAB Europe must be rejected and cannot lead to the imposition of a valid sanction or corrective measure on IAB Europe.

Position of the Litigation Chamber

198. The Litigation Chamber refers to Article 77.1 of the GDPR, according to which data subjects have the right to lodge a complaint in the Member State where they usually reside, have their place of work or where the alleged infringement was committed. The four complaints in English referred to by the defendant were not lodged directly with the DPA, but with the national supervisors with jurisdiction for each of the complainants, in accordance with the locally applicable language legislation. *In casu*, the four complaints have been filed respectively with the Polish supervisory authority, with the Slovenian SA, with the Italian SA as well as with the Spanish SA, which then referred these complaints to the Belgian DPA as the lead supervisory authority, in accordance with the cooperation procedure provided for under Article 56 GDPR.

199. The formal admissibility requirements provided for under Article 58 DPA Act, and more specifically the requirement that a complaint be drawn up in one of the national languages, only apply to complaints filed directly with the DPA. Any other view would erode the effective operation of the right to complain, one of the core elements of the GDPR. Indeed, a complainant who submits his complaint to an authority of a Member State cannot be expected to submit it in the language of the Member State of the lead authority, if that is different from the authority to which he submits his complaint. It follows that the four complaints in question were validly filed with the DPA.

200. In relation to the lack of interest of *Fundacja Panoptykon*, as well as other complainants, in the complaints lodged through the European "one-stop shop" mechanism, raised by the defendant, the Litigation Chamber notes that *Fundacja Panoptykon* lodged the complaint with the Polish supervisory authority on behalf of Ms Katarzyna Szymielewicz in accordance with Article 80.1 GDPR. On the basis of this provision, the complainant has the right to instruct *Fundacja Panoptykon* to lodge the complaint on its behalf.

201. The Litigation Chamber notes that IAB Europe does not explain at all why *Fundacja Panoptykon* should not be considered a complainant and party here. In addition, in the absence of doubts whether the other complaints were admissible, the argument by the defendant would not make any difference towards the outcome of this decision.

202. This argument must therefore be rejected.

b. The inspection report is not properly reasoned

203. The defendant then goes on to address the inadequate reasoning in the inspection report. As a result of the lack of a clearly worded statement of reasons in the inspection report - including the lack of a clearly identified data controller in connection with a clearly defined data processing activity - the defendant argues that the inspection report not only infringes the DPA's obligation to provide express and sufficient reasons for its decisions, but also constitutes a clear breach of IAB Europe's rights of defence. Consequently, the inspection report infringes IAB's rights of defence as laid down in Article 6 ECHR and Article 47 of the Charter of Fundamental Rights.

Position of the Litigation Chamber

204. IAB Europe's claim that the Inspection Service's report of 13 July 2020 is not sufficiently reasoned is incorrect. As can also be seen from the reflection of this Inspection Report in this decision, the Inspection Report contains detailed reasoning.

205. Furthermore, IAB Europe overlooks the fact that, in addition to the report of 13 July 2020, the Inspection Service produced other very extensive and detailed technical reports (Exhibits 24 and 53). Finally, the Litigation Chamber points to the extensive written and oral exchange of views between the parties before its Chamber. IAB Europe's simple assertion of failure to respect its rights of defence is therefore without merit, as set out in the following paragraphs.

c. Incompleteness and bias of the inspection report

206. The defendant refers to Article 58.4 GDPR, which provides that the procedure before the DPA must be conducted in compliance with "*appropriate safeguards, including* [...] *the due process of law*". According to the defendant, that principle applies equally to the investigation carried out by the Inspection Service and to the findings set out in the inspection report.

207. Referring to the similarities with the role and duties of a prosecutor in ordinary criminal proceedings, the defendant claims that the basic principles of loyalty, impartiality and independence also apply to the Inspection Service. The defendant refers to Section IV of its submission and considers that relevant exculpatory elements, of which the Inspection Service was or should have been aware, are missing from the inspection report.

208. The defendant, emphasising that the DPA is obliged to maintain the presumption of innocence of a defendant at all times, including during the investigative phase of proceedings which may lead to penalties of a criminal nature within the meaning of Article 6 ECHR, considers that its presumption of innocence has been infringed and that the claims against IAB Europe must therefore be dismissed.

Position of the Litigation Chamber

As regards the autonomy of the Litigation Chamber from the other bodies of the DPA, including the Inspection Service

209. The Litigation Chamber first notes that the defendant seems to confuse the role and prerogatives of the Litigation Chamber with those of the other bodies of the DPA.

210. As indicated above, the Litigation Chamber is the administrative disputes body of the DPA pursuant to Article 33(1) DPA Act. The provisions governing the procedure before the Litigation Chamber (see Articles 92 to 100 DPA Act) do not show that it is in any way bound by the findings of any other body of the DPA. Consequently, the Litigation Chamber is not bound by the findings of the Inspection Service.

211. It is also recalled that the Inspection Service submitted not one but several detailed and technical reports clearly setting out the deficiencies attributable to the defendant and substantiating its position with the help of legislative, jurisprudential and factual sources, as the complainants point out. The defendant had access to those reports. Moreover, the defendant responded in detail to the reports of the Inspection Service.

212. The defendant further submits that the Inspection Service's report of 13 July 2020 is not exculpatory, but merely incriminating, because the report does not contain "certain exculpatory elements" of IAB Europe. The defendant also refers, without further specification, to Section IV of its submission, in which it sets out its arguments on the merits. In the absence of more detailed information on the exculpatory elements that were omitted from the abovementioned report of the Inspection Service, that complaint must be rejected.

213. The Litigation Chamber notes that even if the defendant's argument were to be followed, *quod non*, it could nevertheless be concluded, as the Market Court has already indicated, that the proceedings before the Litigation Chamber were not unlawful in so far as both parties were given the opportunity to put forward their arguments in their submissions[46]. In view of the complexity of the system, the Litigation Chamber was not able to specify every technical aspect of the system against which charges were brought against the defendant

[46] Market Court, 2019/AR/741, 12 June 2019, p. 12, available on the website of the DPA.

at the outset of the proceedings before the Litigation Chamber, on 13 October 2020, *i.e.* at the time when the parties were invited to present their written submissions (art. 98 DPA Act). However, in order to ensure the procedural rights of the parties, the Litigation Chamber firstly ensured that the defendant had sufficient opportunities to present its arguments before the Litigation Chamber, and secondly, that it remained within the scope of the initial complaints and the Inspection Services' reports, communicated to both parties prior to their written submissions.

As regards the legal framework for the Inspection Service's investigations

214. It should also be recalled that the Inspection Service may conduct any investigation, hold any hearing and collect any information it deems useful in the course of its duties in order to ensure compliance with the fundamental principles of personal data protection[47].

215. The Litigation Chamber also points out that the intervention of the Inspection Service in the proceedings consists of recording findings and that it has no power to impose penalties.

216. Contrary to the defendant's contention, the Inspection Service is not an administrative authority of criminal law within the meaning of Article 6 of the European Convention on Human Rights (hereinafter: "ECHR"), as it has no power to impose penalties and its task is limited to making findings and transmitting them to the Litigation Chamber in its report. As indicated above[48], the findings of the Inspection Service are only elements on which the Litigation Chamber bases its decision at a later stage of the proceedings. Nevertheless, the Litigation Chamber emphasises that the Inspection Service's investigation in the present case was conducted in an impartial manner, in accordance with the requirements of Article 6 ECHR and Article 47 Charter. It disagrees with suggestions made by the defendant in so far as they call into question the impartiality of the Inspection Service.

On respect for the right to a fair trial, including the right to a defence before the Litigation Chamber

217. The Litigation Chamber agrees with the defendant on the importance of applying procedural safeguards relating to due process in the disputes before it. It is also established that these principles are effectively applied before the Litigation Chamber.

---

[47] Cf. Art. 64 DPA Act: "The Inspector General and the inspectors shall exercise the powers referred to in this Chapter for the purpose of supervision as provided for in Article 4(1) of this Act". Also see Art. 72(1) DPA Act: "Without prejudice to the provisions of this Chapter, the Inspector General and the inspectors may conduct any enquiry, control or audit, as well as collect any information they consider useful in order to ensure that the fundamental principles of the protection of personal data, within the framework of this Act and the laws containing provisions relating to the protection of processing of personal data, are effectively respected" (emphasis added).

[48] See para. 209-210 of this decision.

218. As set out above[49], the defendant's complaint concerning the alleged lack of reasoning and impartiality of the Inspection Service's report, on which the defendant relies to conclude that its right to a fair trial has been violated, must be rejected.

219. For the sake of completeness, the Litigation Chamber also points out that the Market Court has already ruled that — in the event that the procedural safeguards in the earlier stage of the proceedings were not guaranteed, *quod non* — parties have an adequate remedy against decisions of administrative bodies, in particular through the possibility of appeal to the Market Court[50].

220. The Market Court added that a lack of impartiality on the part of an administrative authority does not necessarily constitute an infringement of Article 6.1 ECHR if a judicial authority with full power of review, which itself respects the guarantees of Article 6.1 ECHR, can review the decision at issue.

221. According to the Market Court, an infringement of the principle of impartiality of the administration at an earlier stage does not necessarily entail a breach of the right to a fair trial if that infringement can be remedied at a subsequent stage. The possibility of an appeal to a court that respects the guarantees of Article 6 ECHR is intended to allow precisely such corrections[51].

222. Specifically with regard to the Litigation Chamber, the Market Court ruled as follows:

> "[...] *even then, this legal protection by the legal subject is only legally enforceable before a judge (who is part of the judiciary) [...]. The legal possibility of bringing an action/recourse before the Market Court is intended to provide the litigant with the guarantee of Article 6.1 ECHR and, more particularly, with the remedy provided for in Article 47 CFREU [Charter of Fundamental Rights of the European Union]*".[52]

223. Therefore, in the absence of impartiality on the part of the Litigation Chamber, which is not the case here, and in so far as the Market Court exercises full judicial review of the decisions of the Litigation Chamber, it cannot be concluded, *ipso facto,* that the right to a fair hearing in the proceedings has been infringed.

---

[49] See para. 204 et seq. of this decision.

[50] "The legislator has given the citizen a conclusive legal remedy against the conduct of administrative bodies (in this case the DPA) by providing precisely recourse to the Market Court", Court of Appeal Brussels, Market Court section, 19th Chamber A, Market Court section, 2019/AR/741, 12 June 2019, p. 9. The judgements of the Market Court are available on the website of the DPA in their original language (Dutch or French).

[51] "A lack of objective or structural impartiality on the part of an administrative authority does not necessarily constitute an infringement of Article 6.1 ECHR if the decision of that authority can subsequently be reviewed by a court of law with full jurisdiction and which offers all the guarantees provided for in Article 6.1. Consequently, an infringement of the principle of impartiality at an earlier stage does not necessarily lead to a denial of the right to a fair trial if that infringement can still be rectified at a later stage. The organisation of an appeal to a body that meets all the safeguards of Article 6 ECHR serves to make such redress possible", Court of Appeal of Brussels, Market Court Section, 19th Chamber A, Market Cases Chamber, 2019/AR/741, 12 June 2019, p. 10.

[52] Court of Appeal of Brussels, Market Court Section, 2020/AR/329, 2 September 2020.

224. For the sake of clarity and information, the Litigation Chamber notes that while the right to a defence forms part of the fundamental rights that constitute the legal order of the Union and are enshrined in the Charter[53], the fact remains that, as the CJEU has held, the various components of the right to a fair trial, including the right to a defence, are not absolute in nature and that any restriction may be possible for a public interest purpose. This assessment must be made *in concreto*:

> "*However, the Court has already ruled that fundamental rights, including respect for the right to a defence, are not absolute but may include restrictions, provided that they genuinely meet the objectives of general interest pursued by the measure in question and that, having regard to the objective pursued, they cannot be regarded as constituting a disproportionate and intolerable interference impairing the very substance of the rights guaranteed* [...].
>
> *34. Moreover, whether the right to a defence have been infringed must be assessed in the light of the specific circumstances of each case* [...]"[54].

A.9.2. - Infringements of the fundamental rights and freedoms of IAB Europe with regard to the general nature of the procedure for the DPA

a. Administrative penalties and Articles 6 and 7 ECHR and Article 47 of the Charter of Fundamental Rights of the European Union

225. The defendant submits that the measures and fines which the DPA is authorised to impose in the context of Articles 100 and 101 DPA Act, read in conjunction with Article 83 GDPR, must be classified as penalties of a criminal nature within the meaning of international human rights conventions such as the ECHR and the Charter of Fundamental Rights, having regard to the very nature of the offences and the nature and severity of the penalties which may be imposed on a party. As a result, according to the defendant, Articles 6 and 7 ECHR and Article 47 Charter of Fundamental Rights are applicable to the penalties which the DPA may impose on IAB Europe.

226. The defendant then considers that the wide margin between the minimum and maximum amount of administrative penalties of a criminal nature, which, moreover, according to the defendant, puts all infringements on an equal footing while failing to specify the severity of the penalties in the law itself, is contrary to the fundamental principles of substantive legality and proportionality. The same reasoning applies to Articles 100 and 101 DPA Act, *in conjunction with* Article 83 GDPR, which, due to their imprecise and ambiguous wording, do

[53] In this regard, see CJUE, 18 July 2013, *Commission and Others v Kadi*, C- -584/10 P, C- -593/10 P and C- -595/10 P, ECLI:EU:C:2013:518, points 98 and 99.
[54] CJEU, 10 September 2013, C-383/13 PPU, *Affaire G. et R.*, ECLI:EU:C:2013:533, points 33 s.

not allow a party to appropriately assess the criminal law consequences of a certain conduct prior to its occurrence.

227. It would therefore follow that Articles 100 and 101 DPA Act, in conjunction with Article 83 GDPR, are contrary to the fundamental principles of substantive legality and proportionality laid down in Articles 6 and 7 of the ECHR and Article 47 of the Charter of Fundamental Rights. For those reasons, the defendant considers that Articles 100 and 101 DPA Act, read in conjunction with Article 83 GDPR, cannot constitute a valid legal basis for the DPA to impose a sanction on IAB Europe.

Position of the Litigation Chamber

228. First of all, the power to impose an administrative fine and the modalities of its application are laid down in the directly effective Article 83 of the GDPR. In line with the case law of the Market Court, the Litigation Chamber finds that administrative fines, together with the other corrective measures provided for in Article 58 GDPR, form a powerful part of the enforcement tools available to the DPA[55].

229. If the DPA finds one or more infringements of the regulations, it must determine the most appropriate corrective measure(s) to address that infringement. The measures available for this purpose are listed in Article 58.2.*b* to 58.2.*j* GDPR. In particular, Article 58.2.*i* GDPR provides that the supervisory authority has the power, depending on the circumstances of each case, to impose, in addition or instead of the measures referred to in this paragraph, an administrative fine pursuant to Article 83 GDPR. This means that an administrative fine can be both a stand-alone (corrective) measure and a measure taken in conjunction with other corrective measures (and is therefore a kind of complementary measure). The criminal provisions of Sections 83.4 to 83.6 GDPR allow the imposition of an administrative fine for most infringements. Nevertheless, the supervisory authority has the responsibility to always choose the most appropriate measure(s)[56].

230. In addition to the relevant provisions of the GDPR and the DPA Act on the level of administrative fines that the Litigation Chamber may impose, the Litigation Chamber also relies on the case law of the Market Court[57], which formulates requirements on the predictability and reasoning of administrative fines imposed by the Litigation Chamber. For example, this case law has resulted in a form notifying the intention to impose a sanction being submitted to the party concerned, who may react to it and send its comments to the

[55] Court of Appeal Brussels, Market Court Section, 2021/AR/320, 7 July 2021, p. 38.

[56] *Ibidem*.

[57] Among others, judgments of 19 February 2020 (2019/AR/1600), of 24 January 2021 (2020/AR/1333) and of 7 July 2021 (2021/AR/320).

Litigation Chamber before it takes a decision. Accordingly, in the present procedure, this form was sent and the defendant submitted a reaction[58].

231. The Litigation Chamber also refers to the case law of the Market Court, which determined that the GDPR does not provide for a specific fine tag or range for specific infringements, but only an upper limit or maximum amount. In practice, this means that the DPA can decide not only not to impose a fine on the offender, but also that, if it decides to impose a fine, it shall be between the minimum, starting at 1 EUR, and the maximum foreseen. The fine shall be decided by the DPA taking into account the criteria listed in Article 83(2) GDPR[59].

232. Furthermore, the Litigation Chamber also follows the Article 29 Data Protection Working Party's guidelines on the application and setting of administrative fines under the GDPR, endorsed by the EDPB[60], which detail the criteria of Article 83(2) GDPR that a supervisory authority must apply when assessing whether to impose a fine, as well as the amount of the fine.

233. Furthermore, these guidelines also contain an explanation of Article 58 GDPR relating to the measures that a supervisory authority may choose to take, as the remedies are inherently different in nature and essentially have different purposes. Finally, it specifies that certain measures under Article 58 GDPR may be cumulative and thus constitute a regulatory action based on several remedies.

234. The Market Court, ruling with full jurisdiction, performs a legality and proportionality test of the sanction and will (only) reduce or cancel the fine in case of serious and proven circumstances that the Litigation Chamber would not or not sufficiently take into account.

235. In short, this system sufficiently guarantees that the fundamental legal principles arising from Article 6 of the ECHR and Article 47 of the Charter are complied with.

Legal framework for administrative fines

Relevant provisions in the DPA Act

236. Pursuant to Article 100(1)(13) of the DPA Act, the Litigation Chamber has the power to impose administrative fines. The Litigation Chamber may decide to impose an administrative fine on the prosecuted parties in accordance with the general terms and conditions set out in Article 83 GDPR.

237. Pursuant to Article 103 DPA Act, if an offender has committed several infringements by means of the same act only the heaviest administrative fine of the respective infringements

---

[58] See para. 272-273.

[59] Court of Appeal Brussels, Market Court Section, 2021/AR/320, 7 July 2021, p. 42.

[60] EDPB - Guidelines on the application and setting of administrative fines for the purposes of Regulation (EU) 2016/679, WP253, published on http://www.edpb.europa.eu.

shall apply. In the event of overlapping infringements, the rates of the administrative fines shall be added together without the total amount exceeding twice the highest amount of the fine applicable to the infringements committed.

Relevant provisions in the GDPR

238. Once an infringement of the Regulation has been established, based on the assessment of the facts of the case, the competent supervisory authority should determine the most appropriate corrective measures to address the infringement. The provisions of Article 58(2)(b)-(j)[61] set out the tools that supervisory authorities can use to address non-compliance by a data controller or processor.

    a. to issue warnings to a data controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

    b. to issue reprimands to a data controller or a processor where processing operations have infringed provisions of this Regulation;

    c. to order the data controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

    d. to order the data controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

    e. to order the data controller to communicate a personal data breach to the data subject;

    f. to impose a temporary or definitive limitation including a ban on processing;

    g. to order the rectification or erasure of personal data or the restriction of processing pursuant to Articles 16, 17 and 18 GDPR, as well as the notification of such actions to recipients to whom the personal data have been disclosed, in accordance with Articles 17(2) and 19 GDPR;

    h. to revoke a certification, or order the certification body to revoke a certification issued under Articles 42 and 43 GDPR, or order the certification body not to issue a certification if the certification requirements are no longer fulfilled;

    i. depending on the circumstances of each case, in addition to or instead of the measures referred to in this paragraph, to impose an administrative fine pursuant to Article 83 GDPR; and;

[61] Article 58(2)(a) states that a warning may be issued. In other words, in the case to which the provision relates, there is not yet a breach of the regulation.

j. to order the suspension of data flows to a recipient in a third country or to an international organisation.

239. The power to impose an administrative fine is regulated in Article 83 GDPR, which reads as follows:

> "*General conditions for the imposition of administrative fines*
>
> *1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.*
>
> *2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*
>
> *a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
>
> *a) the intentional or negligent character of the infringement;*
> *b) any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
> *c) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
> *d) any relevant previous infringements by the controller or processor;*
> *e) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
> *f) the categories of personal data affected by the infringement;*
> *g) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;*
> *h) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;*
> *i) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and*
> *j) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.*
>
> *3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.*
>
> *4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:*
>
> *b) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;*
> *c) the obligations of the certification body pursuant to Articles 42 and 43;*
> *d) the obligations of the monitoring body pursuant to Article 41(4).*
>
> *5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:*

a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
b) the data subjects' rights pursuant to Articles 12 to 22;
c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
d) any obligations pursuant to Member State law adopted under Chapter IX;
e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. […]"

240. A reading of points *(a)* to *(k)* of Article 83(2) GDPR, as well as the additional explanations in paragraphs 3 to 6 of that same provision, is sufficient to refute the defendant's argument that the various offences listed in Article 83 RGPD are placed on an equal footing.

241. The various criteria to assess the severity of the penalties are clearly set out in Article 83 itself and in recitals 148 to 150 GDPR. Article 83.2 also makes it clear that an analysis must be made "according to the circumstances of the case".

242. The Litigation Chamber already referred to the Guidelines on the application and setting of administrative fines under the GDPR, endorsed by the EDPB. These Guidelines provide guidance on the interpretation of the individual facts of the case in the light of the criteria set out in Article 83.2 GDPR. The Guidelines bind the Litigation Chamber as an organ of the DPA, a member of the EDPB.

243. In order to strengthen the enforcement of the rules of the GDPR, recital 148 GDPR clarifies that penalties, including administrative fines, should be imposed for any breach of the Regulation, in addition to or as an alternative to appropriate measures imposed by the supervisory authorities under this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the data controller or

processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

244. Contrary to what the defendant maintains, the GDPR does not therefore impose a minimum amount of fine, but only maximum amounts which, depending on the infringements committed, may amount to 2% or 4% of the turnover of a data controller, or EUR 10,000,000 or 20,000,000 respectively. These amounts are of a dissuasive nature, and it is for the Litigation Chamber to modulate the amount of the fine according to the circumstances of the case, taking into account the requirement of proportionality and with a view to ensuring the effectiveness of the provisions of the GDPR.

245. Since the various offences listed in Article 83 GDPR are not treated in the same way and since the various criteria to assess the severity of the penalties are clearly set out, the defendant's argument that the combined reading of Article 83 GDPR and Articles 100 and 101 DPA Act infringes the principles of legality and proportionality, and thus Articles 6 and 7 ECHR and 47 of the Charter of Fundamental Rights of the European Union, because of its vagueness must be rejected.

246. Article 83 GDPR is a directly effective provision of an EU Regulation and it is the task of the Litigation Chamber to ensure the effective operation of this Regulation. It is not for the Litigation Chamber, as a body of a national administrative authority, to rule on the possible unlawfulness of that provision.

247. In addition, the Constitutional Court ruled in its judgment no. 25/2016, of 18 February 2016 (p24-28) that a single, wide margin for an administrative fine, allowing the administrative authority to adjust the administrative fine to the gravity of the infringement, does not violate the principle of legality:

> "*B.18.2.* [...] *The principle of legality in criminal matters, which derives from the aforementioned constitutional and treaty provisions, is also based on the idea that the criminal law must be formulated in terms which enable any person, at the time when he adopts a course of conduct, to determine whether that conduct is punishable or not and, where appropriate, to know the sanction to be imposed.* [...]
>
> *However, the principle of legality in criminal matters does not prevent the law from granting the court discretion. Indeed, the general nature of the laws, the diverse situations to which they apply and the evolution of the conduct they punish must be taken into account.*
>
> *B.18.3. In the same way, to determine whether the ranges between the upper and lower limits of the sentences considered by the ordering body are so broad as to infringe the principle of the foreseeability of the sanction, account must be taken of the specific features of the offences to which those penalties are attached.* [...]

B.20.1. The assessment of the seriousness of a crime and of the severity with which the crime may be punished is within the discretion of the competent legislature. It may impose particularly severe penalties in cases where the offences may seriously affect the fundamental rights of individuals and the interests of the community. It is therefore up to the competent legislator to establish the limits and amounts within which the discretion of the court and of the administration must be exercised. The Court could only reject such a system if it were manifestly unreasonable.

B.20.2. The ordering body cannot be blamed for wanting to rationalise and simplify the environmental criminal law in force in the Region. In order to achieve that objective, it could establish a single and sufficiently wide margin between the upper and lower limits of the sanction, both for criminal penalties and for alternative administrative fines, in order to allow the court or the administrative authority to adjust the sanction or the alternative administrative fine to the seriousness of the crime.

B.20.3. With regard specifically to the offence of exceeding the noise standards laid down by the Government, the contested provisions are addressed to persons subject to the law who are professionals and can assess with sufficient accuracy the seriousness of the offence they are committing and the corresponding severity of the sanction to which they are subject. In addition, the choice of sanction must be justified, either by the judge or by the administrative authority. In the latter case, the decision is subject to judicial review.

B.20.4. It follows from the foregoing that the contested provisions do not confer on the court or administrative authority any discretion going beyond the limits of what is permissible under the principle of the foreseeability of penalties

248. The defendant's argument that Articles 100 and 101 DPA Act *in conjunction with* Article 83 GDPR, which form the basis of the power of the Litigation Chamber to impose administrative penalties and fines, infringe the principles of legality and proportionality and thus the right to a fair hearing must therefore be rejected.

b. The internal rules of the DPA do not comply with the fundamental principle of the formal legality of criminal sanctions, enshrined in Articles 12 and 14 of the Belgian Constitution

249. The principle of formal legality, enshrined in Articles 12 and 14 of the Belgian Constitution, requires that the essential elements of the rules relating to the offences made punishable, the nature and level of the sanction, and the procedure guaranteeing that the right to a defence are safeguarded, be laid down by the Chamber of Representatives in accordance with the legislative procedure laid down by the Belgian Constitution.

250. Since this principle applies not only to criminal penalties *stricto sensu*, but also to administrative penalties of a criminal nature, it is fully applicable to the DPA sanctioning procedure.

251. In this regard, the defendant submits that various aspects of the DPA sanctioning procedure are not laid down in a legislative text - in particular, not in the DPA Act, but in the Rules of Internal Procedure of 15 January 2019 (RIO).

252. As a result, the defendant considers that the current proceedings were conducted on the basis of procedural rules that are contrary to Articles 12 and 14 of the Belgian Constitution and therefore lack a valid legal basis, with the result that the complaints against IAB Europe must be dismissed.

Position of the Litigation Chamber

253. The principle of legality means that the essential elements of an offence, such as its nature, the level of punishment and the procedural guarantees relating to it, must be determined by the legislator.

254. The Litigation Chamber notes that the only elements relating to the imposition of a sanction that are not contained in the GDPR, the DPA Act or the law of 30 July 2018, but in the Rules of Internal Order (RIO) of the DPA referred to by the defendant, are by no means essential elements for the imposition of fines. Indeed, it is not the nature of the fine, nor the sanction, that is at issue, but elements of a secondary or organisational nature, for example, with regard to the procedure to be followed in the absence of the president of the Litigation Chamber (Article 44 RIO), or the number of members sitting per case (Article 43 RIO).

255. The Litigation Chamber also emphasises that the independence of a supervisory authority under Article 51 et seq. GDPR means that the organisation of its processes, including for example the assignment of members to a procedure, is at the discretion of the Data Protection Authority, of course within the limits of the general principles of good administration and the relevant national legislation.

256. The defendant's argument that the procedure before the Litigation Chamber infringes the principle of legality is therefore rejected.

c. Appointment of members of the DPA violates Article 53 GDPR

257. The defendant claims that Article 39 DPA Act, which regulates the appointment of the members of the Litigation Chamber, does not in any way clarify the modalities of the appointment procedure. In particular, nowhere does it specify how the hearing of the candidates should proceed, nor does the DPA Act require a written record of the hearing. Moreover, the nomination takes place on the basis of a secret ballot and there are no guarantees as to the adequacy of the information on the candidates provided to the members of the Chamber of Representatives.

258. According to the defendant, the appointment of the members of the DPA, including the members of the Litigation Chamber, therefore does not satisfy the requirements of Article

53 GDPR, which provides that the appointment must be made 'by means of a transparent procedure'.

259. In view of the foregoing, the defendant considers that the members of the Litigation Chamber are not in a position to make a legally valid decision in relation to IAB Europe in this case. For those reasons also, the claims against IAB Europe should be dismissed.

Position of the Litigation Chamber

260. First of all, the Litigation Chamber points out that any imperfections in the appointment procedure of the members of the DPA cannot form part of these proceedings and that the parties cannot invoke a procedural interest in questioning the appointment procedure.

261. The Litigation Chamber reminds that the members of the Litigation Chamber are appointed by the House of Representatives and can only be removed from their positions by the House. Thus, neither the Litigation Chamber nor the Market Court are competent to rule on their appointment. In addition, the parties have no interests in requesting such a ruling.

262. Consequently, the Litigation Chamber rules that this plea is unfounded.

d. The way in which the DPA has handled this procedure is not in line with its duties and powers under Article 57 GDPR

263. In conclusion, the defendant states, both in its initial submission and in the context of the reopening of the debates, that the way in which the DPA, in addition to the original complaint, also considers the additional complaints and grievances made by the complainants, without the relevance of those additional allegations having been examined by the Inspection Service, makes the defence of IAB Europe considerably more difficult.

264. IAB Europe considers that this approach is not only fundamentally incompatible with the duties and responsibilities of a supervisory authority as defined in Article 57 GDPR, but also has the effect that IAB Europe must only defend itself against the allegations contained in the inspection report, as opposed to the subsequent allegations made by the complainants in their subsequent submissions.

Position of the Litigation Chamber

265. The Litigation Chamber emphasises first of all that at no time did the defendant explain which new allegations are the subject of their defences and as such would violate its rights of defence. For this reason alone, the Litigation Chamber considers itself entitled to declare the defendant's plea unfounded.

266. Secondly, the Litigation Chamber notes that the DPA Act in no way prescribes that the Litigation Chamber is bound by an investigation report following an investigation requested to the Inspection Service. Indeed, it does not follow from any provision of the DPA Act that the Litigation Chamber is denied the opportunity to take into account additional or

supplementary elements to the report of the Inspection Service, as long as the consideration of these additional or supplementary elements is sufficiently justified in the decision and the right of defence is sufficiently guaranteed.

267. The Inspection Service may in any case decide not to investigate certain disputed points, in accordance with its prerogative under Article 64(2) DPA Act. In such a case, however, it would be contrary to Article 57 GDPR as well as to the autonomy and independence of the Litigation Chamber, as implemented by Articles 92 to 100 DPA Act, to simply bind the Litigation Chamber to the findings of the Inspection Service, without taking into account the elements put forward in the debates by the parties in the course of the proceedings and in accordance with the right to be heard.

268. Thirdly, the Litigation Chamber rules that the alleged obligation to base debates on the inspection report alone following an investigation by the Inspection Service does not apply. The DPA Act does not provide anywhere that the Litigation Chamber should base its decision solely on the inspection report or on the parties' submissions. It is appropriate for a supervisory authority to also consult other bodies and sources in order to be able to support its decisions if necessary.

269. With regard to the Inspection Service's assessment with a view to a supplementary investigation, and in particular the nature of the time limits provided for in Article 96 DPA Act, the Litigation Chamber is not convinced by the arguments put forward by the defendant. In the present case, the parties have had ample opportunity to make their views known to the Litigation Chamber and to the other party regarding the allegations and charges, including the operation of the TCF, the processing of user preferences and permissions in the TC String, as well as the interrelationship between the TCF and OpenRTB.

270. In addition, the Litigation Chamber finds that there is no doubt about the crucial importance of the TC String for the functioning of the TCF. As a result, the defendant could have expected from the start of the proceedings that the debates would focus on the processing of data in the context of the TC String. Thus, there can be no question at all of new allegations - in so far as they exist, given the lack of any concrete example with which the defendant substantiated its plea - in the complainants' submissions, since they constitute an explanation of the operation of the TCF, which is not disputed as being at the heart of the complaints against IAB Europe.

271. Bearing the above points in mind, the Litigation Chamber rules that this plea is insufficient both in fact and in law.

A.10. - Sanction form, European cooperation procedure and publication of the decision

272. The procedure before the Litigation Chamber includes an exchange of written submissions as well as an oral hearing of the parties involved, as normal steps towards a decision. If the Litigation Chamber proposes, after deliberation, to impose a (punitive) sanction, the Market Court requires the Litigation Chamber to provide the defendant with an opportunity to respond to the intended sanctions, through a standard form covering the retained infringements and the criteria for determining the amount of the fine. This opportunity for contradiction, or right to be heard, pertains to the proposed sanctions only and is therefore only communicated to the defendant.

273. A sanction form has been sent on 11 October 2021, informing the defendant of its infringements against the GDPR as well as of the Litigation Chamber's intent to impose corrective measures and an administrative fine. IAB Europe submitted its response on 1 November, 2021. The defendant contests the calculation of the administrative fine, by claiming that the Litigation Chamber did not consider all relevant elements for determining the amount of the administrative fine under Article 83.2 GDPR. Moreover, the defendant disagrees with the Litigation Chamber's consideration of the total worldwide annual turnover of Interactive Advertising Bureau Inc. (IAB Inc.) for the calculation of the administrative fine, since the latter has no ownership stake in the defendant nor any say in the deployment of IAB Europe's activities. The defendant clarifies that IAB Europe licences the 'IAB' brand name from IAB Inc., and that the various IAB organizations across Europe are separate and distinct organisations.

274. On 8 November, the complainants submitted a request to the Litigation Chamber, asking to be provided with a copy of the sanction form as well as the defendant's reaction, based on the erroneous assumption that the defendant also received further insights into the draft decision of the Litigation Chamber. The Litigation Chamber responds on 9 November 2021 that it will not disclose the sanction form to the complainants. The notification of the sanction form to the defendant takes place within the framework of an objective review of legality and with the specific aim of respecting the defendant's rights of defence, in accordance with the case law of the Market Court. The defendant is thus informed in advance of the nature and severity of the sanction it risks and is given the opportunity to submit its final comments on this point to the Litigation Chamber. Notifying the sanction form to the complainants could not possibly contribute to the same objective, since the sanction envisaged would only be imposed on the defendant, not on the complainants, and would therefore not directly affect the interests of the latter. Neither the rights of the defence nor any other rule of law require that the complainants be able to put forward additional arguments in relation to the penalty which may be imposed on the defendant.

275. On 23 November 2021, the Litigation Chamber submitted its draft decision with the other concerned European supervisory authorities (hereinafter, 'CSAs'), as foreseen under article 60.3 GDPR.

276. On 18 December 2021 the Litigation Chamber received a letter from the complainants in response to the Litigation Chamber's decision not to disclose the content of the sanction form to the complainants. More specifically, the complainants argued that they should be informed whether the defendant has brought new elements to the proceedings. The Litigation Chamber notes that the debates were already closed at that time, and that the reaction of the defendant to the sanction form only pertained to elements concerning the sanction.

277. On 20 December 2021, the Litigation Chamber is notified through the Internal Market Information (IMI) system of a relevant and reasonable objection (RRO) submitted by the Dutch Authority for Personal Data (Autoriteit Persoonsgegevens). The objection pertains to the absence of reasoning by the Litigation Chamber with respect to the Dutch NGO Bits of Freedom's claim that the TCF makes it impossible for users to exercise their data subject rights. The Litigation Chamber has addressed this RRO in its revised draft decision[62].

278. On 21 December 2021, the defendant submitted a letter to the Litigation Chamber, requesting the suspension of the provisional enforcement of the decision, that the Belgian Data Protection Authority does not make the decision public until all appeals have been exhausted, and that the DPA refrains from issuing any public communication about the decision prior to any such final decision. Once again, the Litigation Chamber notes that the debates were already closed at that time.

279. On 21 December 2021, the Litigation Chamber is notified of a relevant and reasonable objection introduced by the Portuguese National Commission for Data Protection (CNPD). The objection pertains to the absence of sanction by the Litigation Chamber with respect to the processing of TC Strings in the absence of a lawful ground under Article 6 GDPR. The CNPD finds that the draft decision must impose upon the defendant the immediate erasure of all personal data unlawfully collected so far. The Litigation Chamber has addressed this RRO in its revised draft decision[63].

280. In addition to the two RROs, the Litigation Chamber received comments from other CSAs regarding the joint-controllership established by the Litigation Chamber, the use of legitimate interest for certain processing operations, the scope of the corrective measures,

[62] See para. 504 to 506.
[63] See para. 535.

as well as the administrative fine envisaged and the relationship between IAB Inc. and IAB Europe.

281. On 13 January 2022, the Litigation Chamber submitted its revised draft decision with the other concerned European supervisory authorities (hereinafter, 'CSAs'), as foreseen under article 60.5 GDPR.

282. On 17 January 2022, the Litigation Chamber notified the parties of the submission of the revised draft decision and the deadline of 27 January 2022 for the CSAs. It also clarified that the written exchanges with the defendant's councils, concerning the sanction form, did not involve new arguments that would require reopening the debates with both parties. Hence, and seeing as both these exchanges and the sanction form will be part of the administrative file, the Litigation Chamber dismissed the complainants request to gain access to the sanction form and the written exchanges that followed with the defendant.

283. On 20 January 2022, the Litigation Chamber received a letter from the claimants, in which they claim that they have the right to obtain a copy of the sanction form and the subsequent exchanges with the defendant, in order to verify themselves whether no new elements were brought up by the latter. The claimants also argue that if the sanction form and subsequent exchanges will be part of the administrative file, and thus accessible in case of an appeal, there is no reason why they should not be granted access during the current proceedings. The claimants further claim, based on a press release by the defendant dd. 5 November 2021, that the Litigation Chamber has agreed to approve a Code of Conduct submitted by the defendant 6 months after its decision. The claimants argue this has not been subject to the debates during the proceedings, and thus request access to all written exchanges with the defendant following the sanction form, as well as the reopening of the debates on the Litigation Chamber's competence to approve a code of conduct or validate an action plan.

284. On 27 January 2022, the Litigation Chamber acknowledged the reception of the claimant's letter, and responded that their arguments will be taken into consideration in its deliberations.

Assessment by the Litigation Chamber

285. The Litigation Chamber first and foremost finds that it is not responsible and cannot be held accountable for public statements made outside of the proceedings by either or both of the parties involved during the Litigation Chamber's deliberations on the merits.

286. Secondly, the Market Court has stated that the claimants do not have any say in the determination of the sanctions imposed by the Litigation Chamber[64]. In this regard, Article 58.2.d of the GDPR grants supervisory authorities to order a controller or a processor to bring processing operations into compliance with the provisions of the GDPR, where appropriate, *in a specified manner and within a specified period.* This provision, read in conjunction with Article 100, §1, 9° of the Data Protection Act, must be interpreted in the sense that an action plan and the inherently involved monitoring of this action plan by the BE DPA, must be seen as one of the sanctions that can be imposed on a controller or processor. The action plan must therefore be seen as a corrective measures, with regard to which the claimants have no stake.

287. With regard to the defendant's request not to publish the decision, the Litigation Chamber reminds of the significant impact of the case, in view of the a large number of data subjects and organisations involved. Moreover, the Litigation Chamber notes that the request by the defendants was submitted after the closure of the debates, and that the defendant itself already published on the case on 5 November 2021. Having considered these elements, the Litigation Chamber considers not to give a positive reply to the defendant's request dd. 21 December 2021 not to publish the decision or issue public communications about the decision prior to the exhaustion of all appeals.

[64] Market Court, 1 December 2021, FOD Financiën v. GBA, nr. 2021/AR/1044, para. 7.3.4: "It is (certainly) not for a complainant to interfere in any way with the expediency, let alone the extent of a sanction. The complaint only concerns (and can only concern) an alleged infringement in such a way that the decision taken by the Dispute Resolution Chamber of the GBA in relation to the complaint - and in which it possibly imposes a sanction on the person concerned - is never an *ultra petita* judgment from the point of view of the complaint."

B. Reasoning

B.1. – Processing of personal data in the context of the Transparency and Consent Framework

288. In this section, the Litigation Chamber examines the concept of personal data as well as the question of whether personal data exists within the context of the Transparency and Consent Framework, designed and managed by IAB Europe[65] and is being processed[66].

289. For a proper understanding of this decision, the Litigation Chamber emphasises that the complainants indicated in their written submissions that they wished to limit themselves to the alleged breaches of the GDPR in the processing of personal data "in the TCF per se"[67]. The Litigation Chamber will therefore not pass judgment in this section on processing responsibility with regard to the processing operations that take place in the context of the OpenRTB system.

B.1.1. – Presence of personal data within the TCF

290. European data protection law, including the GDPR, has always taken a broad view of personal data with the aim of ensuring a high level of data protection and safeguarding the fundamental rights and freedoms of data subjects. The broad interpretation of, inter alia, the concept of personal data and the notion of processing is a key element of the case law of the Court of Justice[68]. The principle that personal data does not only relate to an identified, but also to an *identifiable* natural person was already established in 1981 by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[69].

291. The GDPR unambiguously states that any information about an identified or identifiable natural person ("data subject") constitutes personal data. "Identifiable' should therefore be understood to mean the possibility of identifying a natural person directly or indirectly by means of an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[70].

292. Furthermore, the GDPR provides that, to determine whether a natural person is identifiable, account should be taken of all means of which it can be reasonably assumed they will be

---

[65] See title B.1.1. – Presence of personal data within the TCF.
[66] See title B.1.2. - Processing of personal data within the TCF.
[67] Submission of the complainants dd. 18 February 2021, p. 2.
[68] C. DOCKSEY, H. HIJMANS, "The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law", *EDPL Review*, 2019, p. 300.
[69] Article 2.*a* of the Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, *B.S.*, 30 December 1993 (Convention 108).
[70] Article 4.1 GDPR.

used either by the data controller *or by any other person* to identify the natural person directly or indirectly, such as singling out[71].

293. To determine whether resources can reasonably be expected to be used to identify the natural person, account should also be taken of all objective factors, such as the cost and time required for identification, taking into account the technology available at the time of processing and technological developments[72].

294. Recital 30 GDPR clarifies that natural persons may be linked to online identifiers through their devices, applications, tools and protocols, such as Internet Protocol (IP) addresses, identification cookies or other identifiers. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

295. The former Article 29 Working Party has already addressed the importance of a broad definition of personal data, in particular that a natural person can be considered identifiable when he/she can be distinguished from other members of the group and consequently treated differently [73].

296. This position is also taken by the Court of Justice. It is established case law that the content of the information that qualifies as personal data is not important[74] and that the criterion of identifiability must be interpreted flexibly. **As long as information, due to its content, purpose or effect, can be linked to an identified or identifiable natural person by means that can reasonably be used[75], regardless of whether the information from which the data subject can be identified is held entirely by the same controller or partly by another entity, this information should be considered personal data**[76].

297. The complainants argue in their submission in response that the TC String is a unique character string which is also written into a cookie as a unique identifier and is then stored on a user's device[77]. Furthermore, the complainants take the view that IAB Europe collects

---

[71] Recital 26 GDPR; the English text explicitly refers to "*singling out*" as one of the means of identifying a natural person. See also CJEU Judgment C-582/14 of 19 October 2016, *Patrick Breyer t. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, para. 46, and FR. ZUIDERVEEN BORGESIUS, "Singling out people without knowing their names - Behavioural targeting, pseudonymous data, and the new Data Protection regulation", *Computer Law & Security Review*, vol. 32-2, 2016, pp. 256-271.

[72] *Ibidem.*

[73] WP136 - Opinion 4/2007 on the concept of personal data, p. 14; WP199 - Opinion 08.2012 providing further input on the data protection reform discussions, p. 5.

[74] Opinion of Advocate General Sharpston of 12 December 2013 in Joined Cases C-141/12 and C-372/12, *Y.S.*, para. 45.

[75] CJEU Judgment C-434/16 of 20 December 2017, *Nowak t. Data Protection Commissioner*, ECLI:EU:C:2017:994, para. 35.

[76] CJEU Judgment C-582/14 of 19 October 2016, *Patrick Breyer t. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, para. 43; CJEU Judgment C-434/16 of 20 December 2017, *Nowak t. Data Protection Commissioner*, ECLI:EU:C:2017:994, para. 31: see also FR. ZUIDERVEEN BORGESIUS, "Singling out people without knowing their names - Behavioural targeting, pseudonymous data, and the new Data Protection regulation", *Computer Law & Security Review*, vol. 32-2, 2016, pp. 256-271; and FR. ZUIDERVEEN BORGESIUS, "The Breyer Case of the CJEU - IP Addresses and the Personal Data Definition", *EDPL*, 1/2017, pp. 130-137.

[77] Submissions of the complainants dd. 18 February 2021, para. 25.

additional information about users with the help of the TC String, including sensitive personal data within the meaning of Article 9 GDPR[78].

298. The defendant, on the other hand, refutes the allegations and states that the TC String does not contain any personal data[79] or any information directly or indirectly related to the so-called '*content taxonomy*'[80], which IAB Europe uses as a 'common language' to describe the content of a website[81]. Furthermore, the defendant takes the view that the TC String does not constitute a unique identifier, nor is it conceived for that purpose[82].

299. Notwithstanding the foregoing, the defendant states that it must necessarily be possible to link the TC String with a user, but with the proviso that the link between the preferences conceived in the TC String and the user will be established only at a later stage, in particular in the context of the OpenRTB, and is therefore not covered by the Transparency & Consent Framework[83].

300. Based on the technical documentation of IAB Europe and IAB Tech Lab on the TCF protocol, the Inspection Service concludes that the TC String in itself does not *directly* identify users or devices, as the components that compose the TC String merely reflect technical information, namely whether or not an unidentified user has consented to purposes Y or Z, and whether *adtech vendors* A and B may process the personal data for the accepted purposes.

301. Specifically, a TC String consists of the following fields:

    i. general metadata;
    ii. a binary value for each of the purposes of the processing for which consent may be given;
    iii. a binary value for each of the purposes of processing permitted by a legitimate interest;
    iv. a binary value for each of the adtech vendors who may collect and process the user's personal data on the basis of his consent;
    v. a binary value for each of the adtech vendors who may collect and process the user's personal data on the basis of a legitimate interest;
    vi. any processing restrictions;
    vii. special *opt-in* features in connection with the processing purposes;

[78] Submissions of the complainants dd. 18 February 2021, para. 26.
[79] Defendant's reply brief dd. 25 March 2021, para. 48.
[80] Defendant's reply brief dd. 25 March 2021, para. 51.
[81] https://iabtechlab.com/standards/content-taxonomy/
[82] Defendant's reply brief dd. 25 March 2021, para. 53.
[83] Defendant's reply brief dd. 25 March 2021, para. 54.

viii. a field dedicated to processing purposes that do not fall under the TCF but are specific to the *publisher*;

ix. consent to the processing on legal bases that are not covered by the TCF.

Assessment by the Litigation Chamber

302. While the Litigation Chamber understands that it is not conclusively established that the TC String, due to the limited metadata and values it contains, in itself allows for direct identification of the user, the Litigation Chamber notes that when the consent pop-up is accessed by script from a server managed by the CMP[84], it inevitably also processes the user's IP address, which is explicitly classified as personal data under the GDPR.

303. Indeed, Recital 30 GDPR states that natural persons may be linked to online identifiers through their devices, applications, tools and protocols, such as Internet Protocol (IP) addresses, identification cookies or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

304. As soon as a CMP stores or reads the TC String on a user's device using a *euconsent-v2* cookie, the consent or objection to the processing on the grounds of legitimate interest, as well as the preferences of this user, can be linked to the IP address of the user's device. In other words, CMPs have the technical means to collect IP addresses (as indicated in their pop-up[85]) and to combine all information relating to an identifiable person. The possibility of combining the TC String and the IP address means that this is information about an identifiable user[86].

305. In addition, identification of the user is possible by linking to other data that can be used by participating organisations within TCF, but also in the context of OpenRTB. In that regard, the Litigation Chamber emphasises that the parties in question are not one and the same, but participating organisations — CMPs and adtech vendors — who, as examined in more detail below[87] are obliged to disclose information enabling them to identify users to the defendant, upon simple request.

---

[84] Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 58.

[85] See examples in the Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), pp. 99 ff.

[86] C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, "Consent Management Platforms Under the GDPR: Processors and/or Controllers?", in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, pp. 50-51. The Litigation Chamber notes in this regard that, until this summer, if a 'globally stored' TC String was chosen, the CMPs could access the IAB Europe-managed *consensu.org* internet domain to verify whether a globally scoped consent had been given by the user, which involved the disclosure of the TC String values coupled with users' IP addresses to the CMPs, by IAB Europe. The defendant announced during the hearing that the globally scoped consents functionality would be deprecated.

[87] See para. 358 et seq. of this decision.

306. Therefore, the Litigation Chamber finds that the defendant has reasonable means at its disposal that it can use with respect to registered organisations participating in the TCF, and with which the defendant is able to identify directly or indirectly the user behind a TC String.

307. The Litigation Chamber also understands that the TCF is intended to and therefore inherently involves storing each user's combination of preferences in the form of a unique string in the TC String, in order to communicate those preferences to a large number of adtech vendors.

308. Indeed, the Litigation Chamber found from the inspection reports that adtech vendors as well as other participants within the wider OpenRTB ecosystem read the signal stored in a TC String in order to determine whether they have the required legal basis to process a user's personal data for the purposes to which the user has consented[88].

309. In this regard, the Litigation Chamber emphasises that it is sufficient that certain information is used to single out a natural person to be able to speak of personal data[89]. Also, the purpose of the TC String, namely to capture the preferences of a specific user, leads *de facto* to the TC String being regarded as personal data.

310. **In other words, if the purpose of the processing is the singling out of persons, it may be assumed that the controller or another party has or will have at their disposal the means by which the data subject may reasonably be expected to be identified. To claim that individuals are not identifiable, when the purpose of the processing is precisely to identify them, would be a *contradiction in terminis***[90].

311. Furthermore, the Litigation Chamber is of the opinion that the processing of these preferences has unmistakable consequences for the rights and interests of the data subjects, since these choices determine, among other things, which third parties will receive and process the personal data of the users in the context of the OpenRTB protocol[91].

312. In view of the foregoing findings as well as the broad interpretation of the concept of personal data, as confirmed in the case law of the Court of Justice[92], the Litigation Chamber concludes that the preferences of users in a TC String do constitute personal data, as these preferences relate to a singled out, identifiable natural person[93].

---

[88] Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 75.
[89] WP136 - Opinion 4/2007 on the concept of personal data, p. 14.
[90] WP136 - Opinion 4/2007 on the concept of personal data, p. 16.
[91] CJEU, judgment C-434/16 of 20 December 2017, *Nowak t. Data Protection Commissioner*, para. 39.
[92] See para. 296 of this decision.
[93] CJEU, judgment C-434/16 of 20 December 2017, *Nowak t. Data Protection Commissioner*, para. 34.

B.1.2. - Processing of personal data within the TCF

313. The Inspection Service explains in its technical investigation reports that the TCF is necessarily based on three core components:

   i. a fully customisable user interface that allows TCF-registered *Consent Management Platforms* to collect the user's consent, any objections to processing based on a legitimate interest, and preferences regarding the purposes of processing and authorised *adtech vendors*;

   ii. a *Global Vendors List* that includes partners approved by IAB Europe and specific information regarding their respective processing purposes and legal bases; and

   iii. a standardised mechanism for requesting, storing and optionally sharing authorised *adtech vendors*, consents, objections and preferences through a dedicated API, a standard format for storing partners/consents, and a standardised data structure for transferring partner/consent status[94].

314. The complainants argue that the generation of the TC String corresponds to the automated creation of a unique string of characters associated with a specific user, through which his data exchange preferences are captured by the intervention of a CMP connected to the TCF[95].

315. Furthermore, the complainants refer to the sharing of the TC String with CMPs and other participants in the TCF. Specifically, they argue that the storage of a TC String in a specific *euconsent-v2* cookie, on a storage system chosen by the CMP or associated with the *consensu.org* internet domain managed by IAB Europe, also constitutes processing of user preferences.

316. The defendant, on the other hand, argues that there is no processing of personal data within the meaning of Section 4(2) GDPR in the context of the TCF, given its view that the TC String as such cannot be regarded as personal data.

Assessment by the Litigation Chamber

317. First and foremost, the Litigation Chamber refers to the definition of processing personal data as being any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

[94] Consent Management Platform API v2.0, August 2019 (Exhibit 34), p. 4; Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), pp. 58-59.
[95] Submissions of the complainants dd. 18 February 2021, para. 27.

disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction[96].

318. The TCF provides a standardised approach for collecting and exchanging personal data - i.e. consent, any objections, and preferences - from well-defined, already identified or at least identifiable users in a supposedly GDPR-compliant manner. The fact that participating organisations can directly identify data subjects with additional data such as an IP address from the TC String, which captures these consents, objections and preferences, means not only that the TC String can be considered personal data[97], but also that the participating organisations *(adtech vendors*) necessarily *process* personal data.

319. Taking into account the connection between the TCF and the OpenRTB protocol, the Litigation Chamber refers to the guidelines of the former Article 29 Working Party on Online Advertising, in which the Working Party noted that the methods of advertising based on surfing behaviour inherently involve the processing of personal data, as such advertising entails the collection of IP addresses and the processing of unique identifiers, so that data subjects can be followed online even if their real names are not known[98].

320. The Litigation Chamber understands that the *Transparency and Consent Framework* inherently entails the collection, processing, storage and subsequent sharing of users' preferences with other parties, whether or not in combination with additional personal data in the context of the OpenRTB.

321. Consequently, the Litigation Chamber finds that there is in fact processing of personal data within the meaning of Article 4.2 of the GDPR. This conclusion is also confirmed by consideration of the possibility that the TC Strings may at any time be linked to immediately identifiable information, whether provided by the data subject or not.

B.2. - Responsibility of IAB Europe for the processing operations within the Transparency and Consent Framework

322. IAB Europe states that it is neither data controller nor jointly responsible for the processing of personal data collected by the participating organisations in the context of the TCF.

323. However, the Litigation Chamber finds that this reasoning cannot be followed for several reasons. First of all, the broad interpretation by the Court of Justice of the concept of a data controller (B.2.1. - Broad interpretation of the concept of data controller by the Court of

[96] Art. 4.2) GDPR.

[97] See previous section, B.1.1. – Presence of personal data within the TCF.

[98] WP171 - Opinion 2/2010 on online behavioural advertising, 22 June 2010, p. 10, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_nl.pdf

Justice and the EDPB) must be applied. The fact that IAB Europe has a decisive influence on the purpose (B.2.2. - Determining the purposes of the processing of personal data within the TCF) and means (B.2.3. - Determining the means for processing personal data within a TCF) of the processing by imposing compulsory TCF parameters also needs to be taken into account.

B.2.1. - Broad interpretation of the concept of data controller by the Court of Justice and the EDPB

324. The GDPR defines a "data controller" as the entity that, alone or jointly with others, determines the purposes and means of the processing of personal data[99]. This definition should be understood in the light of the legislator's objective of placing the main responsibility for the protection of personal data on the entity that actually exercises control over the data processing. This means that not only the legal qualification, but also the actual reality[100]must be taken into account.

325. The EDPB has clarified that the concept of data controller refers to the influence of the data controller on the processing, based on a power of decision or monitoring of the processing activities. Such monitoring may be based on legal provisions, on an implicit power or on the exercise of a de facto influence[101]. In essence, determining the purposes and the means corresponds to deciding respectively the "why" and the "how" of the processing: given a particular processing operation, the controller is the actor who exerts such influence over the processing of personal data, thus determining why the processing is taking place (i.e., “to what end”; or “what for”) and how this objective shall be attained (*i.e.* which means shall be employed to pursue the objective)[102].

326. The power to determine the means and purposes of processing activities may first be linked to the functional role of an organisation[103]. The responsibility may also be assigned on the basis of the contractual provisions between the parties involved, although these are not always decisive[104], or on the basis of an assessment of the actual control of a party. For example, determining the means and purposes may result from a decisive influence on the processing, in particular on why processing is carried out in a certain manner[105].

---

[99] Art. 4.7) GDPR

[100] L. A. BYGRAVE & L. TOSONI, “Article 4(7). Controller" in *The EU General Data Protection Regulation. A Commentary*, Oxford University Press, 2020, p. 148.

[101] EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 20 et seq.

[102] *Ibidem*, para. 35.

[103] D. De Bot, *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context*, Wolters Kluwer, 2020, para. 362.

[104] D. De Bot, *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context*, Wolters Kluwer, 2020, para. 363-365.

[105] EDPB - Guidelines 7/2020 on the concepts of controller and processor in the GDPR, v2.0, 2021, para. 20.

327. In its Jehovah's Witnesses judgment[106], the Court of Justice gives a broad interpretation to the concept of a data controller. This judgment is relevant and applicable to the present case, as it clarifies that the definition of data controller must be interpreted broadly, in order to ensure 'effective and complete protection of the data subjects'[107], and that no access to the personal data concerned is required in order to qualify as a data controller[108]. The Litigation Chamber quotes the relevant recitals of the aforementioned judgment below:

> "65. *As Article 2(d) of Directive 95/46 expressly provides, the term 'data controller' refers to the natural or legal person who, 'alone or jointly with others', determines the purposes and means of the processing of personal data. This concept does not therefore necessarily refer to a single natural or legal person and may involve several participants in such processing, each of whom is then subject to data protection provisions (see, to that effect, Judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, point 29).*
>
> *66. Although the aim of that provision is to ensure effective and complete protection of data subjects through a broad definition of the term 'data controller', the existence of joint responsibility does not necessarily mean that the various participants in the processing of personal data are equally responsible. On the contrary, these participants may be involved in this processing at different stages and to different degrees, so that the assessment of the level of responsibility of each of them must take into account all the relevant circumstances of the particular case (see, to that effect, judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C- -210/16, EU:C:2018:388, points 28, 43 and 44).*
>
> *67. In that regard, neither the wording of Article 2(d) of Directive 95/46, nor any other provision of that directive, permits the conclusion that the purposes and means of the processing must be determined by means of written guidelines or instructions from the data controller.*
>
> *68. However, a natural or legal person who exercises influence over the processing of personal data for reasons of their own and thereby takes part in determining the purposes and means of processing may be regarded as a data controller within the meaning of Article 2(d) of Directive 95/46.*
>
> *69. Moreover, the fact that several participants are responsible for the same processing under that provision does not presuppose that each of them has access to the personal data concerned (see, to that effect, Judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C- -210/16, EU:C:2018:388, point 38).*"

---

[106] CJEU Judgment of 10 July 2018, *Tietosuojavaltuutettu* et *Jehovan todistajat - uskonnollinen yhdyskunta*, C-25/17, ECLI:EU:C:2018:551.

[107] CJEU Judgment of 13 May 2014, *Google Spain SL v. Agencia Española de protección de Datos (AEPD) and Others*, C-131/12, ECLI: EU:C:2014:317, paragraph 34; see also the discussion on the scope of the concept in C. DOCKSEY and H. HIJMANS, "The Court of Justice as a Key Player in Privacy and Data Protection", *European Data Protection Law Review*, 2019, issue 3, (300)304.

[108] CJEU Judgment of 10 July 2018, *Tietosuojavaltuutettu* et *Jehovan todistajat - uskonnollinen yhdyskunta*, C-25/17, ECLI:EU:C:2018:551. See also EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 45.

328. It is therefore clear to the Litigation Chamber that the defendant does not necessarily have to process the personal data concerned itself, nor does it have to be able to grant itself any access to the personal data, in order for IAB Europe to be considered a data controller, as[109] in relation to a framework for which the defendant moreover charges an annual fee of 1.200 EUR to participating organisations[110].

329. Furthermore, the impact or consequences of certain activities on the rights and freedoms of data subjects may also be taken into account when determining an organisation's responsibility. If it appears that an organisation plays a decisive role in the dissemination of personal data[111] or that the processing operations carried out under the influence of the organisation may substantially affect the fundamental rights to privacy and to the protection of personal data[112], that organisation should be regarded as a data controller.

330. *In this case,* the Litigation Chamber concludes that the participating parties, i.e. *publishers* and *adtech vendors*, would not be able to achieve the goals set by IAB Europe without the TCF. IAB Europe's framework thus plays a decisive role with regard to the collection, processing and dissemination of users' preferences, consents and objections, regardless of whether the defendant itself comes into contact with the aforementioned data.

B.2.2. - Determining the purposes of the processing of personal data within the TCF

331. Defining the purposes is the first condition for identifying the data controller of personal data[113]. Moreover, it is generally considered that defining the purposes of processing outweighs defining the means when it comes to establishing the responsibility of an organisation[114]. Incidentally, an erroneous designation by a data controller, such as a designation as a processor that is contradicted by the factual situation, is not binding on the court or supervisory authority[115].

---

[109] CJEU Judgment of 5 June 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, ECLI: EU:C:2017:796, para. 35; CJEU Judgment of 10 July 2018, *Tietosuojavaltuutettu* et *Jehovan todistajat - uskonnollinen yhdyskunta*, C-25/17, ECLI:EU:C:2018:551, para. 69.

[110] https://iabeurope.eu/join-the-tcf/

[111] CJEU Judgment of 13 May 2014, *Google Spain SL v. Agencia Española de protección de Datos (AEPD) and Others*, C-131/12; ECLI: EU:C:2014:317, paragraph 36.

[112] CJEU Judgment of 13 May 2014, *Google Spain SL v. Agencia Española de protección de Datos (AEPD) and Others*, C-131/12; ECLI: EU:C:2014:317, para. 38.

[113] Art. 4.7) GDPR; A. DELFORGE Titre 8. Les obligations générales du responsable du traitement et la place du sous-traitant" in *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Larcier, Bruxelles, 2018, para. 9-12.

[114] EDPB - Guidelines 7/2020 on the concepts of controller and processor in the GDPR, v2.0, 2021, para. 20; L. A. BYGRAVE & L. TOSONI, "Article 4(7). Controller" in *The EU General Data Protection Regulation. A Commentary*, Oxford University Press, 2020, p. 150; B. VAN ALSENOY, *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Intersentia, 2019, para 109-110; A. DELFORGE Titre 8. Les obligations générales du responsable du traitement et la place du sous-traitant" in *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Larcier, Bruxelles, 2018, para. 12.

[115] C. de TERWANGNE, "Titre 2. Définitions clés et champ d'application du RGPD" in *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Larcier, Bruxelles, 2018, para. 9-12.

332. The Inspection Service states that the *Transparency and Consent Framework* does not in itself constitute processing of personal data, but is a set of policy documents and technical specifications developed by IAB Europe and IAB Tech Lab[116]. The Litigation Chamber concurs with this statement by the Inspection Service.

333. However, the Litigation Chamber also found that personal data are processed in the context of the TCF, and more specifically the processing of user preferences, which CMPs record via a user interface and store using the TC String. To enable a standardised approach within the TCF, IAB Europe uses both policy documents and technical specifications:

- The *TCF Policies* consist of rules for participation that apply to *publishers*, *Consent Management Providers* (CMPs) and other *adtech vendors*.
- The technical specifications of the TCF, which provide a technical protocol with which participating organisations can immediately exchange the status of the information provided and the choices of the data subjects. These technical specifications are closely aligned with the *TCF Policies*, in order to provide the technical functionality needed to operationalise the TCF standard.

334. The defendant states in its defence that the processing of those preferences, in accordance with the rules imposed by the TCF on participating organisations, pursues the objective of enabling both website and app publishers and the advertising technology partners who support the *targeting*, delivery and measurement of advertising and content *(adtech vendors*) to obtain users' consent, to transparently disclose their processing purposes, and to establish a valid legal basis for the processing of personal data in order to provide digital advertising, among others[117]. This objective is also reflected in the *IAB Europe Transparency & Consent Framework Policies* (hereinafter "*TCF Policies*")[118]:

> "*ii. The goal of the Framework is to help players in the online ecosystem meet certain requirements of the ePrivacy Directive (and by extension its successor, the upcoming ePrivacy Regulation), and General Data Protection Regulation by providing a way of informing users about inter alia the storing and/or accessing of information on their devices, the fact that their personal data is processed, the purposes for which their personal data is processed, the companies that are seeking to process their personal data for these purposes, providing users with choice about the same, and signalling to third parties inter alia which information has been disclosed to users and what users' choices are*."

[116] Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 9.

[117] Defendant's reply brief, § 33.

[118] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32); IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38).

335. It is also apparent from the documentation drawn up by the defendant that the purposes of the TC String are determined by IAB Europe:

> "*A TC String's primary purpose is to encapsulate and encode all the information disclosed to a user and the expression of their preferences for their personal data processing under the GDPR. Using a Consent Management Platform (CMP), the information is captured into an encoded and compact HTTP-transferable string. This string enables communication of transparency and consent information to entities, or "vendors", that process a user's personal data. Vendors decode a TC String to determine whether they have the necessary legal bases to process a user's personal data for their purposes*." [119]

336. Although the Litigation Chamber emphasises that the purpose of the processing of the TC String must be distinguished from the purposes of the processing that takes place outside the TCF, such as the processing and exchange of the personal data that are part of a *bid request* in the context of OpenRTB, it finds that the TCF is offered *with the aim of indirectly promoting the use of OpenRTB*. In that respect, IAB Europe, in its capacity as *Managing Organisation*, acts as a hinge between TCF and OpenRTB, which, incidentally, was developed by IAB Tech Lab.

337. In support of its standpoint, the Litigation Chamber refers to the inventory of possible purposes that participating organisations may pursue within the context of the TCF. For example, the *TCF Policies* for CMPs, *publishers* and other *adtech vendors* respectively stipulate a mandatory list[120] with fixed and predefined Purposes[121], Special purposes[122], Features[123] and Special features defined by IAB Europe:

- Purpose 1 — Store and/or access information on a device
- Purpose 2 — Select basic ads
- Purpose 3 — Create a personalised ads profile
- Purpose 4 — Select personalised ads
- Purpose 5 — Create a personalised content profile
- Purpose 6 — Select personalised content
- Purpose 7 — Measure ad performance

---

[119] Transparency and Consent String with Global Vendor & CMP List Formats v2.0, August 2019 (Exhibit 35), p. 8.

[120] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 26 ff.

[121] The term "Purpose" refers to one of the defined purposes for processing of data, including users' personal data, by participants in the Framework that are defined in the TCF Policies or the Specifications.

[122] "Special Purpose" means one of the defined purposes for processing of data, including users' personal data, by participants in the Framework that are defined in the TCF Policies or the Specifications for which Vendors declare a Legal Basis in the GVL and for which the user is not given choice by a CMP.

[123] "Feature" means one of the features of processing personal data used by participants in the Framework that are defined in the TCF Policies or the Specifications used in pursuit of one or several Purposes for which the user is not given choice separately to the choice afforded regarding the Purposes for which they are used.

- Purpose 8 — Measure content performance
- Purpose 9 — Apply market research to generate audience insights
- Purpose 10 — Develop and improve products
- Special Purpose 1 — Ensure security, prevent fraud, and debug
- Special Purpose 2 — Technically deliver ads or content
- Feature 1 — Match and combine offline data sources
- Feature 2 — Link different devices
- Feature 3 — Receive and use automatically-sent device characteristics for identification
- Special Feature 1 — Use precise geolocation data
- Special Feature 2 — Actively scan device characteristics for identification

338. The Litigation Chamber concludes from this that the purpose of the TC String, and in the broader sense of the processing of the TC String within the TCF as translated into the *TCF Policies*, has been established by IAB Europe.

B.2.3. - Determining the means for processing personal data within a TCF

339. Determining the means of processing is the second cornerstone of the concept of controllership. With regard to the means of processing, the EDPB makes a distinction between so-called “essential” and “non-essential” means. The choice of non-essential means may, in principle, be left to a processor without any reduction in the responsibility of the entity that determined the purposes[124].

340. "Essential means" are closely linked to the purpose and scope of the processing and are inherently reserved to the controller. Examples of essential means relate to the type of personal data processed ("what data are processed?"), the duration of the processing ("how long are they processed?"), the categories of recipients ("who has access to them?") and the categories of data subjects ("whose personal data are processed?"). "Non-essential means", on the other hand, mainly concern the practical aspects of the implementation, such as the choice of a particular type of hardware or software or the detailed security measures that can be left to the processor to decide[125].

341. It is established by the Litigation Chamber, and also confirmed by the defendant[126], that the *Transparency and Consent Framework* constitutes a framework of binding rules for the participating organisations with regard to the processing of user preferences. Participants

[124] EDPB - Guidelines 7/2020 on the concepts of controller and processor in the GDPR, v2.0, 2021, para. 39-41.
[125] EDPB - Guidelines 07/2020 on the concepts of controller and processor in the GDPR, v2.0, 2021, para. 40.
[126] Defendant's reply brief dd. 25 March 2021, para. 35.

in the TCF are assumed to accept the *Terms and Conditions for the IAB Europe Transparency & Consent Framework* (hereinafter "*Terms and Conditions*")[127] in order to register. By doing so, the Litigation Chamber finds that IAB Europe does not *only* monitor compliance with the TCF specifications and policies, as Managing Organisation. In addition, the defendant is *also* defining the rules applicable to the processing of TC Strings under the TCF, as well as imposing these rules on participating organisations.

342. In the following paragraphs, the Litigation Chamber will examine the extent to which essential means of processing the TC String are actually determined by IAB Europe.

343. Generation, modification and reading of the TC String – In the first place, the *TCF Technical Specifications*[128], the *IAB Europe Transparency and Consent Framework Implementation Guidelines* (hereinafter "*TCF Implementation Guidelines*")[129] and the *TCF Policies*[130] explain how CMPs can collect user approval, must generate a unique TC String, and need to store the value of the TC String.

344. Moreover, CMPs are obliged to register with IAB Europe in order to be able to generate a TC String[131] and must follow the technical specifications developed by IAB Europe in cooperation with IAB Tech Lab regarding the API[132] with which CMPs can generate the TC String and adtech vendors and publishers can read it[133]. These specifications also show that the CMP API plays an essential role in the TCF, as it provides a standardised way for parties, such as the *publisher* or an *advertising vendor*, to access the users' preferences, which are managed by the CMP[134]. The Litigation Chamber notes that the use of this API is mandatory when communicating between CMPs and *adtech vendors*.

345. With regard to the content of the TC String, the *TCF Technical Specifications* specify which information is included, including metadata such as the exact time the TC String was generated or modified.

346. In this regard, the Litigation Chamber refers to the *Wirtschaftsakademie* judgment, in which the Court of Justice held that the entity responsible for laying down, and *a fortiori* imposing, settings in relation to a data processing operation, thereby participates in determining the

---

[127] Terms and Conditions for the IAB Europe Transparency & Consent Framework ("Terms and Conditions") (Exhibit 33).

[128] Transparency and Consent String with Global Vendor & CMP List Formats v2.0, August 2019 (Piece 35).

[129] IAB Europe Transparency and Consent Framework Implementation Guidelines, August 2019 (Exhibit 36).

[130] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32); IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38).

[131] Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 76.

[132] An API is a programming interface that allows you to "plug in" to an application to exchange data. An API is open and offered by the program owner. APIs are used in various fields of digital marketing to enable, for example, automated gateways for data exchange between programs such as Adwords, AdExchange and an agency or vendor. It can also be used by adtech vendors, agencies or software suppliers to automate advertising campaigns.

[133] Consent Management Platform API v2.0, August 2019 (Exhibit 34), p. 4.

[134] Consent Management Platform API v2.0, August 2019 (Exhibit 34), p. 6.

purposes and means of that processing and must therefore be regarded as the data controller[135].

347. Storage location - In their written evidence, the complainants argue that IAB Europe is responsible for managing the internet domain "*consensu.org*", to which the so-called *globally scoped* consent cookies[136] refer and which as such allows CMPs to consult and modify the TC Strings shared across multiple websites or applications.

348. In contrast, IAB Europe states in its submissions that although it has registered the *consensu.org* domain, there is no storage of the TC String on IAB Europe's servers to which that *consensu.org* domain refers. Indeed, IAB Europe delegates a subdomain of *consensu.org* to each registered CMP[137], which stores the TC String on the user's device using a *euconsent-v2* cookie and associates it with the *consensu.org* domain. According to the defendant, it is therefore only the CMP that generates and stores the TC String and the CMP's own servers that read out the TC String.

349. In order to establish the responsibility of IAB Europe for the processing of the TC Strings, it is necessary to determine to what extent the delegation of a sub-domain to a CMP by IAB Europe implies that the defendant establishes at least the means (and any purposes) of such processing.

350. The *TCF Technical Specifications* prescribe that sharing the TC String with CMPs should take place in two ways: either by storing the TC String in a storage system chosen by the CMP, if it is a service-specific consent[138]; or by storing the TC String in a shared *globally scoped consent* cookie associated with the IAB Europe's *consensu.org* internet domain[139].

351. Based on the technical reports and the statements of the parties at the hearing, the Litigation Chamber concludes that a service-specific consent by means of a first-party *euconsent-v2* cookie has been established, and is therefore stored exclusively on the user's device. In this first scenario, the *euconsent-v2* cookie in question will therefore not be linked to the *consensu.org* domain, nor to the subdomain delegated to the CMP by IAB Europe.

352. However, in exceptional cases where the user's consent also applies to other websites, so-called globally scoped consent cookies, CMPs are required to store the relevant TC String

---

[135] CJEU Judgment of 5 June 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, ECLI: EU:C:2017:796, paragraph 39: "In these circumstances, it must be judged that the administrator of a fan page on Facebook, such as Wirtschaftsakademie, by defining settings according to, in particular, its target audience and objectives for the management or promotion of its activities, participates in determining the purposes and means of the processing of personal data of visitors to its fan page".

[136] Which contain the TC Strings.

[137] More specifically, it concerns the subdomain <*name of the CMP*>.mgr.consensu.org. For example, for Onetrust this is https://cookies.onetrust.mgr.consensu.org/.

[138] In concrete terms, this means that the user's consent is only valid for the website visited, and for the purposes accepted and the adtech vendors approved.

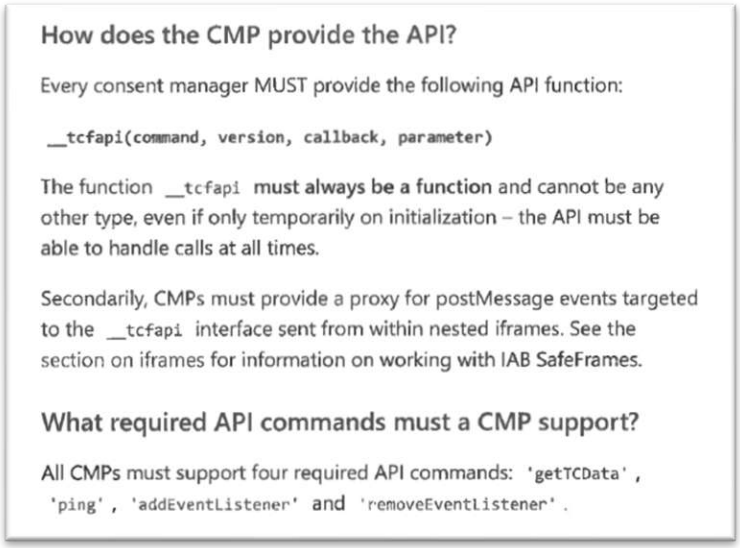
[139] Transparency and Consent String with Global Vendor & CMP List Formats v2.0, August 2019 (Piece 35).

on the user's device by means of a *third-party* cookie, whereby the cookie is associated with the *consensu.org* domain[140]. Only the CMPs are able to read the TC Strings on the user devices.

353. In this second scenario, each CMP is then given a separate sub-domain, assigned by IAB Europe via DNS delegation, where the consent cookie with the TC String is associated with the main domain *consensu.org* and its sub-domains. In concrete terms, this means that the scope of the globally scoped consent cookie includes both the domain *consensu.org* and the subdomains delegated to the CMPs.

354. According to the defendant, the globally scoped consent was only applied to a limited extent and IAB Europe stopped using and supporting it after the hearing. The Litigation Chamber takes note of this, but emphasises that this functionality also indicates that IAB Europe's responsibility goes beyond merely designing a framework.

355. The Litigation Chamber also considers that the defendant establishes the means of processing the TC String as well as the *euconsent-v2* cookie, both for the service-specific and for the globally-scoped consents. The fact that the TCF does not impose a specific mechanism for storing users' consent in the browser but merely recommends that CMPs use a *first-party* cookie does not preclude the finding that the defendant provides a list of possible mechanisms for linking the TC String to an individual user, of which the CMP API is the most common. More specifically, the Litigation Chamber notes that, in its policy document entitled '*Consent Management Platform API*', the defendant prescribes, among other things, the standardised way in which the various parties involved in the TCF can consult the preferences, objections and consents of users[141]:



How does the CMP provide the API?

Every consent manager MUST provide the following API function:

```
__tcfapi(command, version, callback, parameter)
```

The function `__tcfapi` **must always be a function** and cannot be any other type, even if only temporarily on initialization – the API must be able to handle calls at all times.

Secondarily, CMPs must provide a proxy for postMessage events targeted to the `__tcfapi` interface sent from within nested iframes. See the section on iframes for information on working with IAB SafeFrames.

What required API commands must a CMP support?

All CMPs must support four required API commands: `'getTCData'`, `'ping'`, `'addEventListener'` and `'removeEventListener'`.

[140] Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 79.
[141] Consent Management Platform API v2.0, August 2019 (Exhibit 34), p. 6.

356. Categories of recipients of the TC String - The Litigation Chamber also rules that IAB Europe determines with whom the users' preferences are to be shared, by, among other things, providing a list of TCF-registered adtech vendors, the so-called *Global Vendors List* (GVL)[142], as well as a list of permitted CMPs *(Global CMP List*)[143].

357. IAB Europe's documentation shows that *publishers* who wish to use the TCF are obliged to work with a TCF-registered CMP[144]. In addition, the *TCF Implementation Guidelines* state that CMPs are obliged to collect consent and any objections for all purposes and partners chosen by the *publisher*, although this may be extended to all *adtech vendors* included in the GVL[145].

358. Retention period of the TC String - Finally, the two versions of the *TCF Policies* explicitly state that CMPs and participating *adtech vendors* must retain the record of the consent or objection, which is stored in the TC String, for as long as the processing is ongoing and make it available to the Managing Organisation, *i.e.* the defendant, upon the latter's simple request[146]:

> "*8. Record Keeping*
>
> *1. A CMP will maintain records of consent, as required under the Policies and/or the Specifications, and will provide the MO access to such records upon request without undue delay.*
>
> *2. A CMP will retain a record of the UI that has been deployed on any given Publisher at any given time and make this record available to its Publisher client, Vendors, and/or the MO upon request.*
>
> […]
>
> *15. Record Keeping*
>
> *1. A Vendor must maintain records of consent, as required under the Policies and the Specifications, and will provide the MO access to such records upon request without undue delay.*
>
> *2. A Vendor must maintain records of user identification, timestamps, and received Signals for the full duration of the relevant processing. A Vendor may maintain such records of user identification, timestamps, and Signals beyond the duration of the processing as required to comply with legal obligations or to reasonably defend or pursue legal claims, and/or for other processing allowed by law, under a valid legal basis, and consistent with the purposes for which the data was collected."*

---

[142] https://iabeurope.eu/vendor-list/ and https://iabeurope.eu/vendor-list-tcf-v2-0/

[143] https://iabeurope.eu/cmp-list/

[144] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 21

[145] IAB Europe Transparency and Consent Framework Implementation Guidelines, August 2019 (Exhibit 36), p. 13.

[146] IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38), Articles 8 and 15; IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), Articles 8 and 15.

359. The Litigation Chamber therefore finds that IAB Europe bears the responsibility for defining the criteria by which the retention periods of the TC Strings can be determined.

360. It follows from the foregoing that, in addition to the purposes, IAB Europe does in fact determine the means of generating, storing and sharing the TC String by which the preferences, objections and consent of users are processed. The following elements are decisive according to the Litigation Chamber:

i. IAB Europe defines how CMPs can collect consent or objections from users, generate a unique TC String, and store the value of the TC String;

ii. IAB Europe, in collaboration with IAB Tech Lab[147], has developed the technical specifications of the API with which adtech vendors, among others, can access the preferences of the users, which are managed by the CMP, in a standardised way;

iii. IAB Europe determines the storage location and method for both service-specific and globally scoped consent cookies;

iv. IAB Europe manages the lists of registered CMPs and adtech vendors and therefore determines with which possible recipients the data relating to the TC String is communicated;

v. IAB Europe determines the criteria by which the retention periods for TC Strings may be established and the way in which organisations participating in the TCF must make these TC Strings available to the *Managing Organisation*, i.e. the defendant.

361. Based on the foregoing explanations, the Litigation Chamber finds that **the defendant must be considered as data controller for the personal data processing with respect to the registration of the consent signal, objections and users' preferences by means of the TC String, in accordance with the policies and technical specifications of the *Transparency & Consent Framework***.

B.3. - Joint controllership of publishers, CMPs and adtech vendors with regard to the means and purposes of the processing of personal data within the context of the TCF and of the OpenRTB

362. IAB Europe's responsibility does not exclude that there are other data controllers implementing the TCF and relying on the OpenRTB protocol, that have their own or shared responsibility for the personal data processing operations they perform.

[147] IAB Europe worked with IAB Tech Lab to determine the policies for the framework's rules. IAB Europe has also entrusted Tech Lab with the development as well as the hosting of the technical implementations and specifications of the TCF, due to their technological expertise.

B.3.1. - Joint processing responsibility

363. Article 26.1 of the GDPR states that joint responsibility exists when "two or more jointly determine the purposes and means of the processing". The Court of Justice specified that 'the existence of joint responsibility of the various actors does not necessarily mean that they are equally responsible for one and the same processing of personal data. On the contrary, those actors may be involved at different stages and to different degrees, so that the assessment of the level of responsibility of each of them must take account of all the relevant circumstances of the particular case'[148].

364. Again, the EDPB further explained that the assessment of joint processing responsibility should be based on a factual rather than a formal analysis of the actual impact on the purposes and means of processing[149].

365. First of all, the Litigation Chamber underlines that an *identical* decision does not necessarily have to exist in order to speak of joint processing responsibility; it is sufficient that the defined purposes are complementary to each other[150]. The EDPB also emphasises that joint participation in the definition of the means and purposes may take the form of a common decision as well as result from different yet *converging* decisions of two or more entities regarding the purposes and essential means of a data processing operation[151].

366. **Decisions may be considered to be convergent if they are complementary and necessary for the processing in a way that confers a tangible influence on the determination of the purposes and means of processing**. The question to be asked is whether the *intended* processing of personal data would be impossible without the participation of all parties, more specifically, whether the processing activities carried out by each party are inseparable and indivisible.

367. Both in its submissions and during the hearing, IAB Europe emphasised that the TCF and the OpenRTB system are completely independent from each other, in the sense that even without participation in the TCF, adtech vendors can freely process personal data within the context of the OpenRTB. On the other hand, the complainants have always referred to the

---

[148] CJEU Judgment of 10 July 2018, *Tietosuojavaltuutettu et Jehovan todistajat - uskonnollinen yhdyskunta*, C-25/17, ECLI:EU:C:2018:551, para. 66 and CJEU Judgment of 29 July 2019, *Fashion ID GmbH & Co. KG*, C-40/17, ECLI:EU:C:2019:629, para. 70.

[149] EDPB - Guidelines 7/2020 on the concepts of controller and processor in the GDPR, v2.0, 2021, para. 52.

[150] Opinion of Advocate General Bobek in *Fashion ID*, C-40/17, ECLI: EU:C:2018:1039, paragraph 105: "Even though the specific commercial use of the data may not be the same, both the defendant and Facebook Ireland appear to be pursuing commercial purposes in general that appear to be complementary. Although there is no identical purpose, there is a unity of purpose, namely a commercial and an advertising purpose."

[151] EDPB - Guidelines 7/2020 on the concepts of controller and processor in the GDPR, v2.0, 2021, para. 54.

inherent interconnectedness between OpenRTB and the TCF, which the defendant itself would confirm - according to the complainants - in the *TCF Implementation Guidelines*[152].

368. The Litigation Chamber finds that the defendant's argument cannot be followed, given that the defendant repeatedly states in its submissions, that the reason for the existence of the TCF is precisely to bring the processing of personal data based on the OpenRTB protocol, among others, into conformity with the applicable regulations, including the GDPR and the ePrivacy directive. Although the Litigation Chamber understands that the TCF may also be used by *publishers* for other applications[153] *,* whether or not in collaboration with CMPs, it is equally certain that the TCF was never intended to be a stand-alone, independent ecosystem.

369. On the contrary, the Litigation Chamber notes that the *Transparency and Consent Framework* includes policies and technical specifications that should enable website and application publishers *(publishers)* and adtech partners that support the *targeting*, delivery and measurement of advertising and content *(adtech vendors*) to disclose transparently their processing purposes, to establish a legal basis for the processing of personal data for the provision of digital advertising, and to obtain consent or identify objections of users[154].

370. **Thus, the Litigation Chamber finds that the decisions translated by IAB Europe into the provisions of the TCF policies and technical specifications, on the one hand, and the means and purposes determined by the participating organisations in relation to the processing - whether or not in the context of OpenRTB - of users' personal data, , on the other hand, must be regarded as convergent decisions[155]. 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, but to facilitate further processing by third parties (*i.e.* publishers and adtech vendors)**.

371. As a result, the Litigation Chamber finds that IAB Europe and the respective participating organisations should be considered as joint controllers for the collection and subsequent dissemination of users' consent, objections and preferences, as well as for the related processing of their personal data, without the responsibility of participating CMPs and *adtech vendors* detracting from IAB Europe's responsibility.

---

[152] https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/TCF-Implementation-Guidelines.md#how-does-the-tc-string-apply-to-non-openrtb-situations.

[153] Thus, the TCF can also be used for non-marketing-related purposes, e.g. *audience measurement*, *performance measurement*, etc.

[154] Defendant's reply brief dd. 25 March 2021, para. 33.

[155] See para. 365-366.

a. Consent Management Platforms (CMPs)

372. The CMPs ensure the technical implementation of consent banners through which data subjects indicate their choices regarding the processing of their personal data.

373. Specifically, CMPs have the function of storing users' consent, objections and preferences in the TC String, then storing the value in the form of a *euconsent-v2* cookie in the browsers used to visit the website, and finally providing an API to adtech vendors so that they can access the consent, objection and preference values for each individual user[156].

374. CMPs that wish to register in the IAB Europe TCF v2.0 should implement the standardised processing purposes and functionalities in their user interface to collect and store the preferences of the data subject in this regard[157]. They must also comply with the applicable lawful principles, as set out in the IAB Europe TCF v2.0.

375. The Litigation Chamber has already established that the TC String in itself does not directly identify persons or devices. However, once the TC String is placed on the user's device, a CMP can assign a unique identifier to this TC String, *i.e.* the IP address of the device on which it is placed in the form of an *euconsent-v2* cookie[158].

376. To provide a CMP interface to users, *publishers* need to implement the CMP JavaScript code on their website. This code is then loaded directly from the CMP server or via the delegated subdomain. As a result of this HTTP(S) request, both the *publisher*'s server and the CMP's server gain access to the IP address of the user visiting the website and seeing the CMP interface[159].

377. Access to that IP address allows CMPs to enrich the consent, objection and preferences contained in the TC String with other information already in their possession or in the possession of the *publisher* and linked to that same IP address. On this basis, the Litigation Chamber concludes that CMPs process a large number of personal data.

378. The Litigation Chamber assesses the extent to which the CMPs act as processors or as (joint) controllers in the following paragraphs.

379. According to the defendant, as laid down in its TCF Policies, CMPs are in principle considered to be processors[160]. The Litigation Chamber disagrees with this view for the following reasons. The CMPs' main task is to develop and provide interfaces that can have

---

[156] C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, "Consent Management Platforms Under the GDPR: Processors and/or Controllers?", in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, p. 50.

[157] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 9 ff.

[158] See para. 302 et seq. of this decision. See also C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, "Consent Management Platforms Under the GDPR: Processors and/or Controllers?", in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, p. 50.

[159] *Ibidem*, p. 5.

[160] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 9 ff.

a direct impact on the choice of the data subjects. The CMPs therefore play a key role, not only in the context of the TCF, but also with regard to the processing of personal data under the OpenRTB. They are therefore obliged to comply with the data protection principles laid down in Article 5.1 of the GDPR (lawfulness, fairness and transparency of the processing of personal data).

380. Although the *TCF Policies* prohibit CMPs from giving any preference to particular adtech vendors on the *Global Vendors List*, and they must therefore in principle present all registered adtech vendors to users, unless otherwise provided by the *publishers*[161], some authors note that a number of CMPs do not comply with this requirement. This is done either by imposing pre-selected adtech vendors on the *publishers* or by denying them the possibility of deviating from the full list of adtech vendors by default[162].

381. It is also worth noting that CMPs have a wide margin of appreciation regarding the interface they offer to users. After all, the TCF policies impose only *minimum interface requirements* on participating CMPs[163], with the result that in practice the interfaces and compliance with the principles of fairness and transparency can vary greatly depending on which CMP the website and application *publishers* work with[164].

382. The foregoing findings lead the Litigation Chamber to conclude that CMPs play a significant role and therefore bear (joint) responsibility[165] with regard to the purposes and means of the processing of users' personal data within the TCF and the OpenRTB system.

383. The Litigation Chamber notes, however, that this conclusion does not mean that all CMPs must systematically be considered as joint-controllers together with IAB Europe and the website publishers, or that the scope of the joint-controllership is without boundaries. As explained earlier in this decision[166], the list of CMPs implementing the TCF is limitative[167] due to the mandatory registration and approval process with IAB Europe, as Managing Organisation. The Litigation Chamber finds the joint controllership established in relation to, respectively:

    i. the website or application publisher,

    ii. the specific CMP implemented by the publisher and providing the TCF interface to users,

---

[161] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 9, § 8 and p. 10, § 11.

[162] C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, "Consent Management Platforms Under the GDPR: Processors and/or Controllers?", in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, pp. 57-59.

[163] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 61 ff.

[164] Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), pp. 99-103.

[165] See para. 360 of this decision on the processing responsibility of IAB Europe for determining the recipients.

[166] See para. 102; 341 ; 344; 356-360; and 374.

[167] As of November 2021, the list of registered CMPs comprises 76 entries: https://iabeurope.eu/cmp-list/.

iii. IAB Europe, as Managing Organization.

In this respect, the Litigation Chamber underlines that appropriate arrangements must be made between the respective joint-controllers, in accordance with the requirements foreseen under Article 26 GDPR.

384. CMPs are in principle required under the TCF Policies — developed and administered by the defendant — to offer by default *all* TCF-registered adtech vendors in their interface. If CMPs apply the TCF Policies, the Litigation Chamber finds that the defendant is responsible for the essential means of processing, since IAB Europe determines the recipients of the personal data collected, and is thus jointly responsible for the transmission of the personal data, including some data in the *bid request*.

385. If, on the other hand, the CMPs deviate from the TCF Policies, the Litigation Chamber considers that this time the CMPs themselves act as data controllers in respect of the recipients of the personal data. To the extent that CMPs do not comply with the instructions imposed on them, they themselves are fully responsible[168], in line with Article 28.10 GDPR.

386. Finally, when the CMPs determine the list of recipients in accordance with the *publishers*' instructions, the Litigation Chamber finds that the *publishers* bear the main responsibility for the transfer of personal data to adtech vendors, without prejudice to IAB Europe's responsibility, without which the global list of participating *adtech vendors* would not exist in the first place.

b. *Publishers*

387. *Publishers* usually act as data controllers in the context of the TCF, as they are supposed to decide whether or not to cooperate with a registered CMP, and are also able to determine which adtech vendors are allowed to advertise on their website or in their application. In addition, *publishers* can exercise control over the legal ground for a specific processing purpose, and they can exclude certain processing purposes[169].

388. *Bid requests* are sent by *supply-side platforms* (SSPs), in their capacity as representatives of the *publishers*, to *demand-side platforms* (DSPs), which represent adtech vendors. The format and content (or "attributes") of such *bid requests* are determined in accordance with the technical specifications of the OpenRTB protocol, independently of the TCF.

389. As confirmed by the reports of the Inspection Service, IAB Europe is not involved in determining the attributes of a specific *bid request*. It is primarily the publishers of websites

[168] EDPB - Guidelines 7.2020 on the concepts of controller and processor in the GDPR, v2.0, para. 150.
[169] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 21-22.

and applications who decide which attributes are included in a *bid request* and passed on to the adtech vendors.

390. A *bid request* contains at least a unique identifier for each *bid request (Bid ID*) and a unique identifier for the advertising space being auctioned *(Item ID*). In addition, a *bid request* will typically contain information about the user device, user details, website or application, and technical details about the advertising space *(Impression*)[170].

391. On the basis of the foregoing, the Litigation Chamber finds that the *bid request* contains the most personal data, and that these data are not processed by the defendant, but mainly by the *publishers*, the CMPs and the various *adtech vendors* who, in principle, are all required to comply with the values of the TC String, in accordance with the policies of the TCF.

392. To the extent that a *publisher* relies on a CMP that has implemented the TCF, the *bid request* will also contain a TC String indicating the preferences of the website visitor or application user. The Litigation Chamber is of the opinion that this can be considered not only as additional evidence that the TC String is indeed personal data, as it concerns information relating to an *identifiable* natural person[171], but also demonstrates that the preferences stored in the TC String have a direct and significant effect on the subsequent processing activities.

393. Therefore, if a user knowingly or unknowingly gives his consent by means of an "*accept all*" button in a CMP interface, and both the website publisher and the CMP have not deviated from the full list of participating adtech vendors, this means that the personal data of the data subject will be shared with hundreds of third parties.

394. In line with its previous submission with regard to CMPs[172], the Litigation Chamber rules that *publishers* also act as data controllers for the processing of users' preferences in a TC String as well as their personal data processed in a *bid request.*

395. In addition, the Litigation Chamber refers to Article 23.5 of the *TCF Policies*, which prohibits *publishers* from changing the processing purposes, or giving CMPs any instruction to that effect[173].

396. Therefore, insofar as the *publishers* decide not to deviate from the proposed default list of *adtech vendors* and accept all the proposed processing purposes, the Litigation Chamber also considers that IAB Europe is acting as a joint data controller with the *publishers* in

[170] Technical Analysis Report of the Inspection Service, 4 June 2019 (Exhibit 24), pp. 12-13.
[171] See para. 291 et seq. of this decision.
[172] See para. 382 et seq. of this decision.
[173] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 22-23.

respect of the recipients of the TC String as well as the processing purposes for which the users' personal data will be processed.

c. Adtech vendors

397. The Litigation Chamber has already determined that IAB Europe bears responsibility with regard to defining the various processing purposes under the TCF[174].

398. When registering for TCF v2.0, adtech vendors must also choose the intended processing purposes and possible bases, based on a predetermined, fixed list of purposes.

399. In this sense, the Litigation Chamber finds that the adtech vendors, together with the defendant, are jointly responsible for the processing operations that take place within the context of the OpenRTB for the processing purposes foreseen under the TCF and in accordance with the preferences, objections and consents collected within the TCF. The latter aspect, however, does not affect the role that adtech vendors themselves play when they specify the purposes for which they themselves wish to process the personal data contained in a *bid request*, or for subsequent data processing not provided for under the TCF[175].

400. Moreover, the Litigation Chamber makes it clear that, similarly to the CMPs, adtech vendors are also required to register with the TCF in order to benefit from it. This means that the joint-controllership is limited to the registered adtech vendors[176].

d. Assessment by the Litigation Chamber

401. This factual analysis of the role of CMPs, publishers and adtech vendors shows that the decisions on determining the purposes and means of the processing activities carried out by the defendant within the context of the TCF (which aim to bring the processing activities carried out by the aforementioned participating organisations in line with the GDPR and the ePrivacy Directive) complement the decisions regarding the purposes and means of the processing activities carried out by the participating organisations under the OpenRTB and should thus be regarded as convergent decisions.

402. **This leads the Litigation Chamber to the conclusion that the defendant as well as the CMPs, publishers and participating adtech vendors should be regarded as joint data controllers for the collection and dissemination of users' preferences, objections and consent and for the subsequent processing of their personal data**.

[174] See para. 331 *et seq*. of this decision.
[175] WP171 - Opinion 2.2010 on Online Behavioural Advertising, pp. 10-11.
[176] https://iabeurope.eu/vendor-list-tcf-v2-0/.

B.4. On the alleged breaches of the General Data Protection Regulation

B.4.1 - Lawfulness and fairness of processing (Art. 5.1.a and 6 GDPR)

403. With regard to the lawfulness and fairness of the processing, the Litigation Chamber distinguishes two processing activities: on the one hand, the capture itself of the consent signal, objections and preferences of users in the TC String by the CMPs (a), and, on the other hand, the collection and dissemination of the users' personal data by the participating organisations (b).

a. Registration of the consent signal, objections and users' preferences by means of the TC String

404. The Litigation Chamber finds that users are not informed anywhere of the lawful basis for the processing of their own, individual preferences in relation to purposes and permitted adtech vendors by CMPs.

405. The underlying reasoning of the defendant in this regard is that the TC String is not personal data and therefore no basis for its processing is required.

406. As already established, the Litigation Chamber does not agree with the defendant's position[177]. The Litigation Chamber has established that the generation and dissemination of the TC String does involve the processing of personal data.[178] Consequently, this processing must in any case be based on one of the exhaustively listed processing grounds under Article 6 of the GDPR. For this reason, the Litigation Chamber will consider the question of whether one of the legal bases of Article 6 GDPR can be relied on.

407. First of all, the Litigation Chamber finds that neither the *TCF Policies* nor the *TCF Implementation Guidelines* mention an obligation on the part of the CMPs to obtain the unambiguous consent of users before capturing their preferences in a TC String, which is placed on the end devices of users thanks to a *euconsent-v2* cookie. Furthermore, users are never informed about the processing of their preferences by the TC String, with whom their preferences are shared, nor how long their preferences are stored. Since the visitors' consent is never asked, Article 6.1.a *de facto* does not apply as a legal basis for this processing.

408. In addition, the Litigation Chamber points out that Article 6.1.*b* is *prima facie* not applicable to the processing of user preferences and the TC String. In the majority of the cases, even if there were a contractual relationship between the users and the publisher, the data processing involved under the TCF would still not meet the requirement of objective

[177] See *supra* B.1.1. – Presence of personal data within the TCF.
[178] See *supra* B.1.2. - Processing of personal data within the TCF.

necessity for the provision of online services by the publishers to the users concerned (in particular for processing for the purposes of personalisation of content and for advertising based on surfing behaviour)[179].

409. In the absence of any contractual relationship between the data subjects and CMPs or IAB Europe, as well as an unambiguous consent given by the users for placing a *euconsent-v2* cookie, the Litigation Chamber must assess whether Article 6.1.f (legitimate interest) could serve as legal basis: does the legitimate interest pass the threefold test of the CJEU and, if so, could Article 6.1.f GDPR serve as a basis for this preliminary processing of the users' preferences by CMPs, in accordance with the means and purposes as set out by IAB Europe in its *TCF Policies* and *TCF Implementation Guidelines*?

410. In order to rely on Article 6.1.*f* GDPR as a legal ground for the processing of personal data, the legitimate interest of the controller or third parties, which is closely related to (yet distinct from) the concept of processing purpose, must be balanced against the interests or fundamental rights and freedoms of the data subjects. Whereas 'purpose' refers to the specific reason why the data are processed, *i.e.* the aim or intention of the data processing, the notion of interest is linked to the broader stake that a controller may have in the processing, or the benefit that the controller — or a third party, which must not necessarily qualify as a co-controller in respect of the data processing — derives from the processing[180].

411. Pursuant to Article 6.1.*f* of the GDPR and the case law of the Court of Justice, three cumulative conditions must be met in order for a controller to be able to validly rely on this grounds for lawfulness, "*namely, firstly, the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, secondly, the necessity of processing the personal data for the purposes of the legitimate interest pursued and, thirdly, the condition that the fundamental rights and freedoms of the data subject are not prejudiced*" (Rigas judgment[181]).

412. In order to be able to invoke the ground for lawfulness of "legitimate interest" under Article 6.1.*f* of the GDPR, the controller must demonstrate, in other words, that:

    1) the interests it pursues with the processing can be recognised as legitimate (the 'purpose test');

---

[179] EDPB - Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, v2.0, 8 October 2019, para. 23 *et seq*., para. 52 *et seq*. and para. 57 *et seq*., https://edpb.europa.eu. This is a situation different from the pending case before the Court of Justice C-446/21, Maximilian Schrems vs. Facebook Ireland Ltd.

[180] CJEU Judgment of 11 December 2019, *TK v. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 44.

[181] CJEU Judgment of 4 May 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde t. Rīgas pašvaldības SIA "Rīgas satiksme"*, C-13/16; ECLI: EU:C:2017:336, paragraphs 28-31. See also CJEU Judgment of 11 December 2019, *TK v. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 40.

2) the processing envisaged is necessary for the purposes of achieving those interests (the "necessity test"); and

3) the balancing of these interests against the interests, fundamental freedoms and rights of data subjects weighs in favour of the data controller or a third party (the "balancing test").

413. As regards the first condition, the Litigation Chamber considers that the purpose of capturing users' approval and preferences in order to ensure and be able to demonstrate that users have validly consented to or not objected to the processing of their personal data for advertising purposes may be considered to be carried out for a legitimate interest.

414. The interest pursued by the defendant as the data controller may, in accordance with recital 47 of the GDPR, be regarded as legitimate in itself. More specifically, the possibility of storing the preferences of users[182] is an essential part of the TCF and the Litigation Chamber notes that this is done in the legitimate interest of the defendant as well as of third parties involved, such as the participating *adtech vendors*.

415. Thus, the first condition set out in Article 6.1.*f* of the GDPR is fulfilled.

416. In order to fulfil the second condition, it must then be demonstrated that the processing is *necessary* for the achievement of the purposes pursued. This means, in particular, that the question must be asked whether the same result can be achieved by other means without processing personal data or without processing that is unnecessarily burdensome for the data subjects.

417. In view of the objective of enabling both website or application publishers and participating adtech providers to communicate the purposes of their processing in a transparent manner, to establish a valid legal basis for the processing of personal data for the purpose of providing digital advertising, and to obtain consent — or to identify whether an objection has been raised to the processing of data based on their legitimate interest[183], the Litigation Chamber must verify whether the personal data included in the TC String are limited to what is strictly necessary to capture the consent, objections and preferences of a specific user.

418. This second condition is also met by compliance with the principle of data minimisation (Article 5.1.*c* of the GDPR). The Litigation Chamber notes that the information processed in a TC String[184] is limited to data that are strictly necessary to achieve the intended purpose.

---

[182] Including the collection of a valid consent prior to the processing of personal data, or the possibility for the users to object to a processing based on Article 6.1.*f* GDPR at the time of the collection of personal data.

[183] IAB Europe *Transparency & Consent Framework - Policies*, Version 2020-11-18.3.2a, p. 5, https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

[184] See para. 300 and 301 of this decision.

In addition, based on the documents in this file and the parties' defences, the Litigation Chamber has not been able to establish that the TC String is retained indefinitely.

419. In order to verify whether the third condition of Article 6.1.*f* of the GDPR — the so-called "balancing test" between the interests of the data controller, on the one hand, and the fundamental freedoms and rights of the data subject, on the other hand — can be met, the reasonable expectations of the data subject must be taken into account in accordance with recital 47 of the GDPR. In particular, it should be evaluated whether the data subject "may reasonably expect, at the time and in the context of the collection of personal data, that processing may take place for that purpose"[185].

420. This is also emphasised by the Court of Justice in its judgment "*Asociaţia de Proprietari bloc M5A-ScaraA*"[186], in which it states:

> "*Also relevant for this are the data subject 's reasonable expectations that his or her personal data will not be processed when, in the given circumstances of the case, the data subject cannot reasonably expect further processing of the data.*"

421. In this regard, the Litigation Chamber finds it remarkable that no option is offered to users to completely oppose the processing of their preferences in the context of the TCF. Regardless of which choice they make, the CMP will generate a TC String before linking it to the user's unique User ID through a *euconsent-v2* cookie placed on the data subject's end device.

422. Moreover, since users are not informed of the installation of an *euconsent-v2* cookie on their terminal device, whether or not they agree with the purposes and adtech vendors offered by the CMP, and moreover they are not informed of their right to object to such processing, the Litigation Chamber finds that the last condition of Article 6.1.*f* of the GDPR is currently not met.

423. The severity of the breach of the data subject's rights and freedoms is also an essential element of the assessment under Article 6.1.*f* GDPR. The result of this assessment depends on the particular circumstances of a specific case[187]. In this context, according to the Court of Justice, particular account should be taken of 'the nature of the personal data concerned, in particular their potentially sensitive nature, and of the nature and specific way in which they are processed, in particular the number of persons having access to them and the way in which they acquire such access'[188]. In this context, the Litigation Chamber

---

[185] Recital 47 of the GDPR.

[186] CJEU Judgment of 11 December 2019, *TK v. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 58.

[187] *Ibidem*, para. 56.

[188] CJEU Judgment of 11 December 2019, *TK v. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 57.

emphasises the large number of participating organisations that are given access to the TC String, in addition to the reduced control by the data subjects over the nature and the scope of the processing of their personal data by these organisations.

424. In the absence of a valid legal basis, the Litigation Chamber rules that the data processing in the context of the TCF in its current format, whereby CMPs capture the preferences of online users in a TC String, does not comply with Article 6 of the GDPR.

425. It is therefore undeniable to the Litigation Chamber that IAB Europe, as *Managing Organisation* for the TCF, has failed to provide a legal basis for the processing of user preferences in the form of a TC String and has therefore breached article 6 GDPR.

b. Collection and dissemination of personal data in the context of the RTB

426. It is in no way disputed that the TCF is aimed at capturing, through the interfaces offered by the CMPs, the consent of users or their lack of objection to the legitimate interests of the participating *adtech vendors*.

427. For the record, the Litigation Chamber emphasises that these two bases relate to processing activities that take place under the RTB, in accordance with the OpenRTB protocol.

428. However, the Litigation Chamber finds that none of the legal grounds proposed and implemented by the TCF can be lawfully invoked by TCF participants. First of all, the Litigation Chamber considers that the consent of the data subjects obtained through CMPs is not legally valid *(i*) nor is the (pre)contractual necessity applicable *(ii*). Furthermore, the Litigation Chamber finds that the legitimate interest does not meet the threefold test of the CJEU *(iii*). Thus, Article 6 of the GDPR is infringed.

(i) - Consent is not a valid basis for the processing operations in the OpenRTB facilitated by the TCF

429. In order to ensure that *publishers* and *adtech vendors* comply with the stricter transparency and consent requirements under the GDPR with respect to the processing of personal data in the context of OpenRTB (or RTB in general), CMPs provide a relatively standardised interface for users to choose whether to consent or object to the transfer of their personal data to hundreds of third parties at once, for specified purposes.

430. On the basis of the documents in this file, the Litigation Chamber understands that the participants can pursue one or more purposes from the 12 standardised purposes that the

TCF makes available to participating adtech vendors and that are offered to users by means of the CMPs[189].

431. However, the system of CMPs poses problems on several levels, with the result that the consent obtained by these CMPs (via the TCF) for the processing carried out in the context of the OpenRTB is not legally valid in light of Article 7 GDPR.

432. In order to be used as a legitimate basis, consent under Article 7 of the GDPR must meet strict conditions. However, for the reasons set out below, the Litigation Chamber finds that the consent collected by CMPs and publishers in the current version of the TCF is insufficiently free, specific, informed and unambiguous.

433. First of all, the Litigation Chamber finds that the proposed processing purposes are not sufficiently clearly described, and in some cases are even misleading[190]. By way of example, the Litigation Chamber finds that purpose 8 ("*Measure content performance*") and 9 ("*Apply market research to generate audience insights*")[191] provide little or no insight into the scope of the processing, the nature of the personal data processed or for how long the personal data processed will be retained if the user does not withdraw his consent.

434. Furthermore, based on the documents in the file, the Litigation Chamber understands that the *user interface* of the CMPs does not provide an overview of the categories of data collected, which makes it impossible for users to give their informed consent.

435. The Litigation Chamber also notes that the TCF makes it particularly difficult for users to obtain more information about the identity of all data controllers to whom they give consent to process their data for certain purposes before obtaining their consent. In particular, the recipients for whom consent is obtained are so numerous that users would need a disproportionate amount of time to read this information, which means that their consent can rarely be sufficiently informed.

436. Moreover, the information CMPs provide to users remains too general to reflect the specific processing operations of each vendor, thus preventing the necessary granularity of consent.

437. In addition, the Litigation Chamber takes the view that the enrichment of the data in a *bid request* with personal data already held by the *adtech vendors* and the relevant *Data Management Platforms* means that users cannot possibly be properly informed, since the TCF in its current format does not provide for participating organisations to indicate what

[189] For an overview of these TCF purposes, see para. 337 of this decision.
[190] See para. 465 *et seq*. of this decision.
[191] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 34-36.

personal data they already hold and what processing operations they already perform with these data.

438. Finally, the Litigation Chamber finds that consent, once obtained by CMPs, cannot be withdrawn by users as easily as it was given, as required by Article 7 GDPR. First of all, the Litigation Chamber notes that under the *TCF Policies*, *adtech vendors* are required to comply with a user's consent signals in real time[192], while no measure is provided to ensure that *adtech vendors* cannot continue their processing based on a previously received consent signal. After all, the TCF does not provide for proactive communication of the changed consent signals to the *adtech vendors*. In addition, *adtech vendors* can in principle no longer access the personal data of the data subject after the latter has withdrawn his consent, which also means that they cannot identify the user for whom consent has been withdrawn as such, with the result that the *adtech vendors* will continue to process the personal data of the user in question[193].

439. Indeed, the Litigation Chamber understands that CMPs are at the intersection between users and participating *adtech vendors*, who receive their personal data and then process them for their own purposes. Such a configuration therefore means that the withdrawal of a consent via a CMP will only take effect as soon as the *vendor* concerned reads the new values in the modified TC String via the CMP API. In other words, the withdrawal of consent is never immediate and thus cannot be considered effective.

440. Therefore, the Litigation Chamber concludes that Article 6.1.*a* GDPR does not constitute a valid legal basis for the processing and dissemination of personal data in the context of the OpenRTB, insofar as such consent was obtained in accordance with the TCF in its current format.

(ii) - The legitimate interest of the participating organisations does not outweigh the protection of the fundamental rights and freedoms of the data subjects.

441. The question is then to what extent the organisations participating both in the TCF and the OpenRTB *(adtech vendors*) can legitimately rely on Article 6.1.*f* GDPR for the predefined processing purposes that entail targeted advertising or profiling of the users, as opposed to non-marketing related purposes such as audience measurement and performance measurement.

442. As referred to previously[194], the assessment of the legitimate interests should be done on the basis of the three steps approach established by the Court of Justice. This assessment

---

[192] IAB Europe Transparency & Consent Framework Policies v2020-11-18.3.2.a (Exhibit B.13), p. 14.

[193] For more information, see: M. VEALE, FR. ZUIDERVEEN BORGESIUS, "Adtech and Real-Time Bidding under European Data Protection Law", *German Law Journal*, 31 July 2021, p. 26.

[194] See para. 411 *et seq.*

shall be conducted by the data controllers prior to a processing operation based on Article 6.1.f GDPR. They determine the means and purposes of the intended personal data processing activities and are thus able to apply appropriate safeguards to prevent a disproportionate impact on the data subjects. In case of several controllers which are jointly responsible, the principles of accountability and transparency require that the assessment should be performed jointly by all the data controllers involved in the processing.

443. As stated by the Article 29 Working Party, both positive and negative consequences should be taken into consideration when assessing the impact of the processing, which must be necessary and proportionate to achieve the legitimate interests pursued by the data controllers or a third party. Such consequences may include "potential future decisions or actions by third parties, and situations where the processing may lead to the exclusion of, or discrimination against, individuals, defamation, or more broadly, situations where there is a risk of damaging the reputation, negotiating power, or autonomy of the data subject"[195] .

444. With regard to the purpose test, in particular whether the interests pursued by *publishers* and adtech vendors in processing personal data can be recognised as legitimate, the Litigation Chamber understands that the participating organisations have an interest in collecting and processing users' personal data in order to be able to offer tailor-made advertisements.

445. Based on the case law of the Court of Justice and the guidelines of the EDPB, the Litigation Chamber finds that the notion of legitimate interest can have a broad scope, with the understanding that an interest invoked by a data controller must be sufficiently specific, existent, current, and not hypothetical[196].

446. In this regard, the Litigation Chamber can only note that the proposed processing purposes are described in general terms, with the result that it is not easy for users to assess to what extent the collection, dissemination and processing of their personal data are necessary for the intended purposes, insofar as these are also understood by the users.

447. In order to be relevant, a legitimate interest must be in accordance with applicable EU and national law; sufficiently specific and clearly articulated to allow the balancing test to be carried out, and represent a real and present interest. Hence, merely invoking a legitimate interest in the processing of personal data is not sufficient; the outcome of the balancing test will determine whether Article 6.1.*f* GDPR can be relied upon[197].

---

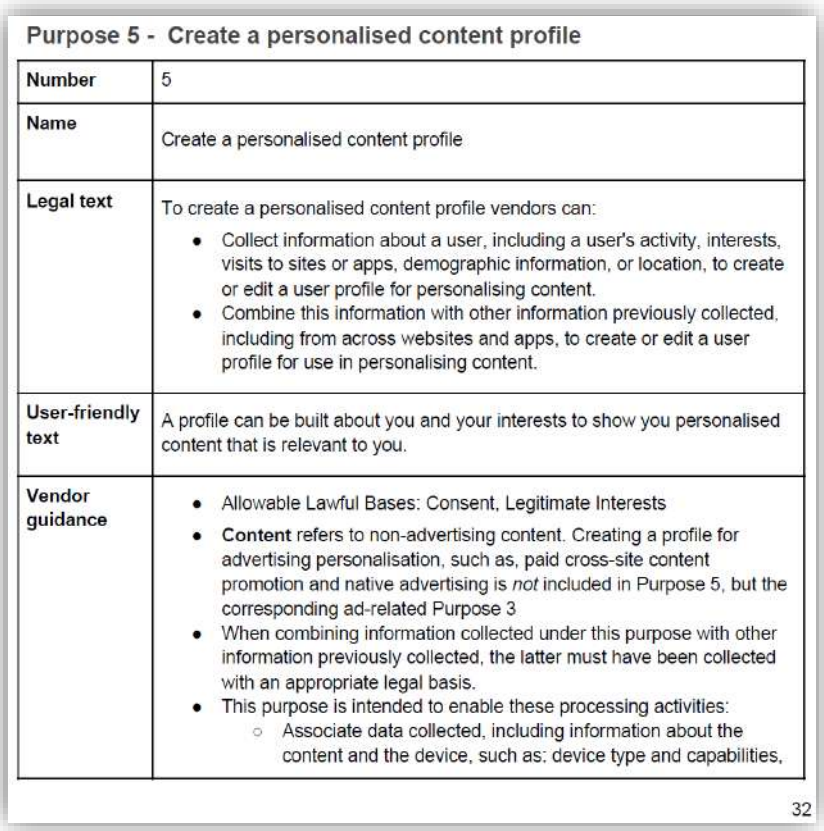
[195] Article 29 Working Party – Opinion 06.2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95-46-EC (WP217), p. 37.
[196] CJEU Judgment of 11 December 2019, *TK v. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 44.
[197] *Ibidem*, p. 25.

448. The *TCF Policies* do not foresee an obligation for the CMPs to explain the legitimate interests at stake in clear terms to the users. Instead, the specific user interface (UI) requirements contained in the *TCF Policies* for framework UIs in connection with legitimate interests, only require from the CMPs that a secondary information layer be provided[198], allowing the users to:

   i. see information about the fact that personal data is processed, and the nature of the personal data processed (e.g. unique identifiers, browsing data);
   ii. see information about the scope of the legitimate interest processing and scope of any objection to such processing;
   iii. access settings within the Framework UI to object to processing of their personal data on the basis of a legitimate interest;
   iv. review the list of processing purposes including their standard name and their full standard description, as defined in Appendix A of the TCF Policies, and to provide users with a way to see which vendors are processing their data for each of the purposes on the basis of a legitimate interest;
   v. exercise their right to object, either with respect to each adtech provider whose processing is based on legitimate interest or, separately, for each purpose pursued by adtech providers on the basis of legitimate interest;
   vi. review the list of named vendors, their purposes and legal bases, and find a link to each vendor's privacy policy.

449. By way of example, the Litigation Chamber refers to the definitions for processing purpose 5 (Create a personalised content profile), in Appendix A of the TCF Policies[199]:

[198] IAB Europe Transparency & Consent Framework Policies v2020-11-18.3.2a, pp. 67-68.
[199] IAB Europe Transparency & Consent Framework Policies v2020-11-18.3.2a, p. 32.



Purpose 5 - Create a personalised content profile

Number	5
Name	Create a personalised content profile
Legal text	To create a personalised content profile vendors can: • Collect information about a user, including a user's activity, interests, visits to sites or apps, demographic information, or location, to create or edit a user profile for personalising content. • Combine this information with other information previously collected, including from across websites and apps, to create or edit a user profile for use in personalising content.
User-friendly text	A profile can be built about you and your interests to show you personalised content that is relevant to you.
Vendor guidance	• Allowable Lawful Bases: Consent, Legitimate Interests • **Content** refers to non-advertising content. Creating a profile for advertising personalisation, such as, paid cross-site content promotion and native advertising is *not* included in Purpose 5, but the corresponding ad-related Purpose 3 • When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate legal basis. • This purpose is intended to enable these processing activities: ○ Associate data collected, including information about the content and the device, such as: device type and capabilities,

32

450. Notwithstanding the fact that the TCF Policies state that they establish minimum requirements for language, design and other elements in the Framework UI, intended to align with legal requirements of EU privacy and data protection law, the Litigation Chamber also notes that the general rules and requirements for framework UIs further specify that:

> "*b. When providing transparency about Purposes and Features, the Framework UI must do so only on the basis of the standard Purpose, Special Purpose, Feature, and Special Feature names and definitions of Appendix A as they are published on the Global Vendor List or using Stacks*[200] *in accordance with the Policies and Specifications. UIs must make available the standard legal text of Purposes, Special Purposes, Features, and Special Features of Appendix A but may substitute or supplement the standard legal definitions with the standard user friendly text of Appendix A so long as the legal text remains available to the user and it is explained that these legal texts are definitive.*"

451. The Litigation Chamber interprets these general rules as prohibiting CMPs and publishers participating to the TCF from further explaining to the data subjects, in a clear and user-friendly manner, both the pursued legitimate interests as well as the reasons for believing

[200] Stacks are, in essence, combination of different processing purposes.

that their interests are not overridden by the interests or fundamental rights and freedoms of the data subjects[201].

452. Although, in the context of the present case, the Litigation Chamber does not express an opinion on whether an economic interest[202] can be regarded as a legitimate interest within the meaning of Article 6.1.*f* of the GDPR, it considers that the lack of specificity of the stated purposes means that the first condition for *specific* lawful processing is not met with the standard descriptions of the processing purposes and pursued interests, as imposed by the *TCF Policies*.

453. In the context of the necessity test, which aims to determine whether the intended processing operations are necessary for achieving the interests pursued, the question should be asked whether the legitimate interests pursued by the processing of data could not reasonably be achieved just as effectively by other means with less interference with the fundamental freedoms and rights of data subjects, in particular their right to respect for their privacy and their right to the protection of personal data as guaranteed by Articles 7 and 8 of the Charter[203].

454. The Court of Justice has also clarified that the condition of necessity of processing must be examined in relation to the principle of data minimisation laid down in Article 5.1.*c* GDPR[204]. In other words, according to the EDPB, it is necessary to consider whether other, less invasive means are available to achieve the same objective.

455. *In this case*, the Litigation Chamber understands that no safeguards are provided to ensure that the personal data collected and disseminated are limited to information that is strictly necessary for the purposes intended[205].

456. In the absence of measures that adequately demonstrate that no inappropriate personal data are being disseminated, the Litigation Chamber is forced to decide that the second condition has not been met.

457. With regard to the balancing test, in particular whether the interests pursued by the *adtech vendors* outweigh the fundamental freedoms and rights of the data subjects, the

---

[201] Article 29 Working Party – Opinion 06.2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95-46-EC (WP217), p. 47.

[202] As opposed to the interest pursued by capturing the users' choices in a TC String, as discussed in para. 404 *et seq*.

[203] CJEU Judgment of 4 May 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde t. Rīgas pašvaldības SIA "Rīgas satiksme"*, C-13/16; ECLI: EU:C:2017:336, para. 47.

[204] *Ibidem*, para. 48.

[205] In this respect, some authors argue that there are alternatives to RTB, in which only minimal information about the user is communicated. See M. VEALE, FR. ZUIDERVEEN BORGESIUS, "Adtech and Real-Time Bidding under European Data Protection Law", German Law Journal, 31 July 2021, pp. 19 et seq. The authors refer in particular to the browser plug-in Adnostic, which was developed 10 years ago and builds up a profile based on the user's surfing behaviour in order to target advertisements, with only minimal information leaving the user's device and behavioural targeting taking place exclusively in the user's browser. In addition, the authors refer to Google's so-called *Federated Learning of Cohorts* (FLoC) system for microtargeting within Chrome.

reasonable expectations of the data subjects should also be taken into account in accordance with recital 47 of the GDPR, in addition to the special circumstances of the particular case[206].

458. The criterion of the seriousness of the breach of the rights and freedoms of the data subject constitutes an essential element of the case-by-case assessment required by Article 6.1.*f* GDPR[207]. In this context, according to the Court of Justice, particular account should be taken of 'the nature of the personal data concerned, in particular their potentially sensitive nature, and of the nature and specific way in which they are processed, in particular the number of persons having access to them and the way in which they acquire such access'[208].

459. Once again, the Litigation Chamber finds that due to the large number of TCF partners that may receive their personal data, data subjects cannot reasonably expect the processing associated with this disclosure. In addition, there is the considerable amount of data that, in accordance with the preferences entered within the TCF system, is collected by means of a *bid request* and transmitted to the adtech vendors within the context of the OpenRTB protocol[209].

460. Furthermore, as the EDPB states, the legitimate interest does not constitute a sufficient legal basis in the context of direct marketing involving behavioural advertising[210]. In addition, the ICO concluded in a recent report that the legitimate interest is not a basis for legality in the context of RTB (yet many publishers rely on this legal ground for their processing) [211]. In short, in view of the above, the Litigation Chamber has decided that the third condition imposed by Article 6.1.*f* GDPR and the case law of the Court of Justice has not been met *in this case*.

461. In light of the aforementioned considerations, the Litigation Chamber finds that **the legitimate interest of participating organizations cannot be deemed an adequate legal ground for the processing activities occurring under the OpenRTB, based on users' preferences and choices captured under the TCF**.

---

[206] CJEU Judgment of 11 December 2019, *TK v. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 58.

[207] *Ibidem*, para. 56.

[208] CJEU Judgment of 11 December 2019, *TK v. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 57.

[209] Norsk Forbrukerrådet - "Out of Control. How consumers are exploited by the online advertising industry", 14 January 2020, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/, pp. 36-37; see also Recommendation CM/Rec(2021)8 of the Committee of Ministers of the Council of Europe to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 3 November 2021: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680a46147.

[210] Article 29 Working Party - Opinion 03/2013 on purpose limitation (WP 203), 2 April 2013, p. 46: "consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research".

[211] Information Commissioner's Office - "Update report into adtech and real time bidding", 20 June 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

(iii) - Contractual necessity is not a valid basis for the processing of personal data in the context of TCF and OpenRTB

462. In line with the EDPB guidelines, the Litigation Chamber notes that, in general, the (pre)contractual necessity of the processing is not a legal ground applicable to behavioural advertising[212].

463. Moreover, the Litigation Chamber notes that the current version of the TCF does not mention Article 6.1.*b* GDPR anywhere as a possible legal basis for the processing of personal data within the TCF and OpenRTB.

464. **On the basis of the foregoing elements, the Litigation Chamber therefore concludes that the processing of personal data under the OpenRTB on the basis of preferences captured in accordance with the current version of the TCF is incompatible with the GDPR, due to an inherent breach of the principles of lawfulness and fairness.**

B.4.2. - Duty of transparency towards data subjects (Art. 12, 13 and 14 GDPR)

465. The complainants raise the issue of the lack of transparency, and more specifically the fact that the OpenRTB ecosystem is so extensive that it is impossible for data subjects to give an informed consent to the processing of their personal data, or to object in an informed manner to the processing of their personal data on the basis of a legitimate interest.

466. The defendant, on the other hand, states that the TCF offers a solution to collect valid consent from users, where applicable, in accordance with the requirements set out in the GDPR and the ePrivacy Directive[213].

467. The Litigation Chamber finds that the information provided under the TCF in its current format to data subjects, albeit for the purposes of processing their personal data in the context of OpenRTB, does not meet the transparency requirements under the GDPR[214].

468. First of all, the Litigation Chamber states that IAB Europe may in certain cases claim the "*records of consent*" that CMPs are required to keep, in accordance with the *TCF Policies*[215], but fails to inform data subjects of this possible processing by IAB Europe.

469. Secondly, the Litigation Chamber finds that the manner in which information is provided to the data subjects, which was laid down by IAB Europe, does not comply with the requirement of a "transparent, comprehensible and easily accessible form"[216]. The former

---

[212] EDPB - Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, v2.0, 8 October 2019, pp. 14 ff, https://edpb.europa.eu.

[213] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32); IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38).

[214] See para. 433 *et seq*. of this decision.

[215] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 11, 14 and 19.

[216] Art. 12.1 GDPR.

Article 29 Working Party stipulates in its transparency guidelines that "the requirement that information and communication to data subjects be provided "in a concise, transparent, comprehensible and easily accessible form" means that data controllers should present the information/communication in an efficient and concise manner in order to avoid information fatigue"[217]. Moreover, data subjects should be able to determine in advance the scope and consequences of the processing and not be surprised later by other ways in which their personal data have been used[218].

470. The Litigation Chamber finds that the approach taken so far does not meet the conditions of transparency and fairness required by the GDPR. Indeed, some of the stated processing purposes are expressed in too generic a manner for data subjects to be adequately informed about the exact scope and nature of the processing of their personal data[219]. This is particularly problematic for purposes that rely on the consent of data subjects, as consent must be specific and sufficiently informed in order to be valid as a legal basis[220].

471. The Litigation Chamber also refers to the examples of CMPs specified in the Technical Report of the Inspection Service, and notes that the interface offered to users does not allow, among other things, the processing purposes associated with the authorisation of a particular *vendor* or which adtech vendors will process their data for a specific purpose to be identified in a simple and clear manner[221].

472. In that regard, the Litigation Chamber emphasises that the large number of third parties, i.e. the *adtech vendors* that will potentially receive and process the personal data of the users contained in the bid request, based on the preferences they have submitted, is not compatible with the condition of a sufficiently informed consent, nor with the broader transparency duty set out in the GDPR.

473. On the basis of the foregoing elements, the Litigation Chamber must therefore rule that the TCF in its current set-up does not comply with the obligations arising from the transparency principle, notably Articles 12, 13 and 14 GDPR.

---

[217] WP260 - Guidance on transparency under the GDPR, para. 8.

[218] WP260 - Guidance on transparency under the GDPR, para. 10.

[219] See para. 433 of this decision for examples as well as para. 441-452 for further analysis by the Litigation Chamber; see also C. MATT, C. SANTOS, N. BIELOVA, "Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?", in *Privacy Technologies and Policy*, APF 2020, LNCS, vol 12121, Springer, 2020, pp. 163-185.

[220] See para. 429-440 of this decision.

[221] Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), pp. 99 *et seq*.

B.4.3. - Accountability (art. 24 GDPR), data protection by design and by default (Art. 25 GDPR), integrity and confidentiality (Art. 5.1.f GDPR), as well as security of processing (Art. 32 GDPR)

a. Principle of accountability and data protection by design and by default

474. Article 24.1 GDPR requires the data controller to implement appropriate technical and organisational measures, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Moreover, these measures shall be reviewed and updated as necessary. This article reflects the principle of "accountability" set out in Article 5.2 of the GDPR, according to which the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability). Article 24.2 of the GDPR stipulates that, where proportionate in relation to processing activities, the measures referred to in Article 24.1 GDPR shall include the implementation of appropriate data protection policies by the controller.

475. Recital 74 of the GDPR adds that "the responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. It is important, in particular, that the controller is responsible for implementing appropriate and effective measures and for demonstrating the conformity of the processing activities with this regulation, including the effectiveness of the measures. These measures must take account of the nature, scope, context and purpose of the trafficking and the risk it poses to the rights and freedoms of physical persons".

476. It is also incumbent on the controller, pursuant to Articles 24 (accountability) and 25 of the GDPR (data protection by design and by default), to integrate the necessary respect for the GDPR rules into its processing and procedures, e.g. to ensure the existence and effectiveness of procedures for handling data subject requests and for checking the integrity and compliance of the TC String.

b. The outline of the security obligation

477. Pursuant to Article 32 of the GDPR, the controller is responsible for ensuring the security of the processing, "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons". In the present case, the Litigation Chamber notes a lack of respect for the obligation to ensure the security of processing on the part of the defendant, which is part of the principle of accountability. This shortcoming will be addressed *below*.

478. This failure to meet the obligation to ensure the security of processing constitutes a fundamental point of the present decision and of the penalties it imposes. The absence of technical and organisational measures aiming to ensure or tend to ensure the integrity of the TC String is considered a serious offence.

479. On the basis of Article 5.1.*f* GDPR, personal data must be processed in such a way as to ensure appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. In the absence of appropriate measures to secure the personal data of the data subjects, the effectiveness of the respect of the fundamental rights to privacy and to the protection of personal data cannot be guaranteed, especially in view of the crucial role played by information and communication technologies in our society.

480. As indicated in the previous section, the lack of an obligation to ensure the security of processing constitutes an important point in the decision[222]. Given the very large number of TC Strings generated each day within the TCF, it is essential that all the rules governing participation in the TCF are observed and complied with by all the parties involved, under the supervision of IAB Europe as the "*Managing Organisation*". The Litigation Chamber recalls that the combined reading of articles 32 (Security of processing), as well as 5.2 and 24 GDPR (principle of accountability) requires the controller to demonstrate its compliance with Article 32, by taking appropriate technical and organisational measures, in a transparent and traceable manner.

481. The Litigation Chamber also recalls the requirement of Article 25 GDPR (data protection by design and by default), which requires the data controller to integrate the necessary compliance with the rules of the GDPR upstream of its actions.

482. It should also be noted that the principle of security with its various components of integrity, confidentiality and availability of the data is set out in Articles 5.1.*f* and 32 of the GDPR and is now regulated in the GDPR at the same level as the fundamental principles of legality, transparency and loyalty.

483. IAB Europe offers the TCF to make OpenRTB compliant with the GDPR. In other words, the purpose of the TCF is to ensure that processing of personal data within the context of the OpenRTB protocol takes place in accordance with the GDPR as well as the ePrivacy Directive. Accordingly, IAB Europe, as *Managing Organisation* for the TCF and jointly responsible for the processing operations carried out within that framework[223], should take

[222] See para. 478 *et seq*. of this decision.

[223] See *supra*, title B.2. - Responsibility of IAB Europe for the processing operations within the Transparency and Consent Framework.

organisational and technical measures to ensure that participants at least comply with the TCF policies.

484. Notwithstanding the fact that in IAB Europe's current TCF system, *adtech vendors* receive consent signals as part of an HTTP(S) request or via browser APIs, some authors take the view that insufficient measures are in place under the TCF to guarantee the integrity of consent signals (particularly their validity) and to ensure that a *vendor* has actually received them (as opposed to having generated them itself)[224].

485. However, in the absence of validation by IAB Europe, it becomes theoretically possible for CMPs to falsify or modify the signal to generate a *euconsent-v2* cookie and thus reproduce a "false consent" from users for all purposes and all *adtech vendors*. This case is also explicitly provided for in the TCF Policies:

> "*A Vendor must not create Signals where no CMP has communicated a Signal and shall only transmit Signals communicated by a CMP or received from a Vendor who forwarded a Signal originating from a CMP without extension, modification, or supplementation, except as expressly allowed for in the Policies and/or Specifications*."[225]

486. The Litigation Chamber takes note of the fact that the possibility of falsification or modification of the TC String by CMPs is foreseen in the defendant's *Transparency & Consent Framework Policies* document, which sets out the basis for the TCF.

487. The Litigation Chamber also relies on the fact that the defendant indicates on its website the introduction of the "*TCF Vendor Compliance Programme*", through which audits of organisations participating in the TCF (listed on the *Global Vendors List*) will take place[226]. The Litigation Chamber encourages all initiatives on the part of the defendant, that are aimed at ensuring compliance with the obligation to process personal data under the TCF in a secure manner on the part of the defendant. Nevertheless, in view of the defendant's lack of systematic monitoring of compliance with the TCF rules by the participating organisations, and taking into account the significant impact of such violations (e.g. falsification or modification of the TC String), the Litigation Chamber considers that this initiative to introduce the TCF Vendor Compliance Programme is insufficient to bring the defendant into compliance with the security obligation.

488. In particular, the Litigation Chamber relies on the fact that the sanctions regime of this new programme, provided by the defendant in the case of failure to comply with the rules of the

---

[224] See on this subject, for example C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, "Consent Management Platforms Under the GDPR: Processors and/or Controllers?", in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, p. 64.

[225] IAB Europe Transparency & Consent Framework Policies, Chapter III 13 (6), https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/#13_Working_with_CMPs

[226] https://iabeurope.eu/blog/iab-europe-launches-new-tcf-vendor-compliance-programme/

TCF, is permissive and not dissuasive. In fact, a vendor may declare himself liable for a breach up to 3 times, without any sanction, before being given 28 days to comply. Only in the event of non-compliance after the expiry of the 28 days will the vendor be removed from the *Global Vendors List*. It can also re-enter the list if it complies with the requirements later on. The programme also allows a vendor to be in breach up to four times, in order to proceed to an immediate suspension during a brief period of 14 days, until the vendor comes into compliance. The " *TCF Vendor Compliance Programme* " is therefore not a sufficient measure for ensuring the security of personal data processing operations carried out under the TCF.

489. The Litigation Chamber also observes that no measures other than the « TCF Vendor Compliance Programme » are foreseen by the defendant to monitor or prevent the falsification or modification of the TC String.

490. With regard to the allegation by the plaintiffs that IAB Europe also violates Articles 44 to 49 GDPR, the Litigation Chamber acknowledges, in view of the scope of the Framework — which involves a large number of participating organisations — that it is evident that personal data captured in the TC Strings will be transferred outside the EEA at some point by CMPs, and that the defendant is acting as data controller in this regard (see para. 356-357). However, the Litigation Chamber notes that the Inspection Service did not include an assessment of a concrete international data transfer in its report. For this reason, the Litigation Chamber concludes that there is an infringement of the GDPR, but in view of the lacking evidence of a systematic international transfer, as well as the scope and nature thereof, the Litigation Chamber finds it is not in a position to sanction the defendant for a violation of articles 44 to 49 GDPR. Notwithstanding the previous, the Litigation Chamber also finds that these international transfers of personal data, where applicable, must be assessed primarily by the publishers and CMPs implementing the TCF. The Litigation Chamber finds that the publishers are responsible and accountable for taking the necessary measures to prevent personal data collected through their website and/or application from being transferred outside the EEA without adequate international transfer mechanisms.

491. This being said, the Litigation Chamber also finds that the defendant should facilitate the due diligence incumbent on the publishers and CMPs, e.g. by requiring *adtech* vendors to indicate clearly whether they are located outside the EEA or whether they intend to transfer personal data outside the EEA through their data processors. Furthermore, the Litigation Chamber notes that, contrary to its obligation under the principles of accountability and of data protection by design and by default, IAB Europe did not foresee any mechanism to ensure that participating publishers and CMPs have put in place adequate mechanisms for potential international transfers of the TC String, as foreseen under Articles to 44 to 49 GDPR, both at the time of its creation and when transmitting the TC String to participating adtech vendors. The preamble of the TCF Policies merely indicates that the TCF "*is not*

intended nor has it been designed to facilitate [...] more strictly regulated processing activities, such as transferring personal data outside of the EU". The Litigation Chamber finds that this does not meet the requirements of Articles 24 and 25 GDPR.

492. The Litigation Chamber notes, for the record, that it is uncertain whether, in view of its current architecture and support of the OpenRTB protocol, the TCF can be reconciled with the GDPR.

493. In this sense, IAB Europe's accountability starts from the moment the organisation designs and makes available a system for the management of consent or objections of users, but fails to take the necessary measures to ensure the conformity, integrity and validity of that consent or objection.

494. The Litigation Chamber therefore finds that, as part of its security and integrity obligations, IAB Europe must take not only organisational but also technically effective measures to ensure and demonstrate the integrity of the preferential signal transmitted by CMPs to *adtech vendors*.

B.4.4. - Additional alleged breaches of the GDPR

a. Purpose limitation and data minimisation (Art. 5.1.*b* and 5.1.*c* GDPR)

495. Although in this decision the Litigation Chamber has already concluded that the processing operations carried out on the basis of the OpenRTB protocol are not in accordance with the basic principles of purpose limitation and data minimisation[227] (as no safeguards are provided to ensure that the personal data collected and disseminated within the framework of the OpenRTB are limited to information that is strictly necessary for the intended purposes), the Litigation Chamber emphasises that the complainants have explicitly indicated in their submissions that the scope of their allegations is limited to the processing operations within the TCF. The Inspection Service also clarified in its report that IAB Europe does not act as a data controller for the processing operations that take place entirely in the context of the OpenRTB protocol.

496. Taking these clarifications into account, the Litigation Chamber concludes that, given the limited amount of data about a user that is stored in a TC String before being saved by means of a *euconsent-v2* cookie, there is no violation of the principles of purpose limitation and data minimisation in the context of the TCF.

[227] See para. 495-496 of this decision

497. Although larger quantities of personal data will be processed at a later stage, including special categories of personal data, this is not the case with the TCF. Within the TCF, therefore, there is no violation of the principles of purpose limitation and data minimisation.

b. Storage limitation (Art. 5.1.*e* GDPR)

498. With regard to the principle of storage limitation and based on the Inspection Service's report, the Litigation Chamber finds there is insufficient evidence that the TC String and the associated storage of users' personal data are stored for an unauthorised period of time, in violation of Article 5.1.*e* GDPR.

499. Therefore, the Litigation Chamber concludes that no violation of article 5.1.*e* GDPR could be established.

c. Integrity and confidentiality (Art. 5.1.*f* GDPR)

500. As already explained above[228], the Litigation Chamber finds that the current version of the TCF offers insufficient safeguards to prevent the values included in a TC String from being modified in an unauthorised manner, with the result that the personal data of a data subject bundled in a *bid request* may be processed for the wrong purposes, in breach of the integrity principle, and/or may end up with the wrong *adtech vendors* or the ones rejected by the user, in breach of the confidentiality principle. The Litigation Chamber therefore rules that the current version of the TCF violates Article 5.1.*f of* the GDPR.

d. Processing of special categories of personal data (Art. 9 GDPR)

501. Although a number of complaints are directed against the RTB system, including the *Authorized Buyers* protocol developed by Google as well as the OpenRTB protocol developed by IAB Tech Lab, the Inspection Service determined in its report, as a preliminary matter, that the Belgian Data Protection Authority did not have jurisdiction for the former and that IAB Tech Lab does not act as a data controller for the latter[229].

502. The Litigation Chamber notes that the Inspection Service reports the lack of appropriate rules for the processing of special categories of personal data under the TCF. However, this observation is not supported by any technical analysis showing that special categories of personal data are actually processed *within the TCF*. On the contrary, the technical analyses by the Inspection Service show that the TC String in itself does not contain any information that can be linked to the taxonomy of the websites visited, where, for example, special categories of personal data may be involved.

[228] See para. 477 *et seq*. of this decision.
[229] Investigation report of the Inspection Service, pp. 8-11.

503. Therefore, the Litigation Chamber rules that this allegation is unfounded and that no breach of Article 9 of the GDPR by the defendant can be established.

e. Exercise of data subject rights (Art. 15 – 22 GDPR)

504. First of all, the Inspection Service notes in its report that certain complainants have argued the impossibility for the data subjects to enforce their rights, although the investigation carried out by the Inspection Service did not confirm these allegations. In view of the lack of evidence of any infringement, the Litigation Chamber limits its reasoning to general observations relating to the exercise of data subject rights.

505. Secondly, the Litigation Chamber refers to the scope of the written submissions by the complainants, in which they specifically restricted their grieves to the processing of the plaintiffs' personal data by the defendant in the particular context of the TCF[230]. As a result, the Litigation Chamber will not assess the circumstances in which data subjects may exercise their rights regarding the processing of personal data contained in the *bid requests*, with respect to the *adtech vendors*, seeing as this processing occurs entirely under the OpenRTB protocol.

506. However, with regard to the current version of the TCF, the Litigation Chamber finds that the TCF does not seem to facilitate the exercise of the data subjects' rights insofar as the CMP interface cannot be retrieved easily and at all times by the users, such as to allow them to amend their preferences and retrieve the identity of the adtech vendors with whom their personal data have been shared by means of a bid request, in accordance with the OpenRTB protocol. In this regard, the Litigation Chamber underlines the importance of a proper implementation and enforcement of the interface requirements defined in the TCF Policies, such as to allow data subjects to effectively exercise their rights vis-à-vis each of the joint-controllers, and notes that the shared responsibility to do so lies primarily with the CMPs and publishers. In the light of the foregoing, the Litigation Chamber is, however, not in a position to establish a violation of the Articles 15-22 GDPR.

f. Records of processing activities (Art. 30 GDPR)

507. The Inspection Service notes in its report that IAB Europe does not keep records of its processing activities. The defendant takes the view, first of all, that it can rely on the exception provided for in Article 30.5 of the GDPR and is therefore not subject to the obligation to keep such records. However, in the course of the investigation, the defendant added a summary of its processing activities to the documents in the file[231].

[230] Submission of the complainants dd. 18 February 2021, p. 2.
[231] IAB Europe's response to the investigation 10 February 2020 (Exhibit 57), p. 23.

508. The Litigation Chamber first notes that the records submitted by the defendant do not contain any activity relating to the TCF, with the exception of *member management, including administration of the TCF*. Contrary to the defendant's assertion, in particular that the records do not need to include the processing activities in the context of the TCF, the Litigation Chamber is of the opinion that the records must at least include access to users' consent signals, objections and preferences.

509. Indeed, in accordance with Article 8 of the *TCF Policies* (v1.1)[232] and Article 15 of the *TCF Policies* (v2.0)[233], the defendant reserves the right, as the *Managing Organisation*, to access the "*records of consent*". The Litigation Chamber also emphasises that the incidental nature of this access to users' preferences has not been proven or raised by the defendant. The stable relationship between IAB Europe as *Managing Organisation* and all organisations participating in the TCF ecosystem should also be taken into account. In view of the large number of participating organisations and the defendant's intention to monitor the compliance of the various CMPs and other *adtech vendors* [234], more thoroughly in the future, IAB Europe should also include this processing in its records of processing activities.

510. Therefore, the Litigation Chamber considers the non-incidental nature of the processing and the infringement of Article 30.1 GDPR found by the Inspection Service to be sufficiently proven.

g. Data protection impact assessment (Art. 35 GDPR)

511. The Litigation Chamber first notes that the defendant does not deny that the TCF can also be used for RTB purposes.

512. The argumentation by the defendant that the TCF can be used for other, non-marketing-related purposes and that the OpenRTB can also operate separately from the TCF is therefore not relevant to the consideration of whether or not a data protection impact assessment is required.

513. After all, the interrelationship between the TCF and the RTB implies that the preferences users enter by using a CMP interface will necessarily have an impact on the way their personal data are subsequently processed by adtech *vendors* within the RTB, as determined by the OpenRTB specification.

[232] IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38), p. 6.
[233] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 14.
[234] Cf. Hearing of 11 June 2021.

514. The Litigation Chamber further refers to Decision No. 01/2019 of the General Secretariat of the Belgian DPA[235], in which the General Secretariat has established a list of processing operations for which a data protection impact assessment is mandatory.

515. It is undisputed for the Litigation Chamber that the TCF was developed, among other things, for the RTB system, in which the online behaviour of users is observed, collected, recorded or influenced in a systematic and automated manner, including for advertising purposes[236]. It is also not disputed that within the RTB, data is widely collected from third parties (Data Management Platforms, or DMPs) in order to analyse or predict the economic situation, health, personal preferences or interests, reliability or behaviour, location or movements of natural persons[237].

516. Considering the large number of data subjects who come into contact with websites and applications implementing the TCF, as well as the growing number of organisations participating in the TCF, on the one hand, and the impact of the TCF on the large-scale processing of personal data in the context of RTB, on the other, the Litigation Chamber finds that, in accordance with Decision No. 01/2019, the Defendant is indeed subject to the obligation to conduct a data protection impact assessment, pursuant to Article 35 of the GDPR. Hence, Article 35 of the GDPR is violated.

h. Designation of a Data Protection Officer (art. 37 GDPR)

517. Article 37 GDPR provides for an obligation to designate a Data Protection Officer (DPO) in cases where:

i. processing is carried out by a public authority or public body; or

ii. a controller or processor is primarily responsible for processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

iii. the controller or processor is primarily responsible for the processing of large volumes of special categories of personal data under Article 9 of the GDPR and of personal data relating to criminal convictions and offences under Article 10 of the GDPR.

[235] Decision of the General Secretariat No. 01/2019 of 16 January 2019, available on the website of the GBA https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-nr.-01-2019-van-16-januari-2019.pdf.
[236] Decision of the General Secretariat No. 01/2019 of 16 January 2019, para. 6.8).
[237] Decision of the General Secretariat No. 01/2019 of 16 January 2019, para. 6.3).

518. The Litigation Chamber has already concluded that the defendant processes personal data because IAB Europe, in its capacity as *Managing Organisation*, can have access to the TC Strings and *the records of consent*[238].

519. The former Article 29 Working Party states that processing activities that are necessary to achieve the purposes of the controller or processor can be considered as core activities within the meaning of Article 37 GDPR. The Litigation Chamber finds that in view of the importance of the TCF to the defendant, the stated purposes of the TCF, as well as the associated processing of personal data in its capacity as *Managing Organisation*, the processing under the TCF belongs to the core activities of IAB Europe.

520. With regard to the concept of 'large-scale processing operations', the Article 29 Working Party clarifies that, inter alia, the following must be taken into account:

    i. the number of data subjects - either as a specific number or as a proportion of the relevant population;
    ii. the amount of data and/or range of the different data items processed;
    iii. the duration or permanence of data processing;
    iv. the geographical extent of the processing activity.

    In the present case , the Litigation Chamber finds that the TCF is offered in various Member States; that the TCF intrinsically requires that the personal data of users be processed in the form of a TC String for as long as this is necessary to be able to demonstrate that consent was obtained in accordance with the *TCF Policies*; and that the personal data processed is furthermore shared with numerous *adtech vendors*. From this, the Litigation Chamber concludes that the TCF involves the large-scale processing of personal data.

521. With regard to the criterion of regular and systematic observation the WP29 interprets the term "regular" in one or more of the following ways:

    i. something that occurs continuously or at specific times during a certain period of time
    ii. something that occurs in a recurring manner, or repetitively at fixed times; or
    iii. something that occurs constantly or periodically

    The Litigation Chamber finds that the contractual obligation for *Vendors* and CMPs to submit records of consent to the defendant, in its capacity as *Managing Organisation*, upon simple request by IAB Europe falls within (i). Thus, there is regular observation of data relating to identifiable users.

522. The term "systematic" should be understood in one or more of the following ways:

[238] See para. 358 and 468 of this decision.

i. Something that occurs according to a system
ii. Prearranged, organised or methodical
iii. Something that occurs in the context of a general data collection programme
iv. Something carried out as part of a strategy

523. Once again, the Litigation Chamber finds that the processing of the TC Strings or *records of consent* by the defendant in the current version of the TCF meets at least the first three criteria. Therefore, the Litigation Chamber rules that the TCF must be regarded as a regular and systematic observation of identifiable users.

524. From the foregoing elements, the Litigation Chamber concludes that IAB Europe should have appointed a DPO, in accordance with Article 37 GDPR. Hence, Article 37 of the GDPR is violated.

C. Sanctions

525. As a preliminary matter, and as developed below, the Litigation Chamber notes that the present decision on the TCF does not directly address deficiencies of the wider OpenRTB framework. However, the Litigation Chamber does draw attention to the great risks to the fundamental rights and freedoms of the data subjects posed by OpenRTB, in particular in view of the large scale of personal data involved, the profiling activities, the prediction of behaviour, and the ensuing surveillance (see *A.3.1.* **- Definitions and operation of the Real-Time Bidding system**). Insofar as the TCF is the tool on which OpenRTB relies to justify its compliance with the GDPR, the TC String plays a pivotal role in the current architecture of the OpenRTB system.

526. Under Article 100 of the DPA Act, the Litigation Chamber has the power to:

1° classify the complaint without taking action;
2° order the dismissal of the case;
3° pronounce a suspension of the pronouncement;
4° propose a transaction;
5° formulate warnings or recommendations;
6° order to comply with the requests of the person concerned to exercise these rights;
7° order that the interested party be informed of the security problem;
8° order the freezing, restriction or temporary or permanent prohibition of processing;
9° order the compliance of the treatment;
10° order the rectification, restriction or erasure of data and the notification to recipients of the personal data;

11° order the withdrawal of the certification bodies' accreditation;

12° impose fines;

13° impose administrative fines;

14° order the suspension of data flows to another State or international body;

15° forward the file to the Brussels Public Prosecutor's Office, which informs it of the action relating to the file;

16° decide, case by case, to publish its decisions on the internet site of the Data Protection Authority.

527. As for the administrative fine that may be imposed pursuant to Article 83 of the GDPR and Articles 100, 13° and 101 DPA Act, Article 83 of the GDPR provides:

> « *1.* Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.
>
> *Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*
>
> *a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
>
> *b) the fact that the violation has been committed deliberately or through negligence;*
>
> *c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
>
> *d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
>
> *e) any relevant previous infringements by the controller or processor;*
>
> *f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
>
> *g) the categories of personal data affected by the infringement;*
>
> *h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;*
>
> *i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;*
>
> *j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and*

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement. ».

528. Recital 150 GDPR[239] further distinguishes between whether the offender is an undertaking or not. In the first hypothesis, the criterion (fixed amount or percentage) for reaching the highest fine should be applied. Where, on the other hand, the offender is not an undertaking, account should be taken of the economic situation of the offender and the general level of incomes in the Member State concerned. This is to prevent the imposition of fines that could be disproportionately high.

529. It is important to contextualise the shortcomings of the defendant in order to identify the most appropriate corrective measures. In this context, the Litigation Chamber will take into account all the circumstances of the case, including — within the limits it specifies below — the reaction submitted by the defendant to the envisaged sanctions communicated by means of the sanction form[240]. In this regard, the Litigation Chamber specifies that the form it sent expressly mentions that it does not involve the reopening of debates. Its sole purpose is to collect the defendant's reaction to the planned sanctions.

530. While measures such as a compliance order or a ban on further processing can put an end to an identified infringement, administrative fines, as set out in Recital 148 of the GDPR, are imposed in case of serious infringements, in addition to or instead of the appropriate measures that are required to remedy the infringement.

531. The Litigation Chamber would also like to point out that it is its sovereign responsibility as an independent administrative authority — in compliance with the relevant articles of the GDPR and the DPA Act — to determine the appropriate corrective measure(s) and sanction(s). This follows from Article 83 GDPR itself, but also the Market Court has emphasised the existence of a wide margin of manoeuvre in its case law, *inter alia* in its judgment of 7 July 2021[241].

532. The Litigation Chamber notes that the complainants are making various requests for sanctions against the defendant. However, it is not for the complainants to ask the Litigation Chamber to order any particular corrective measure or sanction, nor is it up to the Litigation Chamber to give reasons for not accepting any of the requests made by the

[239] Recital 150 of the GDPR: '[...] Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine.[...]".

[240] See para. 534 as well as para. 272 *et seq.* of this decision.

[241] Court of Appeal of Brussels, Market Court Section, 19th Chamber A, Market Cases Section, 2021/AR/320, pp. 37-47.

complainants[242]. These considerations nevertheless leave intact the obligation for the Litigation Chamber to give reasons for the choice of measures and sanctions which it deems appropriate (from the list of measures and sanctions made available to it by Article 58 of the GDPR and Article 100 of the DPA Act) to sentence the defendant.

533. In the present case, the Litigation Chamber notes that the complainants request the Litigation Chamber to take the following measures and sanctions. These proposals are included for information:

> *"1) In application of Article 100, §1, 8° DPA Act (relating to IAB Europe) to:*
>
> *a. prohibit the TC String to be processed in the TCF;*
> *b. prohibit all personal data associated with the processing of the TC String, such as IP addresses, websites visited and apps used, from being processed in the TCF;*
> *c. order the permanent removal from its website and its other public communication channels of all documents, files and records that in any way incite or oblige any third party to carry out such processing;*
>
> *2) In application of Article 100, §1, 10° DPA, order IAB Europe 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;*
>
> *3) In application of Article 100, §1, 10° DPA Act order IAB Europe to inform all recipients of the personal data processed in the TCF of the order imposed by the Litigation Chamber:*
>
> *a. prohibition to process the TC String in the TCF;*
> *b. prohibit all personal data associated with the processing of the TC String, such as IP addresses, websites visited and apps used, from being processed in the TCF;*
> *c. order to permanently delete all TC Strings and other personal data already processed in the TCF from all IT systems, files and data carriers;*
>
> *and this both clearly visible and readable in a bold box at the top of the homepage of IAB Europe's website www.iabeurope.eu in the usual font and size until 6 months after a judgment of the Market Court becomes final, if applicable pursuant to Section 108 of the DPA Act, or by email, in both cases with a hyperlink to the English-language version of the decision of the Litigation Chamber on the website of the GBA;*
>
> *4) In application of Article 100, §1, 12° DPA Act on behalf of IAB Europe order the forfeiture of a penalty payment of EUR 25,000 per started calendar day of delay in the execution of any measure imposed in the interlocutory decision of the Litigation Chamber as from the expiration of seven calendar days after the interlocutory decision of the Litigation Chamber."*

[242] See Court of Appeal of Brussels, Market Court Section, 19th Chamber A, Market Cases Section, 1 December 2021, 2021/AR/1044, p. 25.

534. A sanction form has been sent to the defendant on 11 October 2021. IAB Europe submitted its response on 1 November 2021[243]. This response has been taken into consideration in the following paragraphs.

C.1. - Breaches

535. The Litigation Chamber found the defendant in breach of the following articles:

- **Articles 5.1.*a*** and **6 GDPR** — The current TCF does not provide a legal basis for the processing of user preferences in the form of a TC String. Moreover, the Litigation Chamber notes that the TCF offers two bases for the processing of personal data by participating adtech vendors, but finds that none of them can be used. First, the consent of the data subjects is currently not given in a sufficiently specific, informed and granular manner. Second, the legitimate interest of the organisations participating in the TCF is outweighed by the interests of the data subjects, in view of the large-scale processing of the users' preferences (collected under the TCF) in the context of the OpenRTB protocol and the impact this can have on them. Since none of the grounds for lawfulness set out in Article 6 of the GDPR apply to this processing, as explained above[244], the defendant is in breach of Articles 5.1.*a* and 6 GDPR.

  Taking note of the fact that the defendant itself does no longer have factual or technical control over the TC Strings once these have been generated by the CMPs and stored on the users' devices[245], the Litigation Chamber finds that it cannot impose the *a posteriori* removal of all TC Strings generated until now on the defendant. More specifically, it is the responsibility of the CMPs and the publishers who implement the TCF[246], to take the appropriate measures, in line with Articles 24 and 25 GDPR, ensuring that personal data that has been collected in breach of Articles 5 and 6 GDPR is no longer processed and removed accordingly. Insofar as IAB Europe is still storing TC Strings deriving from the no longer supported globally scoped consent cookies, the Litigation Chamber equally finds that the necessary measures must be taken by the defendant to warrant permanent erasure of these no longer necessary personal data.

- **Articles 12**, **13**, and **14 GDPR** — As developed above (see *B.4.2.* **- Duty of transparency towards data subjects (Art. 12, 13 and 14 GDPR)**), the way in which the information is provided to the data subjects does not meet the requirement of a 'transparent, comprehensible and easily accessible manner'. Users of a website or an application

[243] See title A.10. - Sanction form, European cooperation procedure, *supra*.
[244] See title B.4.1 - Lawfulness and fairness of processing (Art. 5.1.a and 6 GDPR).
[245] In accordance with the mandatory policies and technical specifications established and imposed on TCF participants by IAB Europe.
[246] Furthermore, the Litigation Chamber underlines the fact that none of the CMPs and adtech vendors haven taken part in the present proceedings.

participating in the TCF are not given sufficient information about the categories of personal data collected about them, nor are they able to determine in advance the scope and consequences of the processing. The information given to users is too general to reflect the specific processing of each vendor, which also prevents the granularity — and therefore the validity — of the consent received for the processing carried out using the OpenRTB protocol. Data subjects are unable to determine the scope and consequences of the processing in advance, and therefore do not have sufficient control over the processing of their data to avoid being surprised later by further processing of their personal data.

- **Articles 24**, **25**, **5.1.*f*** and **32 GDPR** — As explained *above*[247], on the basis of Articles 5.1.*f* and 32 GDPR, the controller is obliged to ensure the security of the processing and the integrity of the personal data processed. The Litigation Chamber recalls that the combined reading of Articles 5.1.*f* and 32, as well as 5.2 and 24 GDPR (subjecting the controller to the principle of accountability) requires the controller to demonstrate its compliance with Article 32, by taking appropriate technical and organisational measures, in a transparent and traceable manner. Under the current TCF system, adtech vendors 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). In the absence of systematic and automated monitoring systems of the participating CMPs and *adtech vendors* by the defendant, the integrity of the TC String is not sufficiently ensured, since it is possible for the CMPs to falsify the signal in order to generate an *euconsent-v2* cookie and thus reproduce a "false consent" of the users for all purposes and for all types of partners. As indicated above[248], this hypothesis is also specifically foreseen in the terms and conditions of the TCF. The Litigation Chamber therefore finds that IAB Europe, in its capacity of *Managing Organisation*, has designed and provides a consent management system, but does not take the necessary steps to ensure the validity, integrity and compliance of users' preferences and consent.

  The Litigation Chamber also finds that the current version of the TCF does not facilitate the exercise of the data subject rights, especially taking into consideration the joint-controllership relation between the publisher, the implemented CMP and the defendant. The Litigation Chamber also underlines that the GDPR requires that data subjects rights can be exercised vis-à-vis each of the joint-controllers in the TCF such as to comply with Articles 24 and 25 GDPR.

---

[247] See title B.4.3. - Accountability (art. 24 GDPR), data protection by design and by default (Art. 25 GDPR), integrity and confidentiality (Art. 5.1.f GDPR), as well as security of processing (Art. 32 GDPR)

[248] See para. 485 of this decision.

In light of the above, the Litigation Chamber finds that the defendant is in breach of its obligations of security of processing, integrity of personal data, and data protection by design and data protection by default (Articles 24, 25, 5.1.*f* and 32 GDPR).

- **Article 30 GDPR** — As developed above[249], the Litigation Chamber cannot follow the defendant's argument that it can benefit from the exceptions to the obligation to maintain records of processing activities, provided for in Article 30.5 GDPR. As the records of processing activities of the defendant do not contain any processing operations relating to the TCF, except for the management of members and the administration of the TCF, although IAB Europe as *Managing Organisation* can access the records of consent, the Litigation Chamber finds a breach of Article 30 GDPR by the defendant.
- **Article 35 GDPR** — In view of the large number of data subjects that come into contact with websites and applications implementing the TCF, as well as organisations participating in the TCF, on the one hand, and the impact of the TCF on the large-scale processing of personal data in the OpenRTB system, on the other hand, the Litigation Chamber finds that IAB Europe has failed to carry out a comprehensive data protection impact assessment (DPIA) with regard to the processing of personal data within the TCF, and thus violated Article 35 GDPR. The Litigation Chamber finds that the TCF was developed, among other things, for the RTB system, in which the online behaviour of users is observed, collected, recorded or influenced in a systematic and automated manner, including for advertising purposes. It is also not disputed that within the OpenRTB, data are widely collected from third parties (DMPs) in order to analyse or predict the economic situation, health, personal preferences or interests, reliability or behaviour, location or movements of natural persons.
- **Article 37 GDPR** — Because of the large-scale, regular and systematic observation of identifiable users that the TCF implies, and in view of the defendant's role, more specifically of its capacity as *Managing Organisation*, the Litigation Chamber rules that IAB Europe should have appointed a Data Protection Officer (DPO). By failing to do so, the defendant infringes Article 37 GDPR.

[249] See para. 507 *et seq*. of this decision.

C.2. - Sanctions

536. Therefore, the Litigation Chamber orders the defendant:

I. To render the TCF compliant with the obligation of lawfulness, fairness and transparency (Articles 5.1.*a* and 6 GDPR), by establishing a legal basis for the processing as well as the sharing of user preferences in the context of the TCF, in the form of a TC String and *euconsent-v2* cookie placed on the users' devices for this purpose. These obligations also imply that any personal data collected so far by means of a TC String in the context of the globally scoped consents, which is no longer supported by IAB Europe, shall be deleted without undue delay by the defendant. In addition, the Litigation Chamber orders the defendant to prohibit the use of legitimate interest as a legal ground for processing by the organisations participating in TCF in its current format, via its terms of use.

II. To render the TCF compliant with the transparency and information obligation (Articles 12, 13, and 14 of the GDPR), by requiring TCF-registered CMPs to take a harmonised and GDPR-compliant approach regarding the information to be provided to users through their interface. The information, which covers the categories of data collected, the purposes for which they are collected, and the applicable legal grounds for processing, must be precise, concise and understandable in order to avoid users being surprised by subsequent processing of their personal data by parties other than the publishers or IAB Europe.

III. To ensure compliance of the TCF with the obligations of integrity and security, as well as data protection by design and by default (under Articles 5.1.*f* and 32 GDPR, and 25 GDPR). In this respect, the Litigation Chamber orders to include effective technical and organisational monitoring measures to facilitate the exercise of data subject rights and to guarantee the integrity of the TC String in view of the possibility, in the current state of the system, of falsification of the signal. An example of measures to be put in place under Article 32 of the GDPR is a strict vetting process for organisations participating to the TCF. The Litigation Chamber reminds the defendant as well as the other joint-controllers of their obligation to make the necessary arrangements such as to ensure, amongst other requirements, that data subjects may effectively exercise their rights. Lastly, in the context of Article 25 of the GDPR, the defendant must prohibit, via its terms of use, the organisations participating in the current version of TCF from activating a default consent, as well as from basing the lawfulness of the intended processing activities on the legitimate interest.

IV. To ensure the compliance of the records of processing activities carried out in the framework of the TCF in its current format, and in particular relating to the

processing of users' preferences and consent in the form of a TC String and the placement of a cookie *euconsent-v2* on their devices.

V. To carry out a data protection impact assessment, covering both the processing activities under the TCF and the impact of these activities on subsequent processing under the OpenRTB.

VI. To designate a Data Protection Officer (DPO), responsible, *inter alia*, for ensuring the compliance of personal data processing activities in the context of the TCF, in accordance with Articles 37 to 39 of the GDPR.

537. These compliance measures should be completed within a maximum period of six months following the validation of an action plan by the Belgian Data Protection Authority, which shall be submitted to the Litigation Chamber within two months after this decision. On the ground of Article 100 § 1er, 12° of the DPA Act, a penalty payment of 5.000 EUR per day will be due in case of failure to comply within the above-mentioned time limits.

538. In addition to this compliance order, the Litigation Chamber is of the opinion that an administrative fine is justified in this case for the following reasons, which are analysed on the basis of article 83.2 GDPR.

539. The principles of lawfulness, fairness, transparency and security are part of the essence of the GDPR and infringements of these rights are punishable by the highest fines, according to Article 83.5 GDPR. In this respect, the failure to respect the basic principles of data protection should be penalised by proportionately high fines, depending on the circumstances of the case. In this regard, reference can be made to the Guidelines on the Application and Setting of Administrative Fines, according to which:

> « *Fines are an important tool that supervisory authorities should use in appropriate circumstances. The supervisory authorities are encouraged to use a considered and balanced approach in their use of corrective measures, in order to achieve both an effective and dissuasive as well as a proportionate reaction to the breach. The point is to not qualify the fines as last resort, nor to shy away from issuing fines, but on the other hand not to use them in such a way which would devalue their effectiveness as a tool.* »[250]

540. In its subparagraph (*a*), article 83.2. refers to « the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them ».

541. With regard to the nature and gravity of the infringements, the Litigation Chamber notes that the principles of lawfulness (Articles 5.1.*a* and 6 GDPR), transparency (Articles 12 to 14

[250] Article 29 Working Party – Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253), p. 7.

GDPR) as well as security (Articles 5.1.*f* and 32 GDPR) are fundamental principles of the protection regime set up by the GDPR. The principle of accountability set out in Article 5.2. of the GDPR and developed in Article 24 is also at the heart of the GDPR and reflects the paradigm shift brought about by the GDPR, *i.e.* a shift from a regime based on prior declarations and authorisations by the supervisory authority to greater accountability and responsibility of the controller. Respect of its obligations by the latter and its ability to demonstrate this are therefore only more important.

542. A valid legal basis and transparent information are core elements of the fundamental right to data protection. As far as transparency is concerned, this principle is the 'gateway' that strengthens the control of data subjects over their personal data and enables the exercise of other rights granted to the data subjects by the GDPR, such as the right to object and the right of erasure. Breaches of these principles constitute serious infringements, which may be subject to the highest administrative fines foreseen under the GDPR.

543. The breach of Article 25, on the obligation of data protection by design and by default, as well as of Article 30 on keeping records of processing activities are also significant infringements, particularly in view of the scale of the processing operations and the impact on the privacy of the complainants as well as the other users confronted with websites or applications that have implemented the TCF.

544. As regards the nature and purpose of the processing, and more specifically on the nature of the data, the Litigation Chamber notes that the TC String, as an expression of users' preferences on the processing purposes and the potential adtech vendors being provided through the CMP interface, constitutes the cornerstone of the TCF. Although the scope of this decision is the TCF and its TC String, and the sanction imposed on the defendant pertains solely to that framework, the compliance of the OpenRTB with the GDPR is assessed as part of a holistic analysis of the TCF and its interaction with the former. Insofar as the current version of the TCF is the tool on which OpenRTB relies to justify its compliance with the GDPR, and because the defendant facilitates membership and use of the OpenRTB to a significant number of participating organisations, the Litigation Chamber finds that IAB Europe plays a pivotal role as regards the OpenRTB, without being a data controller in that context.

545. As regards the scope of the contested processing and the number of data subjects affected, the Litigation Chamber notes that the TCF (in its current format), as developed by the defendant (representing large players in the online behavioural advertising sector[251]), offers a unique service on the market. The TCF's scope is therefore essential, given the growing number of partners that signed up to it. Regarding the level of damage incurred by

[251] See para. 36 of this decision.

concerned data subjects, the Litigation Chamber underlines once more that the TC String plays a pivotal role in the current architecture of the OpenRTB system. Thereby, the TC String supports a system posing great risks to the fundamental rights and freedoms of the data subjects, in particular in view of the large scale of personal data involved, the profiling activities, the prediction of behaviour, and the ensuing surveillance of data subjects.

546. With respect to the duration of the infringement, the Litigation Chamber takes note that the TCF is offered by the defendant since 25 April 2018 as a mechanism for obtaining users' consent with respect to predetermined processing purposes, and for the transfer of their personal data to TCF-participants, including adtech vendors. Notwithstanding the various iterations of the framework, which has been upgraded to the second version of the TCF on 21 August 2019, and taking into account the systemic deficiencies of the TCF under the GDPR, the Litigation Chamber finds that the breaches have existed at least since May 2018, with regard to the validity of the collected consent and the placement of a TC String without a valid legal ground, and since August 2019 for the reliance on legitimate interest as a legal ground to process the data subjects' personal data.

547. Article 83.2.*b* GDPR requires the DPA to take into account the intentional or negligent character of the infringement. Observing that the defendant, in its role as *Managing Organisation*, was aware[252] of risks linked to non-compliance with the TCF, in particular relating to the integrity of the TC String and the encapsulated choices and preferences of the users, and in light of the impact of the TC String on the subsequent processing operations under the OpenRTB, the Litigation Chamber finds that IAB Europe was negligent in establishing the measures governing the implementation of the current version of the TCF.

548. In its subparagraph (*c*), article 83.2 GDPR refers to potential actions taken by the controller to mitigate the damage suffered by data subjects. The Litigation Chamber notes the absence of concrete measures taken or introduced by the defendant in order to mitigate the damage suffered by the data subjects (*i.e.* the processing of their personal data regardless of their choices, or in the absence of a valid legal ground).

549. Article 83.2.*d* of the GDPR concerns the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32.

550. Even if the Litigation Chamber does not take into account in the present decision the developments that occurred after the closure of the proceedings in June 2021, the

[252] See para. 485 of this decision.

Litigation Chamber takes note that the defendant already announced during the hearing[253] its intention to introduce a "TCF Vendor Compliance Programme" in September 2021, through which audits of organisations participating in the TCF (listed on the Global Vendors List) will be established.

551. The Litigation Chamber encourages all measures aimed at ensuring compliance with the GDPR. Nevertheless, as explained in para. 487-488, in view of the defendant's lack of systematic monitoring of compliance with the TCF rules by the participating organisations at the time of the complaints, and taking into account the significant impact of such violations (e.g. in case of falsification or modification of the TC String), the Litigation Chamber considers that the announcement of this initiative to increase its compliance with one of its obligations as a data controller for the TCF and consisting of audits of adtech vendors on the *Global Vendors List* demonstrates that the TCF was not compliant with the defendant's safety obligations, including the obligation to mitigate damage suffered by data subjects. No other actions were communicated by the defendant to the Litigation Chamber in this respect.

552. Furthermore, the Litigation Chamber is no longer in a position to review the nature of this programme and, in any event, this new programme does not change the nature of the breaches of the GDPR that occurred until the closure of the debates in June 2021.

553. In light of article 83.2.*e* of the GDPR, the Litigation Chamber notes the absence, at the time of the present decision, of any final decision by other competent supervisory authorities, regarding previous relevant infringements by the defendant in relation to the TCF.

554. Article 83.2.*f* of the GDPR concerns the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement. In this regard, the Litigation Chamber disagrees with the Inspection Service's finding that the defendant did not cooperate sufficiently with the former, apart from the provision and submission of records of processing activities conducted by IAB Europe.

555. Insofar as the categories of personal data affected by the infringement are concerned (Article 83.2.*g* of the GDPR), the Litigation Chamber acknowledges that the personal data contained in and processed by means of the TC String are in adequacy with the principle of data minimisation, having regard to their nature. Notwithstanding the previous, the Litigation Chamber reiterates its position that the TCF plays a pivotal role in supporting the processing operations based on the OpenRTB protocol. Hence, the Litigation Chamber concludes that it cannot exclude that both special and regular categories of personal data

[253] And confirmed by the defendant through a public announcement on its website, on 26 August 2021: https://iabeurope.eu/blog/iab-europe-launches-new-tcf-vendor-compliance-programme/

—processed by means of a bid request to which the TC String is attached— may be affected by the infringements that occurred under the TCF.

556. With regard to article 83.2.*h* of the GDPR, the Litigation Chamber notes that this criterion is not relevant to the present case.

557. Article 83.2.*i* of the GDPR is not applicable in the absence of any previous final decision in this regard, taken against the defendant.

558. Article 83.2.*j* of the GDPR concerns the adherence to approved codes of conduct or approved certification mechanisms. In this context, the Litigation Chamber notes that IAB Europe has previously been in contact with the Belgian Data Protection Authority concerning the drafting and adoption of a Code of Conduct (at the point of time when the proceedings were already pending). The Litigation Chamber also underlines the absence of follow-up by the defendant in this regard since June 2020, without any further explanation by the defendant.

559. Lastly, article 83.2.*k* of the GDPR refers to any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement. The Litigation Chamber did not retain specific factors that would change the amount of the fine.

560. In determining the amount of the administrative fine, article 83.3 to 83.7 GDPR use the term "undertaking", which, based on Recital 150 of the GDPR and as confirmed by the WP29 and the EDPB[254], should be understood in accordance with articles 101 and 102 TFEU. Based on CJEU case law, the term undertaking in Articles 101 and 102 TFEU refers to a single economic unit (SEU), even if this economic unit is legally formed from several natural or legal persons[255].

561. To assess whether several entities form a SEU, the ability of the individual entity to take free decisions should be taken into account. It should also be considered whether a leading entity (the parent company), exercises decisive influence over the other entity or not (examples of criteria are the amount of the participation, personnel or organizational ties, instructions and the existence of company contracts).

562. The Litigation Chamber could not find any indication of decisive influence from IAB Inc. over the defendant IAB Europe, or limitation of freedom of its decision with respect to IAB Inc.

---

[254] Article-29-Working Party – Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253) and confirmed by the EDPB in Endorsement 1/2018 on 25 May 2018; as well as EDPB Binding Decision 1/2021, para. 292.

[255] CJUE Judgment of 23 April 1991. *Klaus Höfner and Fritz Elser v Macrotron GmbH*, C-41/90, ECLI:EU:C:1991:161, paragraph 21, and CJUE Judgment of 14 December 2006, *Confederación Española de Empresarios de Estaciones de Servicio*, C-217/05, ECLI:EU:C:2006:784, para. 40

563. This was also developed by the defendant in its response to the sanction form, wherein IAB Europe claims that IAB Inc. has no ownership stake in the defendant nor any say in the deployment of IAB Europe's activities. The defendant indicated that IAB Inc. (headquartered in the USA) licenses the "IAB" brand to other organizations, and remains an entirely separate and independent entity from IAB Europe.

564. The Litigation Chamber therefore decides to base its decision on the sole financial revenues of IAB Europe as reference for calculating the administrative fine, instead of the annual turnover of IAB Inc.

565. In this regard, the Litigation Chamber takes note that the annual gross benefits of the defendant amounted to EUR 2.471.467 in 2020[256]. As a subsidiary point, the Litigation Chamber also observes that participating organisations are required to pay an annual fee of 1.200 EUR to the defendant upon their registration to the TCF[257]. Having regard to the total number of registered TCF adtech vendors, which has significantly increased from 420 on 25 May 2020 to 744 on 7 June 2021, the Litigation Chamber thus finds that a large part of the income of IAB Europe is generated through the licensing of the TCF. More specifically, IAB Europe would make a gross profit of at least 981.600 EUR for 2021 with the TCF participants' annual fee — including both the adtech vendors and the CMPs[258] — alone.

566. Under Article 83.4, infringements of articles 25, 30, 32, 35 and 37 GDPR may amount to up to 10.000.000 EUR or, in the case of an undertaking, up to 2% of the total annual worldwide turnover of the preceding business year.

567. Under 83.5 GDPR, infringements of articles 5.1.*a*, 5.1.*f*, 6, and 12 to 14 GDPR may amount to up to 20.000.000 EUR or, in the case of an undertaking, up to 4% of the total annual worldwide turnover of the preceding business year. The maximum amount of the fine in this case, as provided for in Article 83.5, is therefore 20.000.000 EUR.

568. As these are, among other things, infringements of a fundamental right enshrined in Article 8 of the Charter of Fundamental Rights of the European Union, the assessment of their seriousness based on Article 83.2.*a* GDPR will be made in an autonomous manner.

569. Based on the elements developed above, the defendant's reaction to the proposed sanction form, as well as the criteria listed in Article 83.2 GDPR, the Litigation Chamber considers that the above-mentioned infringements justify to impose a compliance order in conjunction with an administrative fine of 250.000 EUR (Article 100, § 1 er, 13° and 101 DPA Act) on the defendant, as an effective, proportionate and dissuasive sanction in light of

[256] See Annual Accounts 21/12/2020, available at https://cri.nbb.be/bc9/web/catalog?execution=e1s1.

[257] https://iabeurope.eu/wp-content/uploads/2019/08/TCF-Fact-Sheet_General.pdf

[258] Totalling 74 CMPs on June 7th, 2021: https://iabeurope.eu/cmp-list/. The actual profit is likely to be higher, considering the still increasing number of TCF participants.

Article 83 GDPR. In fixing this amount, the Litigation Chamber took into account the annual business volume of the defendant, which amounted to 2.471.467 EUR in 2020[259].

570. The amount of EUR 250.000 EUR remains, in view of the aforementioned elements, proportionate to the infringements that have been established by the Litigation Chamber. This amount is also much lower than the maximum amount of 20.000.000 EUR provided for by Article 83.5 GDPR.

571. The Litigation Chamber is of the opinion that a lower fine would not meet, in the present case, the criteria required by Article 83.1 of the GDPR, according to which the administrative fine must not only be proportionate, but also effective and dissuasive. These elements derive from the principle of loyal cooperation described in Recital 13 GDPR (in line with Article 4.3 of the Treaty on the European Union).

572. In view of the importance of transparency regarding the decision-making process of the Litigation Chamber and in accordance with Article 100, §1, 16° of the DPA Act, this decision is published on the website of the Data Protection Authority[260]. Having regard to the previous publicity surrounding this case, as well as the general interest to the public, also in view of the a large number of data subjects and organisations involved, the Litigation Chamber has decided not to delete the direct identification data of the parties and persons mentioned, whether natural or legal persons.

[259] See Annual Accounts 21/12/2020 available at https://cri.nbb.be/bc9/web/catalog?execution=e1s1
[260] See also para. 287.

FOR THESE REASONS,

the Litigation Chamber of the Data Protection Authority decides, after deliberation, to:

- order the defendant, pursuant to Article 100(1)(9) of the DPA Act, with a view to bring the processing of personal data within the context of the TCF in line with the provisions of the GDPR, by:
    a. providing a valid legal basis for the processing and dissemination of users' preferences within the context of the TCF, in the form of a TC String and a *euconsent-v2* cookie, as well as prohibiting, via the terms of use of the TCF, the reliance on legitimate interests as a legal ground for the processing of personal data by organisations participating in the TCF in its current form, pursuant to Articles 5.1.*a* and 6 of the GDPR;
    b. ensuring effective technical and organisational monitoring measures in order to guarantee the integrity and confidentiality of the TC String, in accordance with Articles 5.1.*f*, 24, 25 and 32 of the GDPR;
    c. maintaining a strict audit of organisations that join the TCF in order to ensure that participating organisations meet the requirements of the GDPR, in accordance with Articles 5.1.*f*, 24, 25 and 32 of the GDPR;
    d. taking technical and organisational measures to prevent consent from being ticked by default in the CMP interfaces as well as to prevent automatic authorisation of participating vendors relying on legitimate interest for their processing activities, in accordance with Articles 24 and 25 of the GDPR;
    e. forcing CMPs to adopt a uniform and GDPR-compliant approach to the information they submit to users, in accordance with Articles 12 to 14 and 24 of the GDPR;
    f. updating the current records of processing activities, by including the processing of personal data in the TCF by IAB Europe, in accordance with Article 30 of the GDPR;

g. carrying out a data protection impact assessment (DPIA) with regard to the processing activities under the TCF and their impact on the processing activities carried out under the OpenRTB system, as well as adapting this DPIA to future versions or amendments to the current version of the TCF, in accordance with Article 35 of the GDPR;

h. appointing a Data Protection Officer (DPO) in accordance with Articles 37 to 39 of the GDPR.

These compliance measures should be completed within a maximum period of six months following the validation of an action plan by the Belgian Data Protection Authority, which shall be submitted to the Litigation Chamber within two months after this decision. Pursuant to Article 100 § 1er, 12° of the DPA Act, a penalty payment of 5.000 EUR per day will be due in case of failure to comply within the above-mentioned time limits.

- impose an administrative fine of 250.000 EUR on the defendant pursuant to Article 101 of the DPA Act.

This decision may be appealed before the Market Court, pursuant to Article 108(1) of the DPA Act, within a period of thirty days from its notification, with the Data Protection Authority as defendant.

(signed) Hielke HIJMANS
President of the Litigation Chamber