Litigation Chamber

Decision on the merits 21/2022 of February 2, 2022

Unofficial translation from Dutch

File number: DOS-2019-01377

Concerns: Complaint regarding Transparency & Consent Framework

The Litigation Chamber of the Data Protection Authority, composed of Mr. Hielke

Hijmans, chairman, and MM. Yves Poullet and Frank DeSmet;

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

to the free movement of such data, and repealing Directive 95/46/EC (general regulation on the

data protection), hereinafter GDPR;

Having regard to the law of 3 December 2017 establishing the Data Protection Authority (hereinafter

ACL);

Having regard to the internal regulations as approved by the House of Representatives on 20

December 2018 and published in the Belgian Official Gazette on January 15, 2019;

Considering the documents in the file;

made the following decision:

Complainants: Mr. Johnny Ryan, Mr. Pierre Dewitte and Mr. Jef Ausloos, Ms. Katarzyna

Szymielewic having mandated the NGO Panoptykon to act on his behalf, as well as

the NGOs Bits of Freedom and the League of Human Rights, all represented

by Masters Frédéric Debusseré and Ruben Roex, as well as Mr. Bruno Bidon, below

after “the complainants”;

.

.

.

.

.□

.□

The defendant: IAB Europe, whose registered office is located at [...] 1040 Brussels,□

with company number [...], represented by Masters Frank Judo and□

Kristof Van Quathem, hereinafter “the defendant”.□

1□

Contents□

4□

A. Facts and procedure□

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

1.□

During 2019, a series of complaints were filed against Interactive□

Advertising Bureau Europe (hereinafter IAB Europe), for breaching various provisions□

of the GDPR with regard to the large-scale processing of personal data. The□

complaints related in particular to the principles of legality, adequacy, transparency,□

purpose limitation, storage restriction and security, as well as on the□

responsibility.□

2.□

Nine identical or very similar complaints were filed, four of which directly□

with the Data Protection Authority (hereinafter referred to as "DPA") and five via the□

IMI system with supervisory authorities in other EU countries.□

3.□

The Inspection Service has also carried out investigations on its own initiative,□

in accordance with article 63, paragraph 6, of the LCA. Complaints relating to the same subject□

and being directed against the same party (IAB Europe), based on the principles of□

proportionality and necessity in the conduct of investigations (Article 64 of the LCA), the□

Inspection Service has merged the aforementioned files into a single case under the□

file number DOS-2019-01377.□

4.□

The plaintiffs accepted this merger, as well as the request of the Litigation Chamber□

to merge their conclusions and present them jointly, in the interest of

the economy and efficiency of the procedure.

5.

In this international case, four plaintiffs, including the NGO League for Human Rights,

are domiciled in Belgium, one in Ireland, four in different EU states, represented

by the Poland-based NGO Panoptykon, and one complainant is represented by the NGO Bits of

Freedom based in the Netherlands.

6.

Pursuant to Article 4(1) of the LCA, the Data Protection Authority is responsible

to monitor the data protection principles contained in the GDPR and in

other laws containing provisions on the protection of the processing of personal data

personal character.

7.

In accordance with Article 32 of the LCA, the Litigation Chamber is the administrative body

ODA Dispute Resolution1.

8.

In accordance with Articles 51 et seq. of the GDPR and Article 4(1) of the LCA, it is

to the Litigation Chamber, as an administrative body for settling disputes in

the DPA, to exercise effective control over the application of the GDPR and to protect the freedoms and

1 The administrative nature of the disputes before the Litigation Chamber has been confirmed by the Court of Markets. See

in particular the judgment of 12 June 2019, published on the DPA website, as well as the decision 17/2020 of the Chamber

Litigation.

fundamental rights of natural persons with regard to the processing of their personal data

personal character and to facilitate the free movement of personal data within

the European Union. These tasks are further explained in the strategic plan and

ODA management plans, drawn up in accordance with Article 17(2) of the ACL.

9.

In addition, with regard to IMI, Article 56 of the GDPR provides: "Without prejudice to Article

55, the supervisory authority of the main establishment or the sole establishment of the

controller or processor is competent to act as an authority

supervisory authority concerning

the cross-border processing carried out by this

controller or this processor, in accordance with the procedure provided for in

section 60."

10.

Article 4.23 of the GDPR clarifies the notion of cross-border processing in the terms

following: "a processing of personal data which takes place in the Union in the

framework of the activities of establishments in several Member States of a person responsible for the

processing or a processor when the controller or processor is

established in several Member States; or (b) processing of personal data

which takes place in the Union as part of the activities of a single establishment of a

controller or processor, but which materially affects or is

likely to significantly affect data subjects in more than one State

members ; »

11.

The defendant has its only head office in Belgium, but its activities have an impact

significant on stakeholders in several Member States, including the

plaintiffs in Ireland, Poland and the Netherlands, as well as in Belgium. Bedroom

Litigation derives its jurisdiction from a combined reading of Articles 56 and 4(23)(b) of the

GDPR. The DPA was entered by the Polish data protection authorities,

Dutch and Irish following a complaint addressed to them by the complainants

in accordance with Article 77.1 of the GDPR. She declares that she is the control authority

principal (Article 60 of the GDPR).

12.

The following supervisory authorities have indicated their willingness to act as

concerned ("Concerned Supervisory Authority" - "CSA" below): Netherlands,

Latvia, Italy, Sweden, Slovenia, Norway, Hungary, Poland, Portugal, Denmark, France,

Finland, Greece, Spain, Luxembourg, Czech Republic, Austria, Croatia, Cyprus and

Germany (Berlin, Rhineland-Palatinate, North Rhine-Westphalia, Saarland, Lower Saxony,

Brandenburg, Mecklenburg-Western Pomerania, Bavaria), Ireland.

13.

During the procedure, other complaints, the object of which is very similar to that of the

this case, were sent to the Belgian DPA by the Maltese, Romanian, Croatian,

Greek, Portuguese, Swedish, Cypriot and Italian. These complaints are not part of the

this procedure.

6

A.2. - The language of the proceedings: Interlocutory decision 01/2021 modified by the decision

interlocutory 26/2021 of February 23, 2021.

14.

On October 13, 2020,

the Litigation Chamber sent a

letter to the parties,

in accordance with article 98 of the DPA law, informing them of the language of the procedure (the

French), and inviting them to present their written conclusions.

15. In response to the Complainants' request of November 27, 2020, and taking into account the

international nature of this case, the Litigation Chamber rendered on January 8, 2021

interlocutory decision 01/2021 regarding the language of the proceedings. Following an appeal

plaintiffs before the Court of Markets, this interlocutory decision was amended on

February 23, 2021 (interlocutory decision 26/2021).

16. Under this last interlocutory decision, based on an agreement with the parties, the

correspondence of the DPA with the parties is done in Dutch and the decisions

interlocutory and final of the Litigation Chamber are in Dutch. Nevertheless, the

Chambre Litigation provides the parties with a French translation and a translation

English of the final decision.

17. However, the parties are free to use the language of their choice (Dutch, French or

English) in the proceedings before the Litigation Chamber, whether in writing or

orally. In the case of IAB Europe, it is French or English. ODA is not

responsible for translations of procedural documents submitted by a party for the

account of the other.

18. Finally, the Litigation Division points out that it sometimes uses English terminology in

this decision, in cases where the translation into Dutch would reduce the comprehensibility of

decision.

A.3. - RTB and TCF

19. In essence, this case concerns, on the one hand, the compliance of the TCF system with the

GDPR and, on the other hand, the responsibility of IAB Europe, the defendant in this

procedure, and the other different actors involved. Furthermore, it is also

the impact of the TCF on what is known as the real-time auction system (Real-Time

Bidding (RTB)). Considering the complexity of the RTB, it is shown below.

A.3.1. - Definitions and operation of the real-time auction system (Real-Time

Bidding -RTB-)

20. Unlike “traditional” advertising, where the parties involved determine

manually and contractually the terms of the exchange of information, advertising

online is usually done mostly automatically and behind the scenes, for

7□

through "programmatic advertising" methods, including real-time bidding (RTB)□

is the main system2.□

21.□

The real-time auction is defined in the legal literature as "a network of□

partners that enables big data applications in the organizational domain of the□

marketing to improve sales of pre-determined advertising space through a□

real-time marketing based on□

data and personalized advertising□

(behavioural)".3.□

22. Real-time bidding means the use of an automated online auction and□

instant for the sale and purchase of online advertising space. More specifically, this□

means that when an individual accesses a website or application that contains a□

advertising space, behind the scenes, through an automated online auction system and□

algorithms, technology companies representing thousands of advertisers can□

instantly (in real time) make an offer for this advertising space in order to display□

targeted advertisements specifically tailored to that individual's profile.□

23. Real-time bidding works behind the scenes on most websites□

commercial and mobile applications. Thousands of companies are involved and□

receive information about the person visiting the website. In this way,□

billions of advertisements are auctioned every day.□

24. In a real-time auction system, several parties are involved4:□

A. The companies or organizations that created and operate the Time Auction System□

concerned, in particular by defining its policies/governance and protocols□

techniques. The main ones are:□

has.□

the “OpenRTB” system and the “Advertising Common Object Model” (AdCOM) which

associated with it, created by IAB Technology Laboratory, Inc. (abbreviated as "IAB Tech

Lab”) and Interactive Advertising Bureau, Inc. (abbreviated “IAB”), both based in

New York ;

b.

the “Authorized Buyers” system created by Google.

OpenRTB is a standard protocol that aims to simplify the interconnection between

adtech providers of advertising space, publishers (ad exchanges,

sell-side platforms or networks working with publishers) and buyers

advertising space competitors (bidders, demand-side platforms or

2 M. VEALE, FR. ZUIDERVEEN BORGESIUS, “Adtech and Real-Time Bidding under European Data Protection Law”, German

Journal, July 31, 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 in the field

marketing organization to improve sales through real-time, data-driven marketing and

personalized (behavioral) advertising”, available at https://ssrn.com/abstract=3319284; 3 M. VEALE, FR.

ZUIDERVEEN BORGESIUS, IBIDEM, P. 3.

4 Ibid.

networks working with advertisers). The overall goal of OpenRTB is to establish a

common language for communication between buyers and ad tech vendors

advertising space5.

B. On the “supply side”, we find:

has. Businesses that have a website or app with Spaces

advertisers. In RTB jargon, these companies are called “publishers”.

b. Companies operating an automated online platform through which

publishers can optimize the value and volume of their media sales

advertisers by indicating the availability of their advertising space to be displayed on a

data subject and requesting that one or more bid requests

be made for this advertising space. In RTB jargon, these companies are

called “Sell-Side Platforms” (“SSPs”). SSPs provide

inventory

available from

their publishers to the various ad exchanges on the market and

possibly to advertising networks and other “Demand-Side Platforms”

(“DSPs” -see below-). The most advanced SSPs work in real time.

As soon as an advertising space is called up when a page is viewed on the site

of a publisher, the SSP searches for the best offer on this type of advertising space by

based on the profile of the detected visitor, and automatically broadcasts the ad

corresponding6.

C. On the “demand side” we find:

has. Companies wishing to display advertisements for their products or

services in a targeted manner to website visitors and users

applications (advertisers).

b. Companies operating an online platform that allows advertisers and

media agencies to make and optimize their purchases of advertising space,

and on which advertisers' ads are offered7. In RTB jargon,

these companies are called “Demand-Side Platforms” (“DSPs”).

D. Companies, called "Ad Exchanges", play the role of intermediaries between them.

They bring together organizations from the supply and demand side and allow them

automatically communicate with each other so that the DSPs can respond to

requests for offers from SSPs.

5 Technical analysis report from the inspection service, January 6, 2020 (Exhibit 53), p. 11.

6 Technical analysis report from the inspection service, June 4, 2019 (Exhibit 24), p. 5-6.

7 Technical analysis report from the inspection service, June 4, 2019 (Exhibit 24), p. 5

9

E. In addition, there are so-called “Data Management Platforms” (“DMPs”)

(data management platforms) that extract huge amounts and types of

personal data from multiple sources (such as devices,

cookies, mobile identifiers, pixels, analyzes of the behavior of

online browsing, social media, offline data, but also from third parties such

as data brokers, etc.), then centralize this data, and finally analyze it

and categorize them using algorithms and artificial intelligence. Using

a DMP, an advertiser can enrich and combine the data he owns

on (potential) customers with the data it can obtain from a central DMP. Thereby,

one of the main functions of a DMP is to create detailed profiles of

consumers by enriching data in order to optimize targeting and

the effectiveness of marketing and advertising campaigns and to provide offers

personalized on websites and in applications8.

25. Once an advertiser has established detailed consumer profiles through

of a DMP, he submits, via his DSP, requests for offers to

publishers/SSPs offering advertising space corresponding to these profiles of

consumers.

26. In RTB jargon, SSPs, DSPs, Ad Exchanges, Advertisers and DMPs are collectively

referred to as “adtech providers”.

27. Schematically, this can be presented as follows9:

28. This can also be represented as follows10:

8 Technical analysis report from the inspection service, January 6, 2020 (Exhibit 53), p. 7.

9 M. VEALE, FR. ZUIDERVEEN BORGESIUS, “Adtech and Real-Time Bidding under European Data Protection Law”, German

Journal, July 31, 2021, p. 9.

10 Technical analysis report from the inspection service, June 4, 2019 (Exhibit 24), p. 6.

29. The content of a bid request, which contains data about online users, their

device and websites visited, is captured by the OpenRTB protocol or the system

Authorized Buyers. Generally, the following categories of

personal data may be communicated to advertisers in the context of

from bid request 11:

▪ URL of the site visited

▪ Category or subject of the site

▪ Device operating system

▪

▪

Software and browser version

Device manufacturer and model

▪ Mobile phone operator

▪ Screen size

▪

▪

▪

Unique user identification defined by supplier and/or buyer.

Unique identifier of the person from the Ad Exchange, often derived from the Ad cookie

Exchange.

A DSP's user identification, often derived from the Ad Exchange cookie that

is synchronized with a DSP domain cookie.

▪ Year of birth□

▪ Gender□

▪□

Interests□

▪ Metadata reflecting the consent given□

▪ Geography□

▪□

Longitude and latitude□

▪ Zip code□

30. Consequently, the Litigation Division considers that the GDPR applies ratione□

materiae to the RTB system, including the OpenRTB protocol and, to some extent, the□

11 Ibid., p. 10.□

11□

Transparency & Consent Framework (TCF) discussed below are components□

essential, since RTB trading through RFPs involves□

intrinsically the processing of personal data.□

31.□

The different steps and interactions between SSPs, DSPs and DMPs that take place in the□

RTB system can be summarized as follows12:□

i.□

ii.□

iii.□

iv.□

An end user requests a web page;□

The publisher's ad server on the web page selects an SSP;□

The SSP then selects an Ad Exchange;□

The Ad Exchange sends requests for offers to hundreds of partners in the□

network and offers them the possibility of generating an offer in response;□

v.□

The Ad Exchange allows privileged DMPs and/or DSPs to synchronize□

http-cookies;□

vi.□

vii.□

The “Ad Exchange” places the winning bid;□

The DSP serves the advertiser's advertising;□

viii.□

The advertisement is loaded from a CDN (Content Delivery Network, or□

network provider);□

ix.□

The advertiser's server loads a JavaScript for verification;□

R.12 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.□

12□

32. Real-time auctions present a number of risks that arise from the□

nature of the ecosystem and how personal data is□

processed within it. These risks include13:□

▪ profiling and automated decision making□

▪□

large-scale processing (including special categories of data to□

personal character);□

▪ innovative use or application of new technological solutions or□

organizational;□

▪ matching or merging datasets;□

▪□

analysis or prediction of behavior, location or movements□

natural persons;□

▪□

invisible processing of personal data.□

33. In addition, a large number of organizations — such as data controllers,□

joint controllers, processors or other data subjects□

— are part of the ecosystem. This has a potentially significant impact on the protection□

Datas. In addition, most of those affected have a limited understanding□

how the ecosystem processes their personal data.□

34. Accordingly, the GDPR applies to processing carried out under the RTB, which□

are of such a nature that they may create a significant risk to the rights and freedoms□

some people.□

A.3.2. - IAB Europe Transparency and Consent Framework□

Framework-TCF-)□

35.□

IAB Tech Lab designed the OpenRTB protocol, which together with Google's AdBuyers protocol,□

is the most widely used RTB protocol in the world. IAB Tech Lab, based in New York USA□

United, acts as a provider of the OpenRTB standard and should be distinguished from IAB Europe,□

who designed the Transparency and Consent Framework□

Framework-TCF-).□

36.□

IAB Europe is a federation that represents the advertising and marketing sector□

digital at European level. It includes member companies as well as□

national associations, with□

their own member companies.

Indirectly,

IAB Europe represents approximately 5,000 companies, including large corporations and

national members14.

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

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

37. According to IAB Europe, the defendant in these proceedings, the TCF ensures the

accountability and transparency of OpenRTB. The TCF is a separate set of

policies (TCF Policies), technical specifications, terms and conditions, created, managed

and administered by IAB Europe, and, according to the defendant, should be able to inform

users of the legitimate interests pursued by advertisers, as well as to obtain the

valid consent of these users with regard to the processing of their data

personal data in a real-time auction system (such as OpenRTB).

38. Although OpenRTB should be distinguished from TCF, the two systems are related. After all,

IAB Europe claims that the TCF provides an operational framework within which the operations of

data processing that takes place on the basis of the OpenRTB protocol can be put

in compliance with the GDPR (and the ePrivacy Directive).

39. Regarding the TCF IAB Europe declares the following:

“In its current form, the TCF is a cross-industry best practice standard that

facilitates the compliance of the digital advertising sector with certain rules of

privacy and data protection policy and which aims to provide individuals with

greater transparency and control over their personal data. More

specifically, it is a "framework" within which companies operate in a

independent and helps them meet the requirement to have a GDPR legal basis

for any processing of personal data and the obligation to obtain the

user consent for storing and accessing information on a device

the user under the Privacy and Electronic Communications Directive”15

40. Moreover, the main actors within the TCF correspond to a large extent to the

Parties participating in OpenRTB (excluding CMPs):

i.

Publishers—Parties that make advertising space available on their site

web or in their application and who are in direct contact with the users whose

personal data is collected and processed. A publisher can

provide a CMP (see below) on their website or in their app for them

allow to seek and manage the consent of visitors/users to the

processing of their personal data and to facilitate the operation

of TCF16. Publishers decide which adtech providers can collect

data on their website and process the personal data of their

users (and/or access their devices) and for what purposes17.

ii.

Adtech providers — Companies that receive personal data

staff of publishers in order to fill advertising space on websites

15 Free translation, submissions in response of the defendant dated March 25, 2021, para. 32.

16 Information Commissioner's Office, “Update report into adtech and real time bidding”, 20 June 2019, p. 11-

12https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.

17 Conclusions of Respondent's Response dated March 25, 2021, para. 32.

publishers or in publisher applications, such as advertisers,

SSPs, DSPs, Ad Exchanges, and DMPs.

iii.

Consent Management Platforms—For the TCF, there are also

companies that offer “consent management platforms” (hereafter

after “Consent Management Platforms” CMP). Concretely, a CMP takes the

form of a pop-up that appears the first time you connect to a website to

collect the user's consent to the placement of cookies and other

credentials18.

41. An essential part of a CMP intervention is the generation of a chain of

characters consisting of a combination of letters, numbers and other characters.

This string is called “TC String” by IAB Europe, for “Transparency and Consent

String”. The TC String is intended to capture in a structured and automated way the

preferences of a user when visiting a website or application from a publisher that has

integrated into the CMP. This concerns in particular the collection of consent (or not) to the

processing of personal data for marketing and other purposes, sharing

whether or not personal data with third parties (adtech providers) and the exercise

or not of the right of opposition.

42. Adtech vendors decipher the TC String to determine if they have the base

necessary legal basis to process a user's personal data for the purposes

specified. Thanks to its concise data format, the CMP can store and retrieve at any

moment the preferences of a user and transmit this information to the suppliers

adtech who need it19.

43. This can be represented schematically as follows20:

18 Technical analysis report from the inspection service, January 6, 2020 (Exhibit 53), p. 59.

19 Technical analysis report from the inspection service, January 6, 2020 (Exhibit 53), p. 75.

20 Defendant's submissions dated February 18, 2021, para. 18.

i.

ii.

An Internet user browses a publisher's site, for example an information site.

The publisher ensures that a CMP is activated on its website or in its application

when the user starts using it.

iii.

The CMP checks whether a TC String already exists for this user or not. If a CT

String “stored globally”21 is chosen, the CMP will contact the Internet domain

consensus.org run by IAB Europe to check from there if there is already a

so-called "consensus" cookie on the user's device. This particularly concerns the

cookie euconsent-v2.

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 installs a euconsent-v2 cookie on the

user's device or updates the existing cookie.

A.4. - Inspection Service reports

A.4.1. - IAB Europe acts as data controller with respect to

relates to the Transparency and Consent Framework

Framework -TCF) and the personal data processing operations involved therein

relate

44. As part of this procedure, the Inspection Service concentrated its investigation

exclusively on IAB Europe, which the Inspection Service has identified as the responsible

data processing for the Transparency and Consent Framework (hereinafter,

“TCF”). The Inspection Service bases this first observation on the fact that IAB

Europe has developed the TCF, with which IAB Europe imposes binding rules on

participating organizations. 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 users in

online, with regard to the purposes of the processing and the authorized adtech providers.

45. The Inspection Service bases its report on two technical analyzes relating to the

IAB Europe Open Realtime Bidding API specification, as well as the different mechanisms

of the IAB Tech Lab's OpenMedia Specification, including the Transparency and

consent22.

21 Also referred to as “broad consent”

22 Technical analysis reports from the inspection service, June 4, 2019 (Exhibit 24) and January 6, 2020 (Exhibit 53).

46. With respect to the OpenRTB protocol, the Inspection Service finds that IAB Tech Lab,

who developed this open technical standard and is based in New York (USA), simply acts

as the system supplier vis-à-vis the participating organizations and cannot

therefore not be considered a data controller. Unlike TCF,

the OpenRTB allows the processing of personal data according to means and

purposes entirely determined by participating organizations, but not by IAB Tech

Lab.

47. Finally, the Inspection Service indicates that the DPA is not competent for the protocol

Authorized Buyers, which was developed by Google as an alternative to the standard

OpenRTB.

A.4.2. - Identified breaches of the GDPR

48. The Inspection Service finds that IAB Europe violates the legal provisions and the

following principles of the GDPR with its TCF:

▪ 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 relating to special categories of data to be

personal character);

▪ Article 12.1 (transparency of information, communication and procedures for exercising

rights of data subjects)

▪ Article 13 (information to be provided when personal data has been

collected from the data subject)

▪ Article 14 (information to be provided when personal data has not been

not been collected from the data subject)

▪ Article 24.1 (responsibility of the controller);

▪ Articles 32.1 and 32.2 (security of processing).

49. Apart from complaints, the Inspection Service also finds breaches

additional to the following provisions of the GDPR:

▪ Article 30 (record of processing activities);

▪ Article 31 (cooperation with the supervisory authority)

▪ Article 24.1 (responsibility of the controller);

▪ Article 37 (appointment of a data protection officer).

17

Finding 1 - IAB Europe wrongly uses legitimate interest as a legal basis for the

processing of personal data under the TCF, according to which categories

special types of personal data may also be processed in certain

case.

50. Based on the two versions of the IAB Europe Policies on Transparency and

consent of IAB Europe23 (hereinafter TCF Policies), the Inspection Service notes that IAB

Europe places the responsibility for respecting the principles of transparency and fairness on
CMPs and/or publishers. Furthermore, IAB Europe considers that the legitimate interest of
participating organizations constitutes an appropriate basis for data processing
of a personal nature within the framework of the TCF, in order to create an advertising profile of
data subjects and to send them personalized advertisements. However, according to
the Inspection Service, IAB Europe does not provide evidence that the interests, in particular
the fundamental rights and freedoms of the persons concerned have been duly taken into
consideration in the process.

51. Furthermore, the Inspection Service notes that in certain circumstances, categories
particular types of personal data may also be collected and
processed by the participating organizations. For example, participating organizations
could know the websites previously visited by a data subject, which
which would make it possible to deduce or reveal political opinions, religious beliefs
or philosophical, sexual orientation, data relating to health or even
the trade union membership of the persons concerned.

52. The Inspection Service considers that IAB Europe has therefore not complied
adequately the principles of transparency and fairness with regard to the persons concerned.

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

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

54. The IAB Europe24 privacy policy is only available in English. In
Additionally, the Privacy Policy contains several terms which, without explanation
additional, are not clear to those involved. For example, the

Inspection service mentions “services” and “other means”.

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)

24 Room 41.

55. Furthermore, according to the Inspection Service, the information provided is incomplete and inadequate. Firstly, data subjects are not informed of the interests exact legitimate persons pursued by IAB Europe. Second, it is not easy for data subjects to distinguish between the different recipients or categories recipients of their personal data ; the terms "third party" and "partner" are not understandable without further explanation. Thirdly, the persons concerned are not informed, on the one hand, of the reference to appropriate or sufficient guarantees for the international transfer of their personal data outside the EEA or, on the other hand, how to obtain a copy or where it is made available. Fourth, based on of the IAB Europe Privacy Policy, it is not clear to individuals concerned that their personal data can be obtained by IAB Europe via its TCF25. Fifth, the conditions under which people concerned must provide their personal data, in particular if this collection is organized on the basis of a legal, pre-contractual or contractual obligation, are not clearly stated. The persons concerned are also not informed of the possible consequences of a refusal to provide their data.

56. Consequently, the Privacy Policy does not comply with the obligations enshrined by articles 13 and 14 of the GDPR.

Finding 3 - IAB Europe does not provide any compliance checks under the rules of the

TCF policy

57. Based on the two versions of the TCF Policies26, the inspection service considers that IAB Europe does not sufficiently monitor compliance with the rules it has drawn up with regard to participating organizations. In particular, it would be possible for a CMP to continue to exchange personal data with a publisher of which it reasonably believes that it does not comply with the rules imposed by the TCF or the law27.

58. Given the role that IAB Europe assigns itself, namely that of Managing Organization, this disregard for the risks to the rights and freedoms of data subjects would indicate a violation of Article 24.1 GDPR as well as the obligation to provide appropriate security for the processing of personal data, in accordance with articles 32.1 and 32.2 GDPR.

25 IAB Europe Transparency and Consent Framework Terms and Conditions ("Terms and Conditions") (Exhibit 33), p.7.

26 IAB Europe TCF Policies v2019-08-21.3 (Exhibit 32); IAB Europe TCF Policies v2019-04-02.2c (Exhibit 38).

27 IAB Europe TCF Policies v2019-08-21.3 (Exhibit 32), p11; IAB Europe TCF Policies v2019-04-02.2c (Exhibit 38), p6.

Finding 4 - IAB Europe did not maintain a processing register.

59. The Inspection Service also notes that IAB Europe does not consider itself bound to keep a record of processing activities, based on the exception provided for in Article 30.5 GDPR for organizations with fewer than 250 people28. The service inspection also points out that IAB Europe did not initially provide the Service inspection a copy of its record of processing activities.

60. It was only in a second response29 that IAB Europe decided, for the sake of completeness, to provide a record of processing activities, although the organization does not consider itself still not subject to the obligation provided for in Article 30.5 GDPR.

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

61. Based on conclusion 4, and with reference to the delay with which IAB Europe responded
requests for additional information from the Inspection Service,
the service
of inspection concludes that the behavior of IAB Europe within the framework of its investigation is
in violation of the obligation to cooperate under Article 31 of the GDPR.
Finding 6 - IAB Europe has not appointed a data protection officer, although
that as Managing Organization, it reserves the right to access the data (to
personal character) that the organizations participating in the TCF collect and process.
62.
IAB Europe claims30 that it does not meet the conditions referred to in Article 37.1.b of the GDPR,
because “IAB Europe is a professional association whose main activities
consists of providing 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 inform them of the
value that digital advertising brings to the market”. For these reasons, IAB Europe has not
designated data protection officer.
63. According to the Inspection Service, the approach of IAB Europe set out above is not substantiated
by the facts. IAB Europe designed and manages the TCF in its capacity as Managing Organization and,
as such, as well as under the terms and conditions of the TCF of IAB Europe31, has the right to access
to all information provided by the participating organizations, to store it and to
treat them.
28 IAB Europe - Response to Belgian DPA, 26 June 2019 (Exhibit 22), p. 2-3.
29IAB Europe Response to Inspection Report, February 10, 2020 (Exhibit 57).
30 In its response to the inspection service dated 26/06/2019 and 20/08/2019, exhibits 22 and 29.
31 IAB Europe Transparency and Consent Framework Terms and Conditions (“Terms and Conditions”) (Exhibit 33).

A.4.3. - Other considerations than

the inspection department

deems relevant to

assessment of the seriousness of the facts.

64. The Inspection Service refers to the judgment of the Court of Justice of the European Union (here

after the "Court of Justice" in case C-25/17 (Jehovah's Witnesses)32, in which the Court

clarified that the definition of controller must be interpreted in a manner

broad in order to ensure effective and comprehensive protection of data subjects. In this

regard, the Inspection Service argues that IAB Europe is trying to evade its

liability under the GDPR.

65. The Inspection Service mentions the clauses included in title 10 "Liability"

of the TCF Terms and Conditions33, by which IAB Europe imposes the responsibility of the

processing of personal data collected by the parties of the sector of the

digital advertising entirely on CMPs, publishers and other providers

adtech34. Indeed, these clauses expressly provide that IAB Europe does not guarantee in

no way that:

▪

the consent given by the CMPs or publishers, approved partners

(global adtech providers) has been collected and processed in accordance with, among other things,

GDPR;

▪

any data processing carried out within the framework or on behalf of the TCF will be

compliant with all relevant laws and regulations, including GDPR.

AT 5. - Summary of the respondent's response of February 11, 2021

A.5.1. - IAB Europe is not a data controller with respect to the processing

personal data under the TCF.

66.

IAB Europe essentially refutes the Inspection Service's position that the

defendant, in its capacity as Managing Organization, acts as responsible for the

processing of personal data processed by TCF participants.

67. According to the defendant, the TCF in no way obliges the participating organizations 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,

streamlined and standardized way through CMPs. On the other hand, the real purposes

32 Judgment of the CJEU of 10 July 2018, C-25/17, Jehovah's Witnesses, ECLI:EU:C:2018:551.

33 IAB Europe Transparency and Consent Framework Terms and Conditions ("Terms and Conditions") (Exhibit 33).

34 In particular, supply-side platforms, demand-side platforms, Ad Exchanges, advertisers and

data management platforms.

processing are determined by the participating organisations, without the intervention of

the defendant.

68. In the first place, the defendant alleges the absence of legal jurisdiction (ratione

personae) on the part of the DPA, and more particularly of the Inspection Service, to carry out

an investigation and challenge the TCF. The defendant also refers to the capacity of

the DPA to hold the true controllers of the data processing, i.e. the

TCF participants, responsible for possible violations of the GDPR, if applicable.

69. According to the defendant, the TCF as such does not involve any processing of data at

personal character and the inspection report does not show for which activities of

processing IAB Europe must be considered as the controller of the processing of

data.

70. Secondly, it argues that a broad definition of the concept of responsible party

treatment, as proposed by the Inspection Service, is not justified in the

context of the TCF, given that there are already controllers clearly

identified, on the one hand, and taking into account the fact that the TCF has no influence on the

processing of personal data that takes place in the context of the protocol

OpenRTB, on the other hand. More specifically, the defendant mentions the absence of any

influence on the means and purposes of processing within the RTB system.

71.

The defendant also considers that the aforementioned Jehovah's Witnesses judgment does not apply

not to the situation of IAB Europe, for the following reasons:

▪ Unlike the Community of Jehovah's Witnesses, IAB Europe does not organize,

does not coordinate or promote in any way the processing of data to

personal character by TCF participants.

▪ The processing of personal data by TCF participants for purposes

purposes of RTB is not in the interest of IAB Europe.

▪ TCF participants do not have a common goal in dealing with

personal data and only participate in the TCF for the purpose of achieving

their individual purposes in a GDPR-compliant manner.

72. The defendant considers that the judgment in Wirtschaftsakademie35 does not apply to IAB either

Europe, because the defendant never disseminates information (i.e. advertising) for

account or at the request of advertisers, does not choose an advertising platform or

other communication channel and does not set parameters or processing purposes,

unlike the TCF participants who decide these matters. According

the

defendant, IAB Europe does not actively participate in RTB processing and is not

the origin of this treatment, in any way whatsoever. Data processing

35 Judgment of the CJEU of 5 June 2018, C-210/16, Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388.

associated with the OpenRTB protocol is performed exclusively by TCF participants and has
therefore takes place independently of IAB Europe or the TCF.
73. Thirdly, it disputes the definition of controller as it is
explained in the guidelines published by the European Council for the protection of
data (EDPB).36 The defendant claims that IAB Europe does not exercise any power
discretionary as to the purposes or means of the processing of personal data
staff under the TCF. In addition, IAB does not process personal data
personal in a way that could be considered "inseparable" or
“inextricably linked” to the processing of personal data by the
TCF participants. Similarly, the fact that participating organizations pay a
financial fee to IAB Europe does not constitute, according to the defendant, an "advantage
mutual” which would lead to joint processing responsibility.
74. Furthermore, the defendant emphasizes the absence of decisions or guidelines from other
supervisory authorities who could support the opinion of the Inspection Service. In particular, the
Belgian, German, French and British supervisory authorities have not identified IAB
Europe as (joint) controller. More specifically, the Conference
independent data protection authorities of the German Federation and the
Länder noted in September 2019 that IAB Europe only acts as
representative organization in the programmatic advertising sector. Furthermore, the
German supervisory authorities confirmed their position in November 2019,
when they announced that any enforcement proceedings related to complaints against the
online advertising should be brought against TCF participants, but not against IAB
Europe. According to the defendant, the French supervisory authority (CNIL) also accepted
indirectly the idea that IAB Europe was not responsible for the processing carried out by
TCF participants. Also, the UK ICO would never have identified IAB Europe
as a potential controller within the RTB ecosystem, regardless of

any time.

75. Finally, the defendant refers to the possible consequences for other organizations

subject to the GDPR if the Litigation Chamber were to judge 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 organization

umbrella body that draws up and adopts a code of conduct would, by the mere fact of its role as

monitoring, considered jointly responsible with regard to the processing carried out

by other organizations in accordance with this code of conduct.

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

23

A.5.2. - The TCF is GDPR compliant.

has. Legality and legal basis

76. First of all, the defendant claims that IAB Europe, unlike the organizations

participants, is under absolutely no obligation to explain to the Inspection Service the existence

a legitimate interest, including balancing the interests of organizations

participants and the rights and freedoms of data subjects, since IAB Europe does not

does not participate in the TCF and does not act as a data controller.

77. Furthermore, the defendant asserts that the DPA is not authorized to prohibit participants

the TCF to process the personal data of data subjects on the basis

of a legitimate interest. On the contrary, the assessment of the merits of the legitimate interests

invoked by the participants must be done on a case-by-case basis, and cannot therefore be prohibited from

in advance and absolutely by the ODA.

78. With regard to the claims that IAB Europe deals with categories

particulars of personal data in

under the TCF, or would be

jointly responsible for the processing of this personal data by the organizations

participants, the defendant points out that these categories of personal data

personnel may, where applicable, only be processed within the framework of the OpenRTB, by

opposition to the TCF. The defendant refers in this respect to the TCF Policies, which prohibit

expressly the use of the TCF to process special categories of data to

personal character.

b. Transparency

79. Considering the fact that IAB Europe does not act as data controller

personal data processed for the purposes of RTB, the defendant argues that one

also can't expect her to

informed

the people concerned

in accordance with Articles 12 and 13 of the GDPR.

80. Furthermore, the defendant argues that the privacy policy that the Service

of inspection invokes as evidence of possible breaches of the principle of transparency

is applicable exclusively to the processing of personal data collected

on the various Internet sites operated by the defendant, as well as to the data to be

personal character collected within the framework of the participating organizations (in particular,

contact details of representatives of these organizations). In other words, the policy

of confidentiality to which the Inspection Service refers has, according to the defendant,

unrelated to processing activities under the OpenRTB Protocol.

81.

The defendant also disputes any allegation that IAB Europe, in its

as Managing Organization, reserves the right to access personal data

staff collected and exchanged by participating organizations under the TCF

and the OpenRTB protocol. IAB Europe asserts that this assumption is not based on any

evidence and is due to an erroneous interpretation of the possibility offered to the defendant to

treat

personal data of representatives of organizations

participants.

82. Furthermore, the defendant considers that it is entitled to propose the policy of

confidentiality exclusively in English, given that the target audience is mainly

made up of professional and B2B players. The defendant stresses that Belgian law does not

provides for no obligation to make available a privacy policy in

French or Dutch and that, moreover, Belgium has not made use of the possibility

to adopt additional requirements concerning the use of language within the framework

of the EU consumer rights directive.

vs. Security

83. The Respondent submits that the accusations concerning the lack of measures

technical and organizational measures to protect personal data in the

framework of the TCF are unfounded.

84. First of all, the defendant considers that IAB Europe is not subject to Articles 24 and 32

of the GDPR with regard to the processing of data carried out within the TCF, because

the organization is not a controller.

85. Second, the IAB Europe TCF Policies provide that TCF participants must

report breaches of TCF rules to IAB Europe. Once again, the defendant

claims that the Inspection Service is misinterpreting the TCF Policies, in particular by

granting the CMPs the right to end the cooperation if they consider that a publisher

does not comply with the rules, without suffering any contractual disadvantage. Furthermore, the

defendant notes that infringements of the rules provided for by the TCF can always be

reported to the supervisory authorities, who will then take action if they deem it

necessary.

d. International transfer of personal data

86.

IAB Europe refutes the plaintiffs' allegations regarding the international transfer of

personal data under the TCF. The defendant notes in this respect

that these claims are only relevant in the context of the OpenRTB protocol, which

is not at issue in this case. Furthermore, IAB Europe cannot be held

responsible for the transfer under the OpenRTB protocol.

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.

25

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

87. Respondent emphasizes that it may invoke the exception provided for in Article 30.5,

in particular the fact that the organization is not required to keep a register of the activities of

processing, as IAB Europe is not a data controller with respect to

concerns the processing activities carried out within the TCFF and, in addition, the organization

has less than 250 employees. Nevertheless, the defendant emphasizes its own initiative

to draw up a register and submit 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. Given the nature and scope of the processing activities carried out by

organization, the defendant indicates that IAB Europe is not required to appoint a

data protection officer, the criteria set out in Article 37 of the GDPR not being

full.

A.5.5. - IAB Europe cooperated with the Inspection Service.

89. The respondent refutes the allegations of insufficient cooperation with the investigation, noting

that the deadlines imposed by the Inspection Service on the parties to an investigation are not

no cases determined by law, but must be the result of a reasonable evaluation and

must take into account the specific circumstances of the case. In this case, the defendant

believes that IAB Europe has always cooperated in good faith and provided information and

responses with the aim of clarifying its status with respect to the TCF and demonstrating its

GDPR compliance, as it applies to IAB Europe.

90. In addition, the defendant observes that the duty of cooperation provided for in Article 31 of the GDPR

can in no way be interpreted as an obligation to provide documentation

in accordance with the provisions of the GDPR which the defendant does not consider as

necessary.

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

91. Finally, IAB Europe disputes the conclusion of the Inspection Service that the refusal to

the defendant to recognize that IAB Europe acts as data controller,

as well as the large volume of personal data processed and organizations

participants, can be considered as aggravating circumstances.

92. The defendant refers to the absence of clear evidence in the investigation report that these

circumstances are aggravating and concludes that

the allegations are due to a

insufficient knowledge of how the TCF works. Therefore, the defendant

26

asks the Litigation Chamber not to take into account the opinion of the Service

inspection.

A.6. - Summary of the plaintiffs' conclusions of February 18, 2021

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

has. Processing of personal data in the TCF

93. Complainants argue that a unique identification number, such as the generated TC String

and stored in a cookie, is personal data within the meaning of Article 4,

paragraph 1, of the GDPR, a position which has also been expressly confirmed by the

pre-GDPR case law.

94. However, according to the Complainants, the TC String is more than just a unique identifier, because IAB

Europe would also use it to collect information regarding applications

that a data subject uses and the websites that he or she visits. It could also

reveal sensitive data about data subjects within the meaning of Article 9 of the GDPR.

95. Furthermore, the generation of the TC String constitutes in itself, without any doubt, a processing of

personal data. The problem in question is the automated creation, for

a CMP member of the TCF, a unique and linked set of characters intended to capture the

preferences of a specific user regarding authorized exchanges of data with

advertisers.

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

has. by storing the TC String in a global consent cookie shared on the

Internet domain IAB Europe consensus.org; Where

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

a service-specific authorization.

97. According to the complainants, in both cases, IAB Europe is the data controller of these

processing operations. The intervention of IAB Europe is all the more drastic

assuming the global shared consent cookie. Indeed, this cookie of

shared global consent that stores

the TC String points to

the domain

“consensu.org”, operated by IAB Europe, from which CMPs can access and update

update the shared TC String.

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

TCF.

98. First of all, the Complainants submit that IAB Europe, in its “Frequently Asked Questions”

questions" on the TCF, explicitly indicates that it is responsible for the TCF Policies.

27

99. According to the Complainants, it goes without saying that the organization which manages and operates the TCF is also

the controller of this system, including any processing of data to

personal character imposed and organized by the TCF. Indeed, IAB Europe imposes these

personal data processing operations to other participants of

binding manner.

100. In addition, IAB Europe requires CMPs to implement the TCF in accordance with

strictly its Technical specifications. In the Technical specifications of the TCF, 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 global consent, to store the

character string in a global consent cookie shared on the domain

“consensus.org”. As this Internet domain is registered and managed by IAB Europe, the

defendant also has access to the personal data processed in the TCF.

102. Furthermore, according to the Complainants, IAB Europe determines the “essential means” for the

processing of personal data within the TCF. On the one hand, IAB Europe

specifies in detail the elements that must be included in the TC String. And, on the other hand, IAB

Europe determines the categories of recipients of this personal data,

since the defendant is responsible, according to its own terms, for the management of the

Global Vendor List and the management of CMPs participating in the TCF.

103. Complainants also submit that the TCF does not provide an effective mechanism for

enforce certain elements of the TCF Policies 38, whereas a code of conduct is supposed to

be an effective system for compelling its members to comply, as provided

GDPR Article 41.

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

levels

has. Violation of the principles of purpose, proportionality and necessity

104. According to the Complainants, IAB Europe collects the preferences of TCF users via the TC

String for a vague, inaccessible and abusive purpose, while character data

personal data processed are insufficient and irrelevant for this purpose.

105. Furthermore, the processing itself would be anything but proportionate, which means that IAB

Europe violates Articles 5(1)(b) and 5(1)(c) GDPR, as well as its duty

liability as controller, provided for in Article 5, paragraph 2 of the

GDPR. Furthermore, the plaintiffs consider that with the design of the TCF, IAB Europe does not

does not provide the guarantees necessary to comply with the requirements of the GDPR and to protect

38 See para. 133 et seq. of this decision.

the rights of data subjects; therefore, the defendant violates Article 25

GDPR.

The purpose of the processing of the TC String is neither specified nor explicitly defined

for those affected, nor is it justified.

106. According to the complainants, IAB Europe does not provide information to data subjects

regarding the processing of their personal data in the TCF.

107. The purpose of the TC String within the overall objective of the TCF is to capture the

information provided to users and their processing preferences. In others

terms, IAB Europe does process personal data (in particular the TC

String) as part of the TCF because it claims it could make processing

underlying GDPR-compliant marketing. According to the complainants, it is therefore this

purpose which must be assessed with regard to its legality, and in the light of this purpose, it

should assess the proportionality and necessity of the processing carried out by the TC

String as part of the TCF.

The TC String is inadequate and irrelevant for the intended purpose

108. Complainants further claim that the processing operations of the TC String within

of the TCF are insufficient and irrelevant to ensure compliance with the GDPR when

personal data is processed by the OpenRTB protocol.

109. The OpenRTB protocol contains an inherent security issue that makes it impossible for

a system such as the TCF to ensure, among other things, transparency and accountability

necessary with regard to personal data, including the categories

special types of personal data, processed in a bid request after this

this has been sent.

110. The central idea of the TCF is that participants collect user preferences

and pass them as the TC String, so that other participants take

rate the content (i.e. read the TCF signal) and thus be able to respect the preferences

users. However, according to the plaintiffs, there is nothing in the TCF, or in any

system or related mechanism, which effectively ensures that participants in the

OpenRTB protocol are bound by the TCF signal. The TCF signal is therefore nothing more than a

simple notification.

111. Given the inherently unlawful nature of the processing of personal data

personal in the OpenRTB protocol, on the one hand, and of the nature intrinsically

imperfect of a purely signal-based system such as TCF without control

effective, on the other hand, the use of the eTCF, including the processing of the TC String, cannot

never give participants the assurance of being in compliance with the GDPR. Indeed, the

TCF makes no warranty that TCF participants will comply with their obligations

liability (article 5.2 of the GDPR). Nor can it provide protection.□

adequate personal data shared by the OpenRTB protocol (article□

5.1..fGDPR).□

IAB Europe has set up the TCF in such a way that data protection□

is not guaranteed from the design stage.□

112. Complainants argue that the design of the TCF, due to its character□

disproportionate, cannot guarantee the level of data protection required by Article 25□

GDPR, in particular with regard to the obligation to implement technical measures and□

appropriate organizational arrangements to ensure that, in principle, only the data to be□

personal character which 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 because, according to the complainants, this purpose□

cannot and will not be achieved in any event.□

114. Further, the complainants argue that the TC String, as personal data□

independent that uniquely identifies users, is shared with many□

participants through various mechanisms, including IAB's own mechanism□

Europe of the global consent cookie shared on its domain□

Internet□

“consensus.org”.□

b. Violation of the principles of fair, lawful and transparent treatment (Articles 5, 6, 12,□

13 and 14 GDPR).□

115. The complainants allege that the persons concerned are in no way informed□

because□

their personal data (including□

the TC String) are□

systematically and widely handled by IAB Europe within the TCF.

116. According to the complainants, the processing of the personal data of the complainants and

Other IAB Affected Persons in the TCF is ultimately:

▪

anything but legal since there is no legal basis;

▪ neither appropriate nor transparent, since it takes place entirely “behind the back” of

data subjects, without any form of notification.

The processing carried out by IAB Europe has no legal basis and is therefore

illegal.

117.

IAB Europe cannot rely on the consent of the persons concerned (article

6.1.a GDPR), according to

the complainants, because she did not

never asked for or obtained such a

consent. Similarly, TCF Policies, Technical specifications and TCF Terms

30

and Conditions nowhere mention a mechanism by

which IAB Europe

would ask data subjects for permission to generate a string

unique identifier that would share their privacy preferences with

a mass of recipients, even in cases where these people indicate in a CMP

that they do not wish to share their personal data with anyone

that is.

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 Complainants and others

persons concerned (article 6.1.b), because there is no contract between the persons

concerned and IAB Europe.

119. Furthermore, the Complainants argue that the Respondent cannot invoke 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 balance between interests would always be
favor of the persons concerned.

120. First of all, the processing of the TC String does not benefit the data subjects, because
the TCF is not in a position to guarantee security, accountability or transparency. In
Besides, there is no legitimate interest, because this interest is nowhere sufficiently clearly
formulated and it is not possible to weigh it against the interests and rights
fundamentals of the people concerned.

121. Next, in balancing the interests, the 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 this personal data
personal are processed, the reasonable expectations of the data subject and the status of the
controller and data subject.

122. According to the complainants, the consequences of the processing of the TC String are particularly
burdensome for those involved. IAB Europe processing operations
would lead TCF participants to assume that they are correctly informing
data subjects of the processing of personal data by the protocol
OpenRTB, when such is not the case. This would then lead to the sharing and distribution
illicit use of personal data, even sensitive ones, on a considerable scale via
the OpenRTB protocol.

123. The processing of the TC String by IAB Europe would result in the sharing of an online identifier
single with an incalculable number of parts, following the example of what happens with the
unique identifiers in advertising cookies from major advertising companies. He
would therefore allow easy tracking of users on the web and on different devices

(“web and cross-device tracking”). Further, the plaintiffs argue that the TC String may
be combined with data distributed via the OpenRTB protocol, because the TC String is
embedded in a bid request.
31
124. Given the lack of information of the persons concerned on the operations of
processing within the TCF and unrestricted sharing of the TC String with a group
almost unlimited number of recipients, it is clear to the plaintiffs that these operations of
processing exceed the reasonable expectations of data subjects. In
Furthermore, those affected, such as complainants, do not expect the
processing of personal data under the TCF entails the sharing of
their personal data, sometimes sensitive, and their detailed profiles with
many companies through the OpenRTB protocol, without any control
real and effective about what these companies will do with personal data
obtained.
125. The plaintiffs in this case are individuals and interest groups
representing the data protection interests of natural persons.
They have no control over the processing of personal data within the framework
of the TCF (which takes place regardless of whether consent is given or denied in a CMP).
They also have no control over what happens to their personal data.
shared by the OpenRTB protocol. According to the complainants, the persons concerned do not
cannot verify whether OpenRTB participants are indeed following the rules of the
TCF.
IAB Europe processes personal data under the TCF of
surreptitiously, without any form of notification, and the processing is not
therefore neither appropriate nor transparent.
126. Despite the extensive documentation that IAB Europe makes available to TCF participants

on its website, it does not state anywhere that the TCF itself also involves the
processing of personal data, according to
the complainants. In addition,
the
documentation expressly disclaims, with respect to TCF participants, that the TCF
itself involves the processing of personal data.
127. The TCF implementation guidelines seem to suggest that there are
assumptions in which participation in the TCF does not involve the processing of data
of a personal nature. Ultimately, advertisers and DSPs, who are already participating in the
TCF are informed that they must register as adtech providers if they deal
personal data. According to the complainants, this implies that they would not have
to do so if they were not processing personal data. However, this last situation
is entirely impossible, according to the plaintiffs, because the TCF inherently requires the processing of
personal data.
128. According to the complainants, the statements contained in the IAB Europe guidelines are
misleading for the hundreds of adtech vendors that use the TCF. Given
that IAB Europe does not inform TCF participants of the processing of personal data
32
staff that necessarily involves the implementation of a TCF, none of these
participants is informed or does not realize that it has an obligation of transparency. Of this
manner, data subjects - such as complainants - are not informed by any
participant in the processing of personal data within the TCF.
129.
IAB Europe is also not respecting its own obligation of transparency. Neither on its own
website or in other sources, the defendant does not communicate the information
required by Articles 13 and 14 to data subjects, such as complainants. That

would include the following information: that IAB Europe is the data controller□

TCF data and contact details; the contact details of its protection officer□

Datas ; what are the purposes of its processing and the legal basis for the processing;□

what are the categories of personal data processed (in particular the TC□

String); who receives the personal data (at least all TCF participants□

receive the TC String); that IAB Europe intends to transfer the personal data□

personnel to recipients in third countries; how long the data to□

personal character are retained; what are its legitimate interests for the processing;□

what are the rights of data subjects; that the persons concerned can□

lodge a complaint with the data protection authority; that people□

concerned can withdraw the consent they have given; and finally, what is the□

source of personal data.□

130. At the same time, IAB Europe cannot invoke any of the exceptions provided for in□

Article 14.5 of the GDPR for not having to provide this information, since:□

has.□

the persons concerned are not yet in possession of the information,□

since the processing concerning them has so far been carried out in secret□

(Article 14.5.a GDPR);□

b.□

it is not impossible to bring this information to the attention of the people□

concerned and does not require a disproportionate effort, taking into account□

the influence that IAB Europe exerts on the functioning of the TCF (article 14.5.b□

GDPR);□

vs.□

the acquisition of this data is not prescribed by law (Article 14.5.c of the GDPR);□

and□

d.

personal data should not be kept confidential for

reasons of professional secrecy (article 14.5.d GDPR).

IAB Europe's reference to the Vectaury case in France is irrelevant.

131. According to the Complainants, IAB Europe mistakenly believes that it can rely on the decision of

the French supervisory authority CNIL in the Vectaury case. Indeed, IAB Europe affirms to

wrong that it would be strange for the Inspection Service to find offenses relating to the treatment

personal data in the TCF, while the CNIL would not, according to the

33

defendant, raised no problem with regard to the legitimacy of these treatments. The

plaintiffs claim that IAB Europe makes assumptions and draws conclusions that do not

absolutely cannot be inferred from the Vectaury case:

• First of all, the Vectaury case concerned the specific implementation of a CMP

by Vectaury which would have made it possible to implement the TCF. The role of IAB Europe

was not the subject of this procedure and the CNIL therefore did not rule, nor investigate, on

IAB Europe's role in providing the TCF.

• Second, this case specifically concerned the question of whether the

implementation of the TCF by Vectaury could put the underlying treatment of

GDPR-compliant real-time bidding systems. The verdict of the

CNIL was clearly negative, as evidenced by the fact that Vectaury itself

indicates on its website that it has created a completely new method in dialogue with

the CNIL. According to the complainants, it is therefore misleading for IAB Europe to

claim that the CNIL would have legitimized the TCF in itself as sufficient to allow

GDPR compliance of real-time bidding systems.

• Third, the plaintiffs argue that the CNIL investigation did not relate to

the legitimacy of the processing of personal data within the TCF. The

CNIL did not consider the generation and distribution of the TC String as a

autonomous treatment and therefore made no statement about it.

132. According to the complainants, the decisions of the CNIL in the Vectaury case are therefore not

relevant, as it was a clearly different case, directed against a different party,

involving different treatments and under legislation which has since been superseded. The

Litigation Chamber follows the point of view of the plaintiffs and does not discuss the case

Vectaury, which concerns a different case from the present.

vs. Violation 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 as it facilitates the exchange of personal data in the TCF, in particular

exchanging the TC String, with many parties, without checking if 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 and 32

GDPR. However, IAB Europe has not integrated an appropriate protection mechanism:

As with any other processing in the OpenRTB protocol, there is no way to

verify that recipients are indeed processing the TC String in accordance with the GDPR.

Indeed, the plaintiffs claim that none of the mechanisms presented by IAB Europe is

based on a real and proactive monitoring of compliance with the TCF.

34

135. Complainants contest IAB Europe's argument that it is not required to

comply with the TCF, and in particular the agreements entered into under the TCF. Complainants

claim that it is indeed his duty, as data controller,

to implement the agreements concluded within the framework of the TCF and, at least in this way, to

provide certain guarantees for the secure processing of the TC String.

136. Second, the Complainants point to IAB Europe's assertions that, in
As a management organization, it makes "substantial efforts" to enforce the
agreements concluded within the framework of the TCF. According to the complainants, there is no evidence of these
so-called "substantial efforts". The plaintiffs further claim that IAB Europe should
verify compliance with all agreements by each registered TCF participant, which,
given the scale of the data processing, would involve a very large survey
magnitude. Furthermore, the complainants refer to the answer given by IAB Europe itself
to the Inspection Service: "The reporting obligation itself is not currently
controlled. Also, it is difficult to control it as it would be difficult for IAB Europe
to establish if and when a PPC has (or should have had) a "reasonable belief" that another
party did not comply with the regulations"39.
137. Third, the Complainants submit that IAB Europe is wrong to try to hide
behind the contractual arrangements. According to the plaintiffs, the defendant claims that it
sufficient that participants are contractually obligated to report any non-compliance
at IAB Europe.
138. The complainants also argue that IAB Europe, as data controller
data from the TCF, is bound by articles 5.1.f and 32 of the GDPR, although it is practically
cannot guarantee the security of the processed TC String when shared with thousands
recipient companies. According to the plaintiffs, this last point would mean that IAB Europe
actively checks that all recipients of the TC String still respect the
GDPR obligations, so the processing of the received TC String would not be unlawful.
139. Moreover, according to the complainants, practice proves that almost all TCF participants
are illegally processing the TC String, because not a single CMP, not a single publisher, and not a single
seller only provides information on the processing of the TC String, its purpose, its basis
legal or the categories of recipients. This would imply, according to the complainants, that the
transfer of the TC String to these parties is in itself a data breach

personnel which, given its considerable size, gives rise to an obligation to

notification to supervisory authorities.

140. The practical impossibility of providing the guarantees necessary for the protection of personal data

personal character (in particular the TC String) of the persons concerned, when they

are shared with thousands of recipients within the OpenRTB protocol, demonstrates,

39 Letter from IAB Europe to the inspection service of February 10, 2020, p. 8.

according to the plaintiffs, that IAB Europe is in breach of its obligations under the

articles 5.1.f and 32 of the GDPR.

d. The systematic transfer of the TC String to third countries without adequate protection

(violation of Article 44 of the GDPR).

141. Complainants claim that IAB Europe set up the TCF in such a way that

personal data - including the TC String, as it is embedded in requests

offers - are structurally transferred as part of OpenRTB to many

companies located outside the European Economic Area (EEA), without protection

adequate is ensured for these transfers.

142. The complainants refer to the Ad Exchange Xandr (based in the United States), which is affiliated with the

TCF from IAB Europe and therefore receives at least the TC String from EEA users including

the complainants. As responsible for the processing of personal data

in the TCF, IAB Europe must provide a mechanism for transferring personal data

personnel so that Ad Exchanges established outside the EEA can receive the TC

String.

143. Trading the TC String via real-time auction systems such as OpenRTB

are structural in nature and repeat themselves continuously in fractions of seconds. In

indeed, the TC String is sent with the requests for offers. It would therefore be impossible for

IAB Europe, according to the plaintiffs, to invoke one of the exceptions provided for in Article 49 of the

GDPR.

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

145. In accordance with the Schrems II judgment, IAB Europe40 should have, in addition to choosing a form of adequate safeguards, take additional measures to prevent the personal data are not processed in a non-compliant manner in countries third. However, these additional measures are just as insufficient as the appropriate safeguards. The TC String is blind shared with an indefinite number of participants in the OpenRTB protocol, wherever they are in the world.

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

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

A.7.1. - Organizations that process personal data in the context of the RTB system are required to comply with the GDPR and the "Privacy and electronic communication".

146. The defendant first claims that any party participating in the RTB and using the OpenRTB protocol can intervene in the technical operations of storage and/or access on a user's device (e.g. placing website cookies) by under the “Privacy and Electronic Communications” Directive, and/or act as controller or processor of personal data (for example, for digital advertising purposes) under the GDPR. Where applicable, all such parties are responsible for complying with their obligations under the GDPR and the Privacy Directive and Electronic Communications” when engaging in the RTB.

147. Furthermore, according to the defendant, there are thousands of companies engaged in the RTB and

using the OpenRTB protocol, which however do not participate in the TCF. Likewise, the□
parties may use the TCF for purposes other than the RTB. IAB Europe also highlights□
that publishers can use the TCF for a range of online advertising scenarios□
other than the OpenRTB protocol - including other types of RTB protocols, but also□
online advertising that does not involve RTB at all, such as direct inventory selling□
advertising.□

148. The Respondent also refutes the Plaintiffs' allegations that the RTB□
is inherently illegal by reference to the report of the UK supervisory authority□
(ICO) which simply stated that the RTB “requires organizations to assume the□
responsibility for their own data processing, and for the industry to reform□
collectively the RTB”. The ICO would also have highlighted the efforts made in good faith□
by stakeholders such as IAB UK to contribute to this reform process in□
a more recent publication.□

149. In addition, the defendant indicates that several supervisory authorities have requested□
ways to increase□
transparency for□
the persons concerned in□
identifier□
clearly the data controllers with whom the personal data□
will be shared, specifying the purposes of the processing and allowing individuals□
concerned to exercise control over their personal data. This is□
precisely this type of transparency measure that IAB Europe and the TCF intend□
sustain.□

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

started/.□

2020,□

37□

150. Under the TCF, data subjects have the possibility to give their consent□

prior to a certain number of identified third parties (adtech providers) and purposes of□

treatment. According to IAB Europe, this transparency and due diligence constitute a□

appropriate substitute, from a legal compliance point of view, for consent in time□

real, on-the-fly and one-by-one for data access, storage and processing by□

data controllers.□

A.7.2. - IAB Europe cannot be held responsible for the alleged illegal practices of□

participants in the RTB, as the TCF is completely separate from the RTB.□

151. Respondent points out that the TCF is only one of many optional approaches□

which data controllers may choose to help ensure compliance with□

transparency and consent requirements when processing personal data□

personal character for RTB or other advertising purposes. Therefore,□

responsibility for compliance and effective decisions on objectives and means□

of these personal data processing operations is entirely the responsibility of□

to parties engaged in the RTB, not to IAB Europe.□

152. The defendant also states that IAB Europe had contacts with several□

supervisory authorities after the deployment of the first version of the TCF, as well as with□

several publishers. As a result of these discussions, the second version of the TCF was□

elaborate, in which several processing purposes have been grouped under a single□

title in "stacks", and legitimate interest was introduced as a possible legal basis. In□

Additionally, the TCF v2 introduces additional goals and "editor controls" that□

allow publishers to restrict access to a particular objective to a sub-□

set of adtech vendors.□

153. Finally, the defendant specifies that IAB Europe always intended to have the
TCF as a transnational code of conduct.
154. In his conclusion
initial,
the defendant advances procedural arguments
regarding the jurisdiction of the DPA and the manner in which the complaints and investigation were
processed. These defenses are set out below in Section A.9.
155. In its summary submissions, the defendant also asserts that the manner in which
the DPA conducted the procedure does not comply with Article 57 of the GDPR. However, the
complainants were unable to respond, the proceedings were reopened at the request
of the Litigation Chamber.

AT 8. - hearing and reopening of proceedings
156. In accordance with article 51 of the rules of procedure of the Authority for the protection of
given, a hearing was held, to which all parties were invited.
The hearing took place on June 11, 2021.
157. A written record of the hearing is drawn up in order to give the details and information
additional information that was provided during the hearing, without repeating the elements
set out in the conclusions. The parties also had the opportunity to submit their
written comments on the file. A number of items mentioned below
are relevant to this decision.
158. During the hearing, the Inspection Service first confirms its position according to
which IAB Europe acts as data controller
staff under the Transparency and Consent Framework, but not for
OpenRTB.
159. The Inspection Service also specifies that personal data are

collected as provided for in the TCF Policies, in the general conditions42 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 the preferences of a
user should also be considered as personal data.
The Inspection Service also points out 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 user preferences that are collected in the context of the TCF, and
personal data of this same user which is collected and distributed to the
within the OpenRTB protocol. In conclusion, the Inspection Service declares that the values
TC String and the euconsent-v2 cookie do not in themselves identify a user
individual. Although both elements contain personal data,
in the sense that the information relates to a natural person, the Inspection Service
also confirms that it is not possible to identify the specific data subject
based on this information alone.
160. During the hearing, counsel for the defendant raised a point of procedure, namely
that the Litigation Chamber is not authorized to rule on the elements
presented by the complainants before an analysis was carried out on the consistency of
their conclusions with all the complaints. The defendant also asks the
Litigation Chamber to rule on the need to request an investigation
complementary to the Inspection Service, as required by Article 57.1.f GDPR. The
42 IAB Europe Transparency and Consent Framework Terms and Conditions (“Terms and Conditions”) (Exhibit 33),
p.7.

Litigation Chamber will rule on this point of procedure in this
decision43.

161. The Complainants responded orally to the Respondent's procedural arguments at the course of the hearing.

162. With regard to the moment at which the TC String is generated, the defendant emphasizes that notification of this moment cannot lead to the uniqueness of a TC String, because there exists a chance that two unidentified users can give the same preferences to the same time. Moreover, this duration is not enough to speak of a single chain, since the values of the TC String are not persistent and may vary over time or in depending on the websites visited.

163. The defendant also indicates that the scenario of global consent cookies, in which the preferences stored in a TC String apply to multiple websites, is not relevant given its limited scope at the time of the hearing44, as well as the intention of IAB Europe, following the finding that a global consent does not meet the requirement for specific consent45, not to no longer supporting this feature and phasing it out in weeks depending on the hearing.

164. Regarding the question of whether the assignment of a subdomain of consensus.org to a CMP by means of a DNS delegation can be considered as a determination means of processing, the defendant argues that, due to DNS delegation, each sub-domain refers to the CMP servers, which are moreover the only ones able read TC Strings from user devices. Furthermore, the defendant argues that registering a consensu.org subdomain is purely optional and, as as such, does not constitute an essential means of treatment.

165. The complainants point out, on the other hand, that a DNS delegation can always be canceled by the defendant, and that it is immaterial that the defendant does not have access to the cookies

euconsent-v2. Complainants also point out that DNS delegation can be

considered an essential means of processing, since DNS delegation is

used to distribute the TC String further in the TCF ecosystem.

166. Regarding the existence of interfaces between the TCF and OpenRTB, the Complainants point out

that the two systems are intrinsically intertwined due to 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, the

43 See para. 174 et seq. of this decision.

44 According to the defendant, the number of global consent cookies was a maximum of 0.5% of all

consents and preferences collected around the world.

45 Article 4.11 GDPR: “consent” of the person concerned, any expression of will, free, specific, informed

and unequivocal by which the person concerned accepts, by a declaration or by a clear positive act, that data to be

personal character concerning him are the subject of processing;

RFPs, which are regulated by OpenRTB. In other words, these are

used as vehicles to spread the TC String across the OpenRTB ecosystem.

167. Respondent asserts that the two systems can operate independently and

that the TCF was developed with OpenRTB as a starting point and could be used

in this context, with OpenRTB being the most widely used standard in the industry. According

the defendant, this does not mean that the TCF is an essential means of using

the OpenRTB.

168. Respondent claims that Respondent's development of a future code of conduct

in relation to the TCF cannot be considered as proof of its responsibility

(shared) regarding the processing of personal data in the context of the

TCF. The complainants add that it is impossible to verify compliance with the GDPR by the

participating organisations, even if the rules are clearly defined in a policy

of application.

169. In this respect, the defendant refers to the elaboration and progressive implementation
automated compliance programs to monitor the extent to which CMPs and
advertisers (as well as other adtech providers) comply with the TCF Policies, including
including future internal audits of the above parties' processes. The defendant
also points out that the TCF already provides for sanction measures against
adtech providers who do not adhere to the framework, such as the temporary suspension of their
participating in the TCF.
170. As regards the link between the TC String and the individual user, the defendant considers
that the TCF does not determine how this is done, nor how the TC String is then
communicated to adtech suppliers, these elements being entirely subject to the
OpenRTB protocol.
171. The defendant specifies that
use of the consensus.org domain is purely
optional, and further that this domain has not been developed for the purpose of addressing or
store logs related to TC Strings.
172. Finally, the defendant emphasizes its position that the TC String does not constitute a
personal data only after having been linked within the framework of the OpenRTB to a bid
request which already contains personal data.
173. On August 9, 2021, after deliberation, the Litigation Chamber decided to reopen the proceedings
on the specific procedural arguments of IAB Europe.
174. On August 23, 2021, the Litigation Chamber received the first conclusions of the
defendant. The defendant asserts that the Belgian supervisory authority (DPA) violated
GDPR Article 57.1.a and 57.1.f and LCA Article 94(3). ODA would also not have
respected the principle of good administration and the defendant's rights of defence.

175. With regard to Article 57.1.f GDPR, the defendant first argues that the

plaintiffs presented new allegations in their pleadings, which are therefore more

extensive than the initial complaints. Moreover, according to the defendant, the DPA did not investigate

proactively on these new allegations by instructing the Inspection Service to

new or additional investigation. Consequently, the defendant considers that

the DPA has breached its obligations under Article 57.1.f GDPR.

176. Furthermore, defendant submits that, by requesting an initial investigation from the Service

of inspection, the Litigation Chamber is bound de facto to a procedure in which

each allegation or defense must be examined by the Inspection Service. According to

defendant, the decision of the Litigation Division not to request additional

of investigation after an initial investigation and the presentation of the means of defense led

to a violation of Article 94(3) of the ACL.

177. The defendant also indicates that in the absence of an investigation by the Inspection Service

on supposed new allegations in the defenses of the plaintiffs and a

legal qualification of these allegations, it was unable to defend itself against

adequately against complaints filed against IAB Europe. Thus, the procedure

before the Litigation Chamber could be considered as having evolved from a

procedure

inquisitorial to an adversarial procedure in

which

bedroom

Contentious would no longer have acted as an administrative dispute resolution body,

mainly taking into account the claims and documents of the plaintiffs,

so that the rights of defense of IAB Europe would have been violated, according to the defendant.

178. On September 6, 2021, the Litigation Chamber received the complainants' submissions. The

plaintiffs consider, first of all, that the defendant's new pleas exceeded

the limited framework of reopened debates.

179. Second, the Complainants claim that the nature of the proceedings has not changed in any way,

since the procedure was initiated due to complaints lodged with the DPA, in

other words, as an adversarial procedure, and that it remained so throughout

the procedure.

180. Third, the Complainants refer to Articles 63(2) and 94 of the LCA,

as a counter-argument to the assertion that the Litigation Chamber should have

have the Inspection Service examine each of the grounds raised by the complainants.

Indeed, these provisions confer on the Litigation Chamber a discretionary power

to decide whether an (additional) investigation by the Inspection Service is necessary or

nope.

181. In addition, the complainants argue that it is impossible for the Litigation Chamber to

have an investigation or an additional investigation carried out by the Inspection Service

after the conclusions and documents of the parties, taking into account the limited deadlines of 30 days after

42

that the Litigation Chamber was seized by the Frontline Service after the filing of

the complaint, or by the Inspection Service after receipt of the initial investigation report.

182. With regard to the Respondent's argument that the manner in which the Chamber

Litigation has handled the file violates article 57.1.f GDPR, the plaintiffs point out that, while

first, this provision has no direct effect in the sense that the defendant could

derive rights. The plaintiffs also claim that this provision cannot

affect the internal structure and functioning of the supervisory authorities, which, with regard to

concerns ODA and, more specifically, the distribution of powers between its Service

of inspection and its Litigation Chamber, are subject to administrative law (procedural)

Belgian.

183. Furthermore, the Complainants point out that Article 57.1.f GDPR does not refer to a

obligation for

the Litigation Division to request an investigation by the Service

of Inspection on the complaints, but with the capacity of the authorities of control to close the business.

184. In addition, the Complainants claim that the decision of the Litigation Chamber to request

an investigation by the Inspection Service in no way prevents it from relying on the

conclusions and exhibits submitted by the parties, contrary to the position of the

defendant.

185. With respect to the defendant's alleged breach of the principle of diligence,

the plaintiffs maintain that the Litigation Chamber is required, by virtue of this principle,

to properly study all the documents in the file so that its decision is based on a

correct and complete presentation of the facts. However, this principle in no way implies

that the Litigation Division should have a (complementary) investigation carried out by the

Inspection service for each exhibit.

186. With regard to the defendant's rights of defence, the plaintiffs submit

that, on the basis of the various investigation reports of the Inspection Service and the memoranda

and exhibits presented by the plaintiffs, the defendant was sufficiently informed of the

facts and alleged violations of law. Moreover, according to the plaintiffs, the defendant had

sufficient opportunity to defend themselves in writing against the legal claims and

facts made by the plaintiffs, given that the defendant can submit two

conclusion games.

187. Finally, the complainants refer to the absence of concrete examples, in recent

conclusions of the defendant, alleged new allegations on which the

defendant was unable to conclude or which were not investigated

by the Inspection Service.

188. On September 13, 2021, the Litigation Chamber received the respondent'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 full review of the

facts. In addition, the defendant argues that the decision of the Litigation Chamber of

requesting an investigation from the Inspection Service had the effect of transforming the whole

of the procedure into an "inquisitorial" procedure, regardless of whether the procedure

finds its origin in the complaints lodged with the DPA. According to the defendant, the

decision of the Litigation Chamber not to subsequently request additional

of investigation and to base the rest of the procedure solely on the conclusions and documents

of the parties constitutes a violation of his rights of defence.

190. Furthermore, the defendant is of the opinion that the thirty-day period provided for in Article 96, paragraph 1,

of the LCA does not apply to the request of the Litigation Chamber to proceed with

further investigation by the Inspection Service.

191. The defendant bases this reasoning on the distinction made in administrative law

general between expiry periods and order periods. In particular, the defendant

considers that, in the absence of formal provisions in the LCA according to which the

exceeding the 30-day period entails a loss of jurisdiction of the Chamber

Litigation, the deadlines provided for in Article 96 must be respected, but not

nullity of the decision rendered too late. According to the defendant, the Litigation Chamber

therefore remains competent to take an additional investigation decision even

after the expiry of the 30-day order period. This interpretation, according to the defendant,

is in fact the result of the greater importance of the right to defense compared to the right

to a rapid procedure before the Litigation Chamber.

192. As regards the direct effect of Article 57.1.f GDPR, the defendant asserts that

the existence of a margin of discretion for the Member States does not exclude the direct effect

of a provision, but involves examining whether this provision is intended to offer a guarantee to

parts. The defendant considers that Article 57.1. f GDPR meets this requirement and

clarifies that its argument for requesting further investigation is further limited to

an assessment in fact and in law of the supporting elements of the procedure.

193. In conclusion, the Respondent states that it did not receive a clear statement of the nature and the scope of the charges, with the exception of the allegations made in the factums in defense of plaintiffs. In this regard, the defendant asserts that the control reports technical only contain technical descriptions, in which, in addition, the TC String is not mentioned anywhere. In section A.9.- Procedural objections raised by the defendant, the Litigation Chamber indicates the reasons why procedural safeguards, including regarding the nature and scope of the charges, have been respected.

44

A.9. - Procedural objections raised by the defendant

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

has. Inadmissibility of complaints

194. The defendant first argues that some of the complaints were filed in English and therefore do not meet the formal conditions of admissibility laid down in Article 60 of the LCA.

195. Furthermore, the defendant considers that some of the persons who lodged complaints cannot be considered either as "complainants" nor as "parties" within the meaning of Articles 93, 95, 98 and 99 ODA, so that their conclusions must be excluded from the debates and cannot be taken into account.

196. Finally, the defendant asserts that the measures which the DPA may impose under Article 100 of the ACL provide no benefit to these plaintiffs.

197.

IAB Europe therefore considers that the case was unlawfully brought - in particular on the basis of several inadmissible complaints - so that the grievances formulated against him must

be rejected and cannot lead to the imposition of a sanction or measure

corrective valid at IAB Europe.

Position of the Litigation Chamber

198. The Litigation Chamber refers to Article 77.1 of the GDPR, according to which persons

concerned have the right to lodge a complaint in the Member State where they reside

usually have their place of work or in which the alleged offense was committed.

The four complaints in English mentioned by the defendant were not filed

directly with the DPA, but with the supervisory authorities competent to

each of the complainants, in accordance with the locally applicable language legislation. In

casu, the four complaints were lodged respectively with the supervisory authority

Polish SA, the Slovenian SA, the Italian SA as well as the Spanish SA, which then

forwarded these complaints to

the Belgian DPA as lead supervisory authority,

in accordance with the cooperation procedure provided for in Article 56 of the GDPR.

199. The formal conditions of admissibility provided for in Article 58 of the LCA, and more

particularly the obligation to write the complaint in one of the national languages,

apply only to complaints lodged directly with the DPA. Any other point of view

would undermine the proper functioning of the right to lodge a complaint, one of the fundamental elements

of the GDPR. Indeed, one cannot expect a complainant who submits his complaint to an authority

of a Member State that it submits it in the language of the Member State of the principal authority,

if this is different from the authority to which he submits his complaint. It follows that the four

complaints in question have been validly lodged with the DPA.

45

200. With regard to the lack of interest of Fundacja Panoptykon, as well as other

complainants, for complaints lodged through the European “one-stop shop” mechanism

unique", raised by the defendant, the Litigation Chamber notes that Fundacja

Panoptykon filed the complaint with the Polish Supervisory Authority on behalf of Ms.

Katarzyna Szymielewicz, in accordance with Article 80.1 GDPR. Based on this

provision, the complainant has the right to instruct Fundacja Panoptykon to file the complaint

in his name.

201. The Litigation Chamber notes that IAB Europe absolutely does not explain why

Fundacja Panoptykon should not be considered a plaintiff and a party

in this procedure. Moreover, in the absence of doubts about the admissibility of the other

complaints, the defendant's argument would make no difference as to the outcome of this

decision.

202. This argument must therefore be rejected.

b. The inspection report is not properly reasoned

203. The defendant then attacks the insufficient reasoning of the inspection report. In

due to the absence of a clearly formulated reason in the inspection report -

in particular the absence of a clearly identified data controller in

relationship to a clearly defined data processing activity - the defendant

argues that the inspection report not only violates APD's obligation to give reasons

expressly and sufficiently its decisions, but also constitutes a violation

manifesto of the rights of defense of IAB Europe. Therefore, the inspection report

infringes the rights of defense of IAB Europe as set out in Article 6 of

ECHR and Article 47 of the Charter of Fundamental Rights.

Position of the Litigation Chamber

204. IAB Europe's assertion that the Inspection Service report of 13 July

2020 is not motivated enough is incorrect. As also shown in the reflection

of that inspection report in this decision, the inspection report contains a

detailed reasoning.

205. Furthermore, IAB Europe ignores the fact that, in addition to the report of July 13, 2020, the Service

inspection produced other very complete and detailed technical reports (exhibits 24 and

53). Finally, the Litigation Chamber underlines the many written exchanges of views and

between the parties before her. IAB Europe's mere assertion of non-compliance with

its rights of defense is therefore unfounded, as set out in the

following paragraphs.

46

vs. Incompleteness and partiality of the inspection report

206. The defendant refers to Article 58.4 GDPR, which provides that the procedure before the DPA

must be carried out in compliance with “appropriate safeguards, including […] respect for the

legality”. According to the defendant, this principle applies both to the investigation carried out by the

Inspection service only to the findings in the inspection report.

207. Referring to the similarities with the role and duties of a prosecutor in a procedure

ordinary criminal law, the defendant asserts that the fundamental principles of loyalty,

impartiality and independence also apply to the Inspection Service. The

defendant refers to section IV of its pleadings and considers that elements to be

relevant discharge, of which the Inspection Service had or should have had knowledge, are

missing from the inspection report.

208. The defendant, emphasizing that the DPA is required to maintain the presumption of innocence

of a defendant at any time, including during the investigation phase of a proceeding

which may lead to criminal sanctions within the meaning of Article 6 of the ECHR, considers

that his presumption of innocence has been violated and that the claims against IAB Europe

must therefore be rejected.

Position of the Litigation Chamber

With regard to the autonomy of the Litigation Chamber in relation to the

other DPA bodies, including the Inspection Service

209. The Litigation Chamber notes first of all that the defendant seems to confuse the

role and prerogatives of the Litigation Chamber with those of the other DPA bodies.

210. As indicated above, the Litigation Chamber is the administrative body for resolution
DPA disputes, in accordance with Article 33(1) of the LCA. The provisions governing the
proceedings before the Litigation Chamber (see Articles 92 to 100 of the LCA)
not show that it is bound in any way by the conclusions of another
ODA body. Consequently, the Litigation Chamber is not bound by the
conclusions of the Inspection Service.

211.

It is also recalled that the Inspection Service presented not one but several
detailed and technical reports clearly exposing the deficiencies attributable to the
defendant and supporting its position with the help of legislative, jurisprudential and
factual, as the Complainants point out. The defendant had access to these reports.
Moreover, the defendant replied in detail to the reports of the Inspection Service.

212. Respondent further submits that the Inspection Service's report of July 13, 2020
would not be exonerating, but simply incriminating, because this report would not contain
“certain exculpatory material” from IAB Europe. The defendant also refers, without
further clarification, in section IV of its pleadings, in which it sets out its arguments

47

on the background. In the absence of more detailed information on the exculpatory evidence which
been omitted from the aforementioned report of the Inspection Service, this complaint must be dismissed.

213. The Litigation Chamber notes that even if we were to follow the argument of the
respondent, quod non, one could nevertheless conclude, as the Court has already indicated
des Marchés, that the procedure before the Litigation Chamber was not illegal in the
to the extent that both parties have had the opportunity to present their arguments in their
conclusions46. Given the complexity of the system, the Litigation Chamber did not
was able to specify every technical aspect of the system against which

charges were brought against the defendant at the start of the proceedings

before the Litigation Chamber, on October 13, 2020, that is to say when the parties

were invited to submit their conclusions (art. 98 LCA). However, in order to guarantee the

procedural rights of the parties, the Litigation Chamber ensured, on the one hand, that the

defendant has sufficient opportunities to present its arguments before it and,

on the other hand, that it remains within the framework of the initial complaints and reports of the Service

inspection, communicated to both parties before their written conclusions.

Regarding the legal framework for investigations by the Inspection Service

214.

It should also be remembered that the Inspection Service can carry out any investigation,

conduct any hearing and collect any information it deems useful in the context of its

missions in order to ensure compliance with the fundamental principles of the protection of

personal data47.

215. The Litigation Division also recalls that the intervention of the Inspection Service

in the procedure is to record findings and that he does not have the power

to impose penalties.

216. Contrary to what the defendant maintains, the Inspection Service is not a

administrative authority under criminal law within the meaning of Article 6 of the European Convention on

Human Rights (hereinafter: "ECHR"), because it has no power to sanction and its task is

limited to making findings and transmitting them to the Litigation Chamber within

his report. As indicated above48, the findings of the Inspection Service are not

only elements on which the Litigation Chamber bases its decision at a certain stage

later in the procedure. Nevertheless, the Litigation Chamber stresses that the investigation of the

Inspection service in this case was conducted impartially,

in accordance with the requirements of Article 6 of the ECHR and Article 47 of the Charter. She

46 Market Court, 2019/AR/741, June 12, 2019, p. 12, available on the APD website.

47 See Art. 64 of the APD law: "The Inspector General and the inspectors exercise the powers referred to in this chapter with a view to the control as provided for in Article 4, § 1, of this law. » See also art. 72(1) of the DPA law: “Without prejudice to the provisions of this chapter, the Inspector General and the inspectors may carry out any investigation, any control and any hearing, as well as collecting any information they deem useful in order to ensure that the principles fundamentals of the protection of personal data, within the framework of this law and the laws containing provisions relating to the protection of the processing of personal data, are effectively complied with. » (emphasis added).

48 See para. 209-210 of this decision.

opposes the defendant's suggestions insofar as they call into question the impartiality of the Inspection Service.

Regarding respect for the right to a fair trial, including the right to defense before the Litigation Chamber

217. The Litigation Division shares the defendant's opinion on the importance of applying the procedural guarantees relating to the respect of legality in the disputes referred to it. It is also established that these principles are actually applied before the Chamber. Litigation.

218. As explained above49, the defendant's complaint concerning the alleged lack of motivation and impartiality of the report of the Inspection Service, on which the defendant relies on finding a violation of its right to a fair trial, must be rejected.

219. For the sake of completeness, the Litigation Division also recalls that the Court of Marchés has already ruled that — in the event that the procedural safeguards in the phase prior to the proceedings were not assured, quod non — the parties have a adequate recourse against the decisions of the administrative bodies, in particular by the possibility of an appeal before the Court of Markets50.

220. The Markets Court added that a lack of impartiality on the part of an authority

administrative procedure does not necessarily constitute a breach of Article 6.1 ECHR if a

judicial authority endowed with full powers of control, which itself respects the guarantees

of Article 6.1 ECHR, can review the decision in question.

221. According to the Court of Markets, a violation of the principle of impartiality of the administration to a

earlier stage does not necessarily entail a violation of the right to a fair trial

whether this violation can be repaired at a later stage. The possibility of appeal to

a court which respects the guarantees of Article 6 of the ECHR aims precisely to

allow for such corrections.

222. With specific regard to the Litigation Chamber, the Markets Court ruled

as following :

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

50 “The legislator has given the citizen a conclusive remedy against the behavior of administrative bodies (in

in this case the APD) by providing precisely for recourse to the market court", Court of Appeal of Brussels, section of the

Market Court, 19th Chamber A, Market Court Section, 2019/AR/741, 12 June 2019, p. 9.

51“A lack of objective or structural impartiality on the part of an administrative authority does not constitute

necessarily a violation of Article 6.1 of the ECHR if the decision of this authority can subsequently be reviewed

by a fully competent jurisdiction and which offers all the guarantees provided for in article 6.1. Consequently, a

violation of the principle of impartiality at an earlier stage does not necessarily entail a denial of the right to a trial

fairly if this violation can still be corrected at a later stage. The organization of an appeal to a body

which meets all the guarantees of Article 6 of the ECHR serves to make this appeal possible”, Court of Appeal of Brussels,

Markets Court Section, 19th Chamber A, Chamber of the Markets Court, 2019/AR/741, June 12, 2019, p. 10.

"[...] even in this case, this legal protection by the subject of law is not legally

enforceable only before a judge (who is part of the judiciary) [...]. The legal possibility

to bring an action/appeal before the Court of Markets aims to offer the litigant the

guarantee of Article 6.1 of the ECHR and, more particularly, the remedy provided for in Article 47 of

CDFUE [Charter of Fundamental Rights of the European Union]".52

223. Therefore, in the absence of impartiality on the part of the Litigation Division, quod non en

case, and insofar as the Court of Markets exercises judicial control

completeness of the decisions of the Litigation Chamber, it could not be concluded, ipso facto, to

a violation of the right to a fair trial in the proceedings.

224. For the sake of clarity and information, the Litigation Division notes that if the rights

of defense are part of the fundamental rights which constitute the legal order of

the Union and are enshrined in the Charter53, the fact remains that, as judged by the

CJEU, the different components of the right to a fair trial, including the rights of the

defence, are not absolute and that any restriction may be possible for a

grounds of general interest. This assessment must be made in concrete terms:

"However, the Court has already considered that fundamental rights, such as respect for

rights of defence, do not appear as absolute prerogatives, but can

include restrictions, provided that these effectively meet objectives

of general interest pursued by the measure in question and do not constitute, with regard to the aim

continued, a disproportionate and intolerable intervention which would harm the substance

even of the rights thus guaranteed (...) [...].

34. Furthermore, the question of whether the rights of the defense have been violated must be assessed

in the light of the specific circumstances of each case [...]"54.

A.9.2. - Violations of the fundamental rights and freedoms of IAB Europe with regard to the

general nature of the DPA procedure

has. Administrative sanctions and Articles 6 and 7 of the ECHR and Article 47 of the Bill of Rights

fundamentals of the European Union

225. The Respondent argues that the measures and fines that DPA is authorized to

tax under sections 100 and 101 of the LCA, read in conjunction with section 83

of the GDPR, must be qualified as penalties of a criminal nature within the meaning of the conventions

international human rights law such as the ECHR and the Charter of Human Rights

fundamental, given the very nature of the offenses and the nature and severity

sanctions that can be imposed on a party. Therefore, according to the

52 Brussels Court of Appeal, market court section, 2020/AR/329, 2 September 2020. The judgments of the Cour des

Contracts are available on the APD website in their original language (Dutch or French).

53 In this regard, see CJEU, 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, para. 98 and 99.

54 CJEU, 10 September 2013, C-383/13 PPU, Case G. and R., ECLI:EU:C:2013:533, para. 33 et seq.

respondent, Articles 6 and 7 of the ECHR and Article 47 of the Charter of Rights

fundamentals are applicable to the sanctions that the DPA may impose on IAB Europe.

226. The defendant then considers that the large margin between the minimum amount and the

maximum amount of administrative penalties of a criminal nature, which, in addition, according to the

defendant, places all offenses on an equal footing while failing to specify

the severity of the sanctions in the law itself, is contrary to the fundamental principles

substantive legality and proportionality. The same reasoning applies to articles

100 and 101 of the LCA, read in conjunction with Article 83 of the GDPR, which, due to their

imprecise and ambiguous wording, do not allow a party to assess in a manner

appropriate criminal consequences of a certain behavior before it occurs.

227. It would therefore follow that sections 100 and 101 of the LCA, read in conjunction with

Article 83 of the GDPR, would be contrary to the fundamental principles of substantive legality

and proportionality set out in Articles 6 and 7 of the ECHR and Article 47 of the Charter

fundamental rights. For these reasons, the defendant considers that Articles 100

and 101 of the LCA, read in conjunction with Article 83 of the GDPR, could not 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 terms of its application are provided for by Article 83 of the GDPR, with direct effect. In accordance with the case law of the Court of Markets, the Litigation Chamber considers that the administrative fines, as well as the other corrective measures provided for in Article 58 GDPR, constitute a powerful part of the enforcement tools available to the APD55.

229. If the DPA notices one or more infringements of the rules, it must determine the most appropriate corrective action to address this violation. Measures available for this purpose are listed in Article 58.2.b to 58.2.j of the GDPR. Especially, Article 58.2.i GDPR provides that the supervisory authority has the power, depending on the circumstances in each case, to impose, in addition to or instead of the measures referred to in this paragraph, a administrative fine in accordance with Article 83 GDPR. This means a fine administrative can be both a stand-alone (corrective) action and an action taken together with other corrective measures (and therefore constitutes a kind of measure additoinal). The criminal provisions of Articles 83.4 to 83.6 of the GDPR allow the imposition of an administrative fine for most offences. However, the supervisory authority is responsible for always choosing the most appropriate measure or measures appropriate56.

55 Brussels Court of Appeal, market court section, 2021/AR/320, 7 July 2021, p. 38.

56 Ibid.

230. In addition to the relevant provisions of the GDPR and the LCA on the level of fines administrative measures that the Litigation Chamber may impose, the Litigation Chamber is also based on the case law of the Court of Markets57, which formulates requirements on the foreseeability and motivation of the administrative fines imposed by the Litigation Chamber. This case law has, for example, led to a form

notification of the intention to impose a sanction is submitted to the party concerned, who may
react and send their comments to the Litigation Chamber before it takes a
decision. Accordingly, in these proceedings, this form has been sent and the
defendant submitted a reaction58.
231. The Litigation Division also refers to the case law of the Court of Markets,
which found that the GDPR does not provide for a specific fine range for
specific offences, but only an upper limit or maximum amount. In
practice, this means that the DPA can decide not only not to impose a fine
to the offender, but also that, if it decides to impose a fine, it will be
between the minimum, from 1 EUR, and the maximum provided. The fine is decided
by the DPA taking into account the criteria listed in Article 83(2) of the GDPR.59.
232. In addition, the Litigation Chamber also follows the guidelines of the Group of
work Article 29 on data protection concerning the application and fixing of
administrative fines under the GDPR, approved by the EDPB60, which detail the
criteria of Article 83(2) GDPR that a supervisory authority must apply when assessing
whether to impose a fine and the amount of the fine.
233. In addition, these guidelines also contain an explanation of Article 58 of the
GDPR relating to the measures that a supervisory authority may choose to take, being
given that the remedies are by nature different and essentially have different purposes
different. 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 Court of Markets, ruling in full jurisdiction, carries out a review of the legality and
proportionality of the sanction and will reduce or cancel (only) the fine in case of
serious and proven circumstances that the Litigation Division would not or would not take
enough into account.
235. In summary, this system sufficiently guarantees compliance with the legal principles

fundamentals stemming from Article 6 of the ECHR and Article 47 of the Charter.

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

58 See para. 272-273.

59 Brussels Court of Appeal, Market Court section, 2021/AR/320, 7 July 2021, p. 38.

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

Legal framework for administrative fines

Relevant provisions of the ACL

236. Under Article 100(1)(13) of the LCA, the Litigation Chamber has the power to impose administrative fines. The Litigation Chamber may decide to impose a administrative fine to the parties prosecuted according to the general procedures provided for in Article 83 GDPR.

237. Pursuant to section 103 of the ACL, if an offender has committed more than one offense by the same act, only the heaviest administrative fine of the offenses concerned applies. In the event of overlapping offences, the rates of the administrative fines add up without the total amount being able to exceed twice the highest amount amount of the fine applicable to the offenses committed.

Relevant provisions of the GDPR

238. Once an infringement of the Regulation has been established, on the basis of the assessment of the facts of the case, the competent supervisory authority should determine the corrective measures most appropriate to remedy the breach. The provisions of Article 58(2)(b)-(j)61 define the tools that supervisory authorities can use to remedy the non-compliance compliance with the rules by a controller or processor.

has. notify a data controller or processor of the fact that the operations

envisaged treatment are likely to violate the provisions of this

regulation;

b. call a controller or processor to order when the

processing operations have resulted in a breach of the provisions of this

regulation;

vs. order the controller or processor to comply with the

requests made by the data subject to exercise their rights in

application of this regulation;

d. order the controller or processor to put the

processing operations in accordance with

the provisions of this

settlement, where applicable, in a specific manner and within a specified period;

e. order the controller to communicate to the data subject

a personal data breach;

f.

impose a temporary or permanent limitation, including a ban, on the

treatment ;

61 Article 58(2)(a) provides that a warning may be issued. In other words, in the event that the

provision relates, a remedial sanction shall not be imposed.

53

g. order the rectification or erasure of personal data or the

restriction of processing pursuant to Articles 16, 17 and 18 GDPR and the

notification of these measures to the recipients to whom the personal data

personnel have been disclosed pursuant to Article 17(2) and

Article 19 GDPR;

h. revoke a certification or order the certification body to revoke

a certification issued pursuant to Articles 42 and 43 GDPR, or order□

the certification body not to issue certification if the requirements□

applicable to the certification are not or no longer satisfied;□

i.□

depending on the specific characteristics of each case, impose a fine□

administrative pursuant to Article 83 GDPR, in addition to or instead of the□

measures referred to in this paragraph; and□

d. order the suspension of data flows addressed to a recipient located in□

a third country or an international organisation.□

239. The power to impose an administrative fine is governed by Article 83 of the GDPR, which□

has:□

General conditions for imposing administrative fines□

1. Each supervisory authority shall ensure that administrative fines imposed pursuant to□

of this article for breaches of this Regulation referred to in paragraphs 4, 5 and 6□

are, in each case, effective, proportionate and dissuasive.□

2. Depending on the specific characteristics of each case, the administrative fines are□

imposed in addition to or instead of the measures referred to in point (2) of Article 58□

a) to h), and j). To decide whether to impose an administrative fine and to decide on the□

amount of the administrative fine, due account shall be taken, in each case, of□

of the following elements:□

has)□

the nature, gravity and duration of the breach, taking into account the nature, scope or□

the purpose of the processing concerned, as well as the number of data subjects□

affected and the level of damage they suffered;□

has)□

b)□

vs)□

d)□

e)□

f)□

g)□

h)□

whether the breach was committed willfully or negligently;□

any action taken by the controller or processor to mitigate the□

damage suffered by the persons concerned;□

the degree of responsibility of the controller or processor, account□

given the technical and organizational measures they have implemented pursuant to□

sections 25 and 32;□

any relevant breach previously committed by the controller or□

the subcontractor ;□

the degree of cooperation established with the supervisory authority with a view to remedying the□

violation and to mitigate any adverse effects;□

the categories of personal data affected by the breach;□

the manner in which the supervisory authority became aware of the breach, in particular whether,□

and the extent to which the controller or processor notified the□

breach ;□

where measures referred to in Article 58(2) have previously been□

ordered against the controller or processor concerned□

for the same purpose, compliance with these measures;□

54□

i)□

j)□

the application of codes of conduct approved pursuant to Article 40 or

certification mechanisms approved under Article 42; and

any other aggravating or mitigating circumstance applicable to the circumstances of

the species, such as the financial advantages obtained or the losses avoided, directly

or indirectly, as a result of the breach.

3. If a controller or processor willfully or negligently violates

several provisions of these rules, within the framework of the same operation of

processing or related processing operations, the total amount of the administrative fine

cannot exceed the amount set for the most serious violation.

4. Violations of the following provisions are subject, in accordance with paragraph 2,

administrative fines of up to EUR 10,000,000 or, in the case of

company, up to 2% of the total worldwide annual turnover of the preceding financial year, the

the highest amount being retained:

b)

the obligations incumbent on the controller and the processor under

articles 8, 11, 25 to 39, 42 and 43;

the obligations of the certification body under Articles 42 and 43;

the obligations incumbent on the body responsible for monitoring codes of conduct under

of Article 41, paragraph 4.

vs)

d)

5. Violations of the following provisions are subject, in accordance with paragraph 2,

administrative fines of up to EUR 20,000,000 or, in the case of

company, up to 4% of the total worldwide annual turnover of the preceding financial year, the

the highest amount being retained:

has)

the basic principles of processing, including the conditions applicable to the

consent under Articles 5, 6, 7 and 9;

the rights enjoyed by data subjects under Articles 12 to 22;

transfers of personal data to a recipient located in a country

third party or an international organization under Articles 44 to 49;

all obligations deriving from the law of the Member States adopted pursuant to the

chapter IX;

non-compliance with an injunction, a temporary or permanent restriction of processing

or the suspension of data flows ordered by the supervisory authority pursuant to

article 58, paragraph 2, or the fact of not granting the foreseen access, in violation of

Article 58, paragraph 1.

b)

vs)

d)

e)

6. Non-compliance with an injunction issued by the supervisory authority under Article 58,

paragraph 2, shall be subject, in accordance with paragraph 2 of this article, to fines

administrative costs of up to EUR 20,000,000 or, in the case of a company,

up to 4% of the total worldwide annual turnover of the preceding financial year, the amount

higher being retained.

7. Without prejudice to the powers of the supervisory authorities with regard to adoption

corrective measures pursuant to Article 58(2), each Member State may

establish the rules determining whether and to what extent administrative fines may

be imposed on public authorities and public bodies established in its territory.

8. The exercise by the supervisory authority of the powers conferred on it by this article is

subject to appropriate procedural safeguards in accordance with Union law and

law of the Member States, including an effective judicial remedy and a procedure

regular.

9. […]”

240. The reading of Article 83, paragraph 2, GDPR, points (a) to (k), as well as explanations

additional information contained in paragraphs 3 to 6 of the same provision, is sufficient to refute

55

the defendant's argument that the various offenses listed in article

83 GDPR are placed on an equal footing.

241. The various criteria for assessing the severity of sanctions are clearly

set out in Article 83 itself and in recitals 148 to 150 of the GDPR. Section 83.2

also specifies that an analysis must be made "according to the circumstances of

the species”.

242. The Litigation Division has already referred to the Guidelines on the application and

setting of administrative fines under the GDPR, approved by the EDPB. These lines

guidelines provide advice on the interpretation of the individual facts of the case at the

light of the criteria set out in Article 83.2 of the GDPR. The guidelines are binding on the House

Litigation as a body of the DPA, member of the EDPB.

243. In order to reinforce the application of the rules of the GDPR, recital 148 of the GDPR specifies that

Sanctions including administrative fines should be imposed for any

violation of the regulations, in addition to or instead of the appropriate measures imposed by

supervisory authorities under this Regulation. In the event of a minor violation or if

the fine that may be imposed constitutes a disproportionate burden on a

natural person, a call to order may be sent rather than a fine. It suits

however, to take due account of the nature, gravity and duration of the violation, the

intentional nature of the violation and of the measures taken to mitigate the damage suffered,

the degree of responsibility or any relevant breach previously committed, the

how the supervisory authority became aware of the breach, compliance with

measures ordered against the controller or processor,

application of a code of conduct, and any other aggravating or

mitigating. The application of sanctions, including administrative fines, should

subject to appropriate procedural safeguards in accordance with the general principles of

Union and Charter law, including the right to effective judicial protection

and due process.

244. Contrary to what the defendant maintains, the GDPR therefore does not impose an amount

minimum fine, but only maximum amounts which, depending on the infringements

committed, may amount to 2% or 4% of the turnover of a manager of

salary, i.e. 10,000,000 or 20,000,000 euros respectively. These amounts have a

dissuasive nature and it is up to the Litigation Chamber to modulate the amount of

the fine depending on 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 offenses listed in Article 83 GDPR are not dealt with

in the same way and that the various criteria for assessing the severity of

sanctions are clearly set out, the defendant's argument must be rejected

that the combined reading of Article 83 GDPR and Articles 100 and 101 of the LCA

56

violates the principles of legality and proportionality, and therefore Articles 6 and 7 ECHR and 47

of the Charter of Fundamental Rights of the European Union, because of its vagueness.

246. Article 83 GDPR is a provision with direct effect of an EU regulation and it is for

the Litigation Chamber to ensure the proper functioning of this regulation. It does not belong

not in the Litigation Chamber, as a body of a national administrative authority,

to rule on the possible illegality of this provision.

247. Furthermore, the Constitutional Court ruled in its judgment no. 25/2016 of 18 February 2016

(p24-28) that a single and wide margin for an administrative fine, allowing

the administrative authority to adapt the administrative fine to the seriousness of the offence,

does not violate the principle of legality:

“B.18.2.

“B.18.2. Furthermore, the principle of legality in criminal matters which derives from the provisions

above-mentioned constitutional and conventional rules stem from the idea that criminal law must be

formulated in terms that allow everyone to know, when adopting a

behavior, whether or not it is punishable and, if so, to know the penalty

incurred. (…)

However, the principle of legality in criminal matters does not prevent the law from attributing a

discretion of the judge. It is indeed necessary to take into account the character of generality of the

laws, the diversity of the situations to which they apply and the evolution of

behaviors they suppress.

Similarly, in order to determine whether the ranges of sentences adopted by the legislator

schedule are so broad that they would disregard the principle of predictability of the

penalty, it is necessary to take into account the specificities of the offenses to which these penalties

relate. (…)

B.20.1. The assessment of the seriousness of an offense and the severity with which

the offense can be punished is within the discretion of the competent legislator. he can

impose particularly heavy penalties in matters where the offenses are of

likely to seriously undermine the fundamental rights of individuals and the interests of

the community. It is therefore up to the competent legislator to set the limits and

the amounts to

judge and that of

the discretion of the

inside which

administration must be exercised. The Court could only censure such a system if it were

patently unreasonable.

B.20.2. The ordinance legislator cannot be criticized for having wanted to rationalize

and simplify the environmental criminal law in force in the Region. In order to achieve this

objective, he was able to provide for a single and sufficiently wide range of sentences, both in terms of

with regard to criminal sanctions than alternative administrative fines, in order to

allow the judge or the administrative authority to adapt the penalty or the administrative fine

alternative to the seriousness of the offence.

57

B.20.3. With specific regard to the offense of exceeding the standards of

noise set by the Government, the contested provisions are aimed at litigants

professionals who can assess with sufficient precision the seriousness of the offense

they commit and the correlative importance of the sanction to which they expose themselves. By

elsewhere, the choice of the sanction must be justified, either by the judge, or by the authority

administration. In the latter case, a judicial appeal is open against the decision.

B.20.4. It follows from the foregoing that the contested provisions do not attribute to the judge or

to the administrative authority a power of appreciation which would exceed the limits of what is admitted

the principle of foreseeability of the sentence. »

248. The defendant's argument that Articles 100 and 101

of the LCA, read together with Article 83 of the GDPR, which form the basis of the

power of the Litigation Chamber to impose administrative sanctions and

fines, violate the principles of legality and proportionality and, therefore, the right to a

fair trial.

b. The rules of procedure of the DPA would not respect the fundamental principle of legality

formal criminal penalties, 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 offenses punished, the nature
and at the level of the sanction, as well as the procedure guaranteeing the safeguard of the rights of
defence, be fixed by the House of Representatives according to the legislative procedure
provided for by the Belgian Constitution.

250. Since this principle applies not only to penal sanctions stricto sensu, but also to
administrative sanctions of a criminal nature, it would be fully applicable to the procedure of
ODA penalty.

251. In this respect, the defendant claims that several aspects of the sanction procedure of
ODA are not fixed in a legislative text - in particular, not in the LCA, but
in the internal rules of January 15, 2019 (ROI).

252. Accordingly, the Respondent considers that these proceedings were conducted on the basis of
basis of rules of procedure contrary to Articles 12 and 14 of the Belgian Constitution and
that it is therefore devoid of a valid legal basis, so that the complaints against IAB
Europe should be rejected.

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 the sanction and the related procedural guarantees, must be
determined by the legislator.

254. The Litigation Chamber notes that the only elements relating to the imposition of a
sanction which does not appear in the GDPR, nor in the LCA, nor in the law of July 30, 2018, but
in the Rules of Procedure (ROI) of the APD to which the defendant refers, are not
in no way essential elements for the imposition of fines. In fact, it is not the
nature of the fine, nor the penalty, which are in question, but elements of a
secondary or organizational, for example as to the procedure to be followed in the absence of the
president of the Litigation Chamber (article 44 ROI), or the number of members sitting

per case (article 43 ROI).

255. The Litigation Chamber also emphasizes that the independence of a supervisory authority

control pursuant to Article 51 et seq. of the GDPR means that the organization of its

process, 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 relevant national legislation.

256. The defendant's argument that the proceedings before the Litigation Chamber

would violate the principle of legality is therefore rejected.

vs. Appointment of DPA members would violate GDPR Article 53

257. The defendant claims that Article 39 of the LCA, which regulates the appointment of members of

the Litigation Chamber, in no way specifies the terms of the procedure for

nomination. In particular, it does not specify anywhere how the interviewing of candidates should be

take place, and data protection law does not require a written record of

the hearing. Furthermore, the appointment takes place on the basis of a secret ballot and there is no

guarantee as to the adequacy of the information on the candidates provided to the members of

representatives room.

258. According to the Respondent, the appointment of members of the APD, including members of the

Litigation Chamber, would therefore not meet the requirements of Article 53 GDPR, which

provides that the appointment must be made "through a transparent procedure".

259. In view of the foregoing, the Respondent considers that the members of the Chamber

Litigation would not be able to make a legally valid decision to

towards IAB Europe in this matter. For these reasons too, the claims against

IAB Europe should be rejected.

Position of the Litigation Chamber

260. First of all, the Litigation Chamber recalls that any imperfections in the

procedure for appointing DPA members cannot be part of this procedure

and that the parties cannot invoke a procedural interest to challenge the

designation procedure.

59

261. The Litigation Chamber recalls that the members of the Litigation Chamber are

appointed by the House of Representatives and cannot be removed from office

only by this one. Thus, neither the Litigation Division nor the Market Court are

competent to decide on their appointment. Furthermore, the parties have no interest in

request such a decision.

262. Consequently, the Litigation Chamber finds that this allegation is unfounded.

d. The DPA's handling of this procedure would not be in accordance with its obligations and

its powers under Article 57 of the GDPR.

263. In conclusion, the defendant indicates, both in its initial conclusion and in the context of

the reopening of the proceedings, that the way in which the DPA, in addition to the initial complaint, examines

also the additional complaints and grievances formulated by the complainants, without the

relevance of these additional allegations has been examined by the Inspection Service,

makes defending 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 such as

defined in Article 57 of the GDPR, but also has the effect that IAB Europe is not required to

defend only against the allegations contained in the inspection report, and not against

subsequent allegations made by

the complainants in

their presentations

subsequent arguments.

Position of the Litigation Chamber

265. The Litigation Division firstly emphasizes that at no time did the defendant

explained what new allegations are the subject of his defenses and

would thus violate his rights of defence. For this reason alone, the Litigation Chamber

considers itself justified in declaring the defendant's argument unfounded.

266. Secondly, the Litigation Chamber notes that the LCA in no way prescribes that the

Litigation Chamber would be bound by an investigation report following a requested investigation

to the Inspection Service. Indeed, it does not follow from any provision of the LCA that the Chamber

Litigation would be deprived of

the possibility of taking into account elements

additional or complementary to the report of the Inspection Service, provided that

investigation and consideration of these additional elements are sufficiently

justified in the decision and that the rights of the defense are sufficiently guaranteed.

267. The Inspection Service may in any case decide not to investigate certain

disputed points, in accordance with the prerogative conferred on it by article 64 (2) of the LCA. In

such a case, it would however be contrary to Article 57 GDPR as well as to the autonomy and

the independence of the Litigation Chamber, as implemented by articles 92

to 100 of the LCA, to purely and simply bind the Litigation Chamber by the

60

conclusions of the Inspection Service, without taking into account the elements put forward in the

debates by the parties during the proceedings and in accordance with the right to be heard.

268. Thirdly, the Litigation Chamber decides that the alleged obligation to found the

debates on the sole inspection report following an investigation by the Inspection Service is not

not applicable. The LCA does not provide anywhere that the Litigation Chamber should base its

decision solely on the inspection report or on the conclusions of the parties. He

agrees that a supervisory authority also consults other bodies and sources in order to

to be able to support its decisions if necessary.

269. As for

the assessment of the Inspection Service with a view to an investigation

complementary, and in particular the nature of the time limits provided for in Article 96 of the LCA, the

Chambre Litigation is not convinced by

the arguments put forward by

the

defendant. In this case, the parties have had ample opportunity to make known their

point of view to the Litigation Chamber and to the opposing party concerning the allegations and

the charges, including the operation of the TCF, the processing of preferences and

user permissions in the TC String, as well as the interrelation between the TCF and

the OpenRTB.

270. Furthermore, the Litigation Chamber considers that there is no doubt about the crucial importance

of the TC String for the operation of the TCF. Therefore, the defendant could

expect, from the beginning of the procedure, that the debates focus on the

data processing within the framework of the TC String. Thus, there can be no question

new allegations - insofar as they exist, given the absence of examples

with which the defendant supported its argument - in the conclusions of the

plaintiffs, since they constitute an explanation of the operation of the TCF, of which it is not

not disputed that it is at the heart of the complaints against IAB Europe.

271. In view of the foregoing, the Litigation Division finds that this means 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 concerned, as usual steps within the framework

of a decision. If the Litigation Chamber proposes, after deliberation, to impose a

(punitive) sanction, the Court of Markets requires that the Litigation Chamber give the

defendant the advisability of responding to the envisaged sanctions, by means of a

standard form also covering the offenses retained and the criteria for

determination of the amount of the fine. This possibility of contradictory, or right to be

of course, concerns only the sanctions proposed and is therefore only communicated to the

respondent.

61

273. A sanction form was sent on October 11, 2021 to the Respondent, informing this

last of its breaches of the GDPR as well as the intention of the Litigation Chamber

to impose corrective measures and an administrative fine. IAB Europe submitted its

answer

on November 1, 2021. The defendant contests

the calculation of

the fine

administrative, asserting that the Litigation Chamber did not take into account all the

elements relevant to determining the amount of the administrative fine pursuant to

article 83.2 GDPR. Furthermore, the defendant contests the Chamber's taking into account

Interactive Advertising Bureau Inc. Total Worldwide Annual Revenue Litigation

(IAB Inc.) for the calculation of the administrative fine, since the latter has no

participation in the defendant nor any right of inspection on the deployment of the activities

from IAB Europe. The defendant specifies that IAB Europe obtains the license of the brand name

"IAB" with the IAB Inc. and that the various IAB organizations in Europe are

separate and distinct organizations.

274. On November 8, 2021, the plaintiffs submitted a request to the Litigation Chamber,

requesting to receive a copy of the sanction form as well as the reaction of the

defendant, based on the erroneous assumption that the defendant also received

additional information on the Litigation Chamber's draft decision. The

Chambre Litigation responds on November 9, 2021 that it will not disclose the form
sanction to complainants. Notification of the penalty form to the defendant takes place
within the framework of an objective control of legality and with the specific aim of respecting the rights
of the defendant's defence, in accordance with the case law of the Court of Markets. the
defendant is thus informed in advance of the nature and severity of the sanction that he risks
and has the opportunity to submit its final conclusions on this point to the Chamber
Litigation. Notification of the sanction form to complainants could not
contribute to the same objective, since the envisaged sanction would only be imposed on the
defendant, and not to the plaintiffs, and would therefore not directly affect the interests of those
last. Neither the rights of defense nor any other rule of law require that
complainants can present additional conclusions in relation to the sanction
which the defendant is likely to be inflicted.

275. On 23 November 2021, the Litigation Chamber submitted its draft decision to the other
supervisory authorities concerned (hereinafter, "CSAs"), as provided for in Article 60.3 of the
GDPR.

276. On December 18, 2021, the Litigation Chamber received a letter from the complainants in response
the decision of the Litigation Division not to disclose the content of the application form
sanction to complainants. Specifically, the Complainants argued that they should be
informed if the defendant has brought new elements to the proceedings. Bedroom
Litigation notes that the debates were already closed at that time, and that the reaction
of the defendant in the penalty form only related to elements concerning the
sanction.

277. On December 20, 2021, the Litigation Chamber is informed by the information system
on the Internal Market (IMI) of a relevant and reasoned objection (RRO) submitted by
the Dutch Authority (Autoriteit Persoonsgegevens, “AP”). The objection relates to

the absence of reasoning from the Litigation Chamber concerning the assertion of the NGO
Dutch Bits of Freedom that the TCF makes it impossible to exercise their rights
by the persons concerned. The Litigation Division addressed this objection in its
revised draft decision62.

278. On December 21, 2021, the defendant submits a letter to the Litigation Chamber,
requesting the suspension of the provisional execution of the decision, that the DPA does not return the
public decision until all remedies have been exhausted, and the DPA abstains
any public communication about the decision prior to such final decision. Once
again, the Litigation Chamber notes that the debates were already closed at that time.

279. On December 21, 2021, the Litigation Chamber is notified of a relevant and
reasoned submitted by the Portuguese Authority (Comissão Nacional de Proteção de Dados,
“CNPD”). The objection relates to the absence of a sanction taken by the Litigation Chamber
with regard to the processing of TC Strings in the absence of a legal basis provided for in Article 6 GDPR.
The CNPD considers that the draft decision should require the defendant to erase
immediately of all personal data unlawfully collected to date. The
The Litigation Chamber addressed this objection in its revised draft decision63.

280. In addition to the two relevant and reasoned objections, the Litigation Division received
comments from other CSAs regarding co-responsibility established by the Chamber
Litigation, the use of legitimate interest for certain processing operations, the scope of
corrective measures, as well as the envisaged administrative fine and the relationship between IAB
Inc. and IAB Europe.

281. On January 13, 2022, the Litigation Chamber submitted its revised draft decision to the
other relevant supervisory authorities, as provided for in Article 60.5 of the GDPR.

282. On January 17, 2022, the Litigation Chamber notified the parties of the filing of the draft
revised decision and the deadline of January 27, 2022 for CSAs. She also clarified
that the written exchanges with counsel for the defendant, concerning the form of

sanction, did not include new arguments that would require reopening the

discussions with both parties. Consequently, and given that both these exchanges and the form of

penalty will be part of the administrative file, the Litigation Chamber rejected the

asks the complainants to have access to the sanction form and to the written exchanges which

followed with the defendant.

62 See para. 504-506

63 See para. 535.

63

283. On January 20, 2022, the Litigation Chamber received a letter from the complainants, in which

they reaffirm that they have the right to obtain a copy of the sanction form and exchanges

with the defendant, in order to verify for themselves that no new element

was raised by the latter. The complainants also argue that if the form of

sanction and subsequent exchanges will be part of the administrative file, and will therefore be

accessible in the event of an appeal, there is no reason not to grant them access during

the current procedure. The plaintiffs further claim, on the basis of a press release from

defendant's press dated November 5, 2021, which the Litigation Chamber has

agreed to approve a Code of Conduct submitted by the defendant 6 months after its

decision. The plaintiffs argue that this was not discussed during the

procedure, and therefore request access to all written exchanges with the defendant following

to the sanction sheet, as well as the reopening of the debates on the jurisdiction of the Chamber

Litigation to approve a code of conduct or validate an action plan.

284. On January 27, 2022, the Litigation Chamber acknowledged receipt of the letter from counsel for

complainants, and responded that their arguments will be considered in its

deliberation.

Position of the Litigation Chamber

285. The Litigation Division finds above all that it is not responsible and cannot be

held responsible for public statements made outside the proceedings by

either party concerned during deliberation on the merits by the Chamber

Litigation.

286. Second, the Court of Markets stated that plaintiffs have no say

in the determination of the sanctions imposed by the Litigation Chamber64. In this regard,

Article 58.2.d of the GDPR grants supervisory authorities the power to order a

controller or a subcontractor to put the processing operations into

compliance with the provisions of the GDPR, where applicable, in a manner and within a time

determined. This provision, read in conjunction with Article 100, § 1, 9° of the LCA, must

be interpreted in the sense that an action plan and the intrinsic monitoring of this action plan

by the DPA, should be considered as one of the sanctions that can be imposed on

a data controller or a processor. The action plan must therefore be

considered a remedy, in respect of which the Complainants have no

interest in asserting their case.

287. With regard to the Respondent's request not to publish the decision, the Chamber

Litigation recalls the significant impact of the case, given the large number of

64 Market Court, 1 December 2021, FOD Financiën c. GBA, no. 2021/AR/1044, para. 7.3.4: “It does (certainly) belong

not for a Complainant to interfere in any way with the appropriateness, much less with

the extent of a sanction. The complaint only relates (and can only relate) to an alleged infringement such that the

decision taken by the Litigation Chamber of the APD concerning the complaint - and possibly imposing a sanction on the

person concerned - can never be considered an ultra petita judgment from the point of view of the complaint. ”

64

people concerned and organizations involved. In addition, the Litigation Chamber

notes that the defendants' request was submitted after the closing of the hearings, and that the

defendant itself has already published on the case on November 5, 2021. In view of these

elements, the Litigation Chamber decides not to respond to the request of the

defendant dd. December 21, 2021 regarding the non-publication of the decision and

the absence of public communications on the decision before exhaustion of all

remedies.

B. Reasoning

B.1. - Processing of personal data in the context of Transparency and

Consent Framework

288. In this section, the Litigation Chamber examines the concept of personal data

personal as well as the question whether personal data exist in

the context of the Transparency and Consent Framework, designed and managed by IAB Europe65, and if

they are processed.

289. For a good understanding of this decision, the Litigation Chamber emphasizes that

the complainants indicated in their written submissions that they wished to limit themselves to

alleged violations of the GDPR in the processing of personal data "in

the TCF itself"67. The Litigation Chamber will therefore not rule on this

section on liability for processing operations that take place in the context of

of the OpenRTB protocol.

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

290. European data protection legislation, including the GDPR, has always been

adopted a broad view of personal data with the aim of ensuring a level

high level of data protection and to safeguard the fundamental rights and freedoms of

persons concerned. The broad interpretation of the concept of personal data

and the concept of processing, among others, is a key element of the Court's case-law

of justice68. The principle that personal data does not concern

only a natural person

identified, but also a natural person

identifiable, was already established in 1981 by the Council of Europe Convention for the

65 See heading B.1.1. – Presence of personal data in the TCF.

66 See heading B.1.2. - Processing of personal data in the TCF.

67 Plaintiffs' conclusions of February 18, 2021, p. 2: “in het TCF op zich”.

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.

65

protection of individuals with regard to the automatic processing of personal data

personal69.

291. The GDPR states unambiguously that any information relating to a natural person

identified or identifiable (“data subject”) constitutes personal data

personal. "Identifiable" should therefore be understood as the possibility of identifying a

natural person directly or indirectly by means of an identifier such as a name,

an identification number, location data, online identifier or one or more

several elements specific to the physical, physiological, genetic, psychic identity,

economic, cultural or social status of that natural person.

292. In addition, the GDPR provides that, in order to determine whether a natural person is identifiable, it is

account should be taken of all means which may reasonably be expected to

will be used either by the data controller or by any other person, to

identify the natural person directly or indirectly, such as techniques of

targeting71.

293. In determining whether it can reasonably be expected that the resources will be used

to identify the natural person, account should also be taken of all the

objective factors, such as the cost and time required for identification, taking into account

the technology available at the time of processing and technological developments72.

294. Recital 30 of the GDPR clarifies that natural persons may be linked to

online identifiers through their devices, applications, tools and protocols,

such as Internet Protocol (IP) addresses, cookie IDs or other

identifiers. These identifiers can leave traces which, in particular when they are

combined with unique identifiers and other information received by the servers,

can be used to create profiles of natural persons and to identify these persons.

295. The former Article 29 Working Party has already addressed the importance of a broad definition of

personal data, in particular the fact that a natural person can be

considered identifiable when it can be distinguished from other members of the

group and therefore treated differently.

296. This position is also adopted by the Court of Justice. It is case law

constant that the content of the information qualified as personal data

69 Article 2.a of the Convention of 28 January 1981 for the protection of individuals with regard to the automatic processing of

personal data, B.S., 30 December 1993 (Convention 108).

70 Article 4.1 GDPR

71 Recital 26 GDPR; the English text explicitly refers to "singling out" as one of the means

to identify a natural person. See also CJEU judgment C-582/14 of October 19, 2016, Patrick Breyer t.

Bundesrepublik Deutschland, ECLI:EU:C:2016:779, para. 46FR. ZUIDERVEEN BORGESIUS, “Singling out people without

knowing their names - Behavioral targeting, pseudonymous data, and the new Data Protection regulation”, Computer Law

& Security Review, vol. 32-2, 2016, p. 256-271.

72 Ibid.

73 WP136 - Opinion 4/2007 on the concept of personal data, p. 14; WP199 - Opinion 08.2012 providing a

further contribution to discussions on data protection reform, p. 5.

is not important74 and that the criterion of identifiability must be interpreted in a flexible manner.

As long as information, by reason of its content, purpose or effect,

can be linked to an identified or identifiable natural person by means

that can be reasonably implemented75, and this, that the information from

which the data subject can be identified are wholly owned by

the same data controller or in part by another entity, this information

should be considered as personal data.

297. Complainants argue in their reply submissions that the TC String is a string

of unique characters which is also written in a cookie as a unique identifier

and which is then stored on a user's device77. Furthermore, the plaintiffs consider

that IAB Europe collects additional information about users using the

TC String, including sensitive personal data within the meaning of Article 9 of the

GDPR78.

298. The defendant, on the other hand, refutes the allegations and asserts that the TC String does not contain

no personal data79 nor any

information directly or

indirectly linked to the “content taxonomy80”, which IAB Europe uses as a “language

common” to describe the content of a website81. Furthermore, the defendant considers that the

TC String does not constitute a unique identifier and is not designed for this purpose82.

299. Notwithstanding the foregoing, the defendant indicates that it must necessarily be possible

to link the TC String to a user, but provided that this link between the preferences

designed in the TC String and the user is not established until later, namely in the

framework of the OpenRTB, and is therefore not covered by the Transparency and Consent

Framework83.

300. Based on technical documentation from IAB Europe and the IAB Tech Lab on the

TCF protocol, the Inspection Service concludes that the TC String in itself does not identify

users or devices directly, because the elements that compose it only do

reflect technical information, whether or not an unidentified user has consented

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 See also CJEU judgment C-582/14 of 19 October 2016, Patrick Breyer t. Bundesrepublik Deutschland,

ECLI:EU:C:2016:779, para. 43; judgment of the CJEU C-434/16 of December 20, 2017, Nowak t. Privacy Commissioner

data, ECLI:EU:C:2017:994, para. 31: see also FR. ZUIDERVEEN BORGESIUS, “Singling out people without knowing their

names - Behavioral targeting, pseudonymous data, and the new Data Protection regulation”, Computer Law & Security

Review, vol. 32-2, 2016, p. 256-271; and FR. ZUIDERVEEN BORGESIUS, “The Breyer Case of the CJEU - IP Addresses and t

Personal Data Definition”, EDPL, 1/2017, p. 130-137.

77 Complainants' submissions of February 18, 2021, para. 25.

78 Submissions of the Complainants of February 18, 2021, para. 26.

79 Respondent's submissions of March 25, 2021, para. 48.

80 Respondent's submissions of March 25, 2021, para. 51.

81 https://iabtechlab.com/standards/content-taxonomy/

82 Respondent's submissions of March 25, 2021, para. 53.

83 Respondent's submissions of March 25, 2021, para. 54.

for purposes Y or Z, and whether adtech providers A and B may process the data to

personal character for the accepted purposes.

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

i.

ii.

iii.

iv.

v.

vi.

vii.

viii.□

ix.□

general metadata;□

a binary value for each of the processing purposes for which the□

consent can be given;□

a binary value for each of the processing purposes permitted by an interest□

legit ;□

a binary value for each of the adtech providers that can collect and□

process the personal data of the user on the basis of his□

consent ;□

a binary value for each of the adtech providers that can collect and□

process the user's personal data on the basis of an interest□

legit ;□

any restriction of processing;□

special opt-in features in relation to the processing purposes;□

a field dedicated to processing purposes that do not fall under the TCF but which are□

vendor-specific;□

consent to processing on legal bases that are not covered by the□

TCF.□

Position of the Litigation Chamber□

302. Although the Litigation Chamber understands that it has not been conclusively established□

than the TC String, due to the limited metadata and values it contains,□

itself allows direct identification of the user, the Litigation Chamber□

note that when the consent pop-up is accessed, via a script, from a server□

managed by the CMP84, this inevitably also processes the IP address of the user, which is□

explicitly classified as personal data within the meaning of the GDPR.□

303. Indeed, recital 30 of the GDPR indicates that natural persons may be linked
to online identifiers through their devices, applications, tools and
protocols, such as Internet Protocol (IP) addresses, cookie IDs or
other identifiers such as radio frequency identification tags. These
identifiers can leave traces which, especially when combined with
unique identifiers and other information received by servers, may be used to
create profiles of natural persons and to identify these persons.
304. As soon as a CMP stores or reads the TC String on a user's device through a cookie
euconsent-v2, consent or objection to processing for reasons of interest
84 Technical analysis report from the Inspection Service, January 6, 2020 (Exhibit 53), p. 58.

legitimate, 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-up85) and combine all
information relating to an identifiable person. The possibility of combining the TC String and
the IP address implies that it is information about an identifiable user86.
305. In addition, the identification of the user is possible by establishing a link with other
data that can be used by participating organizations within the framework of the TCF,
but also in the context of the OpenRTB protocol. In this regard, the Litigation Chamber
stresses that it is not a single party, but participating organizations
— CMPs and adtech providers—which, as discussed in more detail below87, are
obliged to communicate to the defendant, on simple request, the information
to identify users.
306. Consequently, the Litigation Chamber finds that the defendant has
reasonable means it may use against registered organizations that
participate in the TCF, and with which the defendant is able to directly identify

or indirectly the user behind a TC String.

307. The Litigation Division also understands that the TCF is intended for recording

each user's combination of preferences as a single string

in the TC String, in order to communicate these preferences to a large number of suppliers

adtech, and therefore inherently involves the recording of such data.

308. The Litigation Chamber has in fact noted, on the basis of the investigation reports of the

Inspection Service, that adtech providers as well as other participants within

the wider OpenRTB ecosystem read the signal contained in a TC String in order to

determine whether they have the required legal basis to process the personal data

personal data of a user, for the purposes to which the latter has consented88.

309. In this regard, the Litigation Division emphasizes that it is sufficient for certain information to be

used to individualize a natural person, to be able to talk about data to

personal character. Additionally, the purpose of the TC String, i.e. entering preferences

of a specific user, leads de facto to consider the TC String as data to

personal character.

85 See the examples in the technical analysis report of the Inspection Service, January 6, 2020 (exhibit 53), p. 99 and

following.

86 C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, “Consent Management Platforms Under the GDPR: Process

and/or Controllers? », in Privacy Technologies and Policy, APF 2021, LNCS, vol 12703, Springer, 2021, pp. 50-51. Bedroom

Contentious notes in this respect that, until this summer, if a "globally stored" TC String was chosen, the CMPs could

access the internet domain consensu.org managed by IAB Europe to check whether a consent with a global scope had been

given by the user, which involved disclosing the values of the TC String coupled with the users' IP addresses

to the CMPs, by IAB Europe. The defendant announced during the hearing that the functionality of the consents within

overall would be depreciated.

87 See paras. 358 and following of this decision.

88 Technical analysis report from the Inspection Service, January 6, 2020 (Exhibit 53), p. 75.

89 WP136 - Opinion 4/2007 on the concept of personal data, p. 14.

69

310. In other words, if the purpose of the processing is to isolate people, it can be assumed

that the controller or another party has or will have at its disposal the means

by which it can reasonably be expected that the data subject will be identified.

Claiming that people are not identifiable, when the purpose of the processing is

precisely to identify them would be a contradictio in terminis90.

311. In addition, the Litigation Division is of the opinion that the use of these preferences has

undoubted consequences on the rights and interests of the data subjects, since

these choices determine, among other things, which third parties will receive and process the data to

personal character of users within the framework of the OpenRTB91 protocol.

312. In view of the above findings and of the broad interpretation of the concept

of personal data, as confirmed by the case law of the Court of

justice92, the Litigation Chamber concludes that the user preferences contained

in a TC String do indeed constitute personal data, since these

preferences relate to an individualized and identifiable natural person.

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

313. The Inspection Service explains in its technical investigation reports that the TCF is based

necessarily on three fundamental elements:

i.

a fully customizable user interface that allows Consent

Management Platforms (CMP) registered with the TCF to obtain the consent of

the user, his possible objections to processing based on an interest

legitimate, and their preferences regarding the purposes of the processing as well as the

authorized adtech providers;

ii.

a□

list of global adtech providers which includes□

the partners□

approved by IAB Europe and specific information regarding their□

processing purposes and their respective legal bases; and□

iii.□

a standardized mechanism for requesting, recording and possibly sharing□

authorized adtech providers, consents, objections and□

preferences through a dedicated API, a standard format for storing□

partners/consents, and a standardized data structure for□

transfer the status of partners/consents94.□

90 WP136 - Opinion 4/2007 on the concept of personal data, p. 14.□

91 CJEU judgment C-434/16 of 20 December 2017, Nowak t. Data Protection Commissioner, para. 39.□

92 See para. 296 and following of this decision.□

93Judgment of the CJEU C-434/16 of December 20, 2017, Nowak t. Data Protection Commissioner, para. 34.□

94 API Consent Management Platform v2.0, August 2019 (Exhibit 34), p. 4; Service technical analysis report□

d'Inspection, January 6, 2020 (Exhibit 53), p. 58-59.□

70□

314. Complainants argue that the creation of the TC String corresponds to the generation□

automated a unique string of characters associated with a specific user, for□

which their data exchange preferences are entered following□

the intervention of a CMP registered with the TCF95.□

315. In addition, Complainants refer to the sharing of the TC String with CMPs and other□

TCF participants. Specifically, they argue that storing a TC String in□

a specific euconsent-v2 cookie, on a storage system chosen by the CMP or□

associated with the internet domain consensus.org managed by IAB Europe, also constitutes a□

handling user preferences.

316. The defendant, on the other hand, argues that there is no data processing at

personal character within the meaning of Article 4(2) of the GDPR in the context of the TCF, given its

view that the TC String as such cannot be considered as a

personal data.

Assessment by the Litigation Chamber

317. Firstly, the Litigation Division refers to the definition of data processing

of a personal nature as being any transaction or set of transactions

whether or not carried out using automated processes and applied to data or

sets of personal data, such as the collection, recording,

organization, structuring, storage, adaptation or modification, extraction,

the consultation, use, communication by transmission, dissemination or any other

form of provision,

reconciliation or

interconnection,

the

limitation,

erasure or destruction96.

318. The TCF provides a standardized approach for the collection and exchange of data across

personal character — i.e. consent, possible objections and

preferences — of well-defined users, already identified or at least identifiable, of a

purportedly GDPR-compliant manner. The fact that participating organizations can

directly identify data subjects with the help of additional data,

such as an IP address, from the TC String that captures these consents, objections and

preferences, not only means that the TC String can be considered a

personal data97, but also leads to participating organizations (suppliers

adtech), inevitably process personal data.

319. Given the link between the TCF and the OpenRTB protocol, the Litigation Chamber refers to the guidelines of the former Article 29 Working Party on advertising in online, in which the Task Force noted that online advertising methods

95 Submissions of the Complainants of February 18, 2021, para. 27.

96 Art. 4.2) GDPR.

97 See previous section B.1.1. – Presence of personal data in the TCF.

browsing behavior inherently involve the processing of data to personal nature, as such advertising involves the collection of IP addresses and the processing of unique identifiers, so that data subjects can be followed online even if their real name is not known98.

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

321. Consequently, the Litigation Division finds that there is indeed data processing of a personal nature within the meaning of Article 4.2 of the GDPR. This conclusion is also confirmed by taking into account the possibility that the TC String may at any time be linked to immediately identifiable information, whether or not provided by the person concerned.

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

322. IAB Europe declares that it is not a data controller or co-responsible for processing of personal data collected by organizations

participants in the framework of the TCF.

323. The Litigation Chamber considers, however, that this reasoning cannot be followed, and this,

for several reasons. First of all, it is appropriate to apply the broad interpretation by the Court

of justice of the notion of controller (B.2.1. - Broad interpretation of the notion

controller by the Court of Justice and the EDPB). The fact that IAB Europe has a

decisive influence on the objective (B.2.2. - Determination of the purposes of the processing of

personal data within the TCF) and the means (B.2.3. - Determination of the

means of processing personal data within the TCF) of the processing in

imposing mandatory TCF parameters must also be taken into account.

B.2.1. - Broad interpretation of the notion of controller by the Court of Justice

and the EDPB

324. The GDPR defines the "controller" as the entity which, alone or jointly

with others, determines the purposes and means of the processing of personal data

staff99. This definition must be understood in light of the legislative objective of

placing primary responsibility for the protection of personal data on

98 WP171 - Opinion 2/2010 on online behavioral advertising, 22 June 2010, p. 10, https://ec.europa.eu/justice/article-

29/documentation/opinion-recommendation/files/2010/wp171_nl.pdf.

99 Art. 4.7) GDPR.

the entity that actually exercises control over the processing of the data. That means

that account must be taken not only of the legal qualification, but also of the reality

effective100.

325. The EDPB clarified that the notion of controller refers to the influence of the

responsible for the treatment on the treatment, based on a decision-making power or

control over processing activities. This control can be based on

legal provisions, on an implied power or on the exercise of a de facto influence101. In

substance,

the determination of ends and means corresponds to deciding

respectively of the “why” and the “how” of the processing: for a given processing,

the controller is the actor who exercises such influence on the processing of

personal data, thus determining the reason for which the processing takes place

(i.e. "to what end"; or "for what purpose") and how this will be achieved

(i.e. what means will be used 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 organization103. Liability can also be

allocated on the basis of contractual arrangements between the parties concerned, although

these are not always decisive104, or on the basis of an assessment of the control

size of a party. The determination of means and ends can for example

result from a decisive influence on the processing, in particular on the reason for

which the processing is carried out in a certain way105.

327. In its “Jehovah’s Witnesses” judgment106, the Court of Justice gave a broad interpretation

to the notion of controller. This decision is relevant and applicable in the present case,

because it specifies that the definition of controller must be interpreted in a manner

wide, in order to ensure “effective and complete protection of the persons concerned”107,

and that it is not necessary to have access to the personal data concerned

to qualify as controller. The Litigation Chamber cites below

below the relevant recitals of the aforementioned judgment:

100 L.A. BYGRAVE & L. TOSONI, “Article 4(7). Controller" in The EU General Data Protection Regulation. A Commentary, Oxfo

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 Ibid., 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, par. 362-365.

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

106CJEU judgment of 10 July 2018, Tietosuojavaltuutettu and Jehovan todistajat - uskonnollinen yhdyskunta, C-25/17,

ECLI:EU:C:2018:551.

107 CJEU judgment of 13 May 2014, Google Spain SL c. Agencia Española de protección de Datos (AEPD) and others, C-131/

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.

108CJEU judgment of 10 July 2018, Tietosuojavaltuutettu and Jehovan todistajat - uskonnollinen yhdyskunta, C-25/17,

ECLI:EU:C:2018:551. EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021,

para. 45.

73

“65. As expressly provided for in Article 2(d) of Directive 95/46, the concept of '

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 notion therefore does not necessarily refer to a

single natural or legal person and may concern several actors participating in this

treatment, each of them must then be subject to the provisions applicable in

data protection

june 2018,

(see, to this effect, judgment of 5

Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, paragraph 29).

66. The purpose of this provision being to ensure, through a broad definition of the notion of

accountable", effective and complete protection of data subjects, the existence

of joint liability does not necessarily translate into joint liability.

equivalent, for the same processing of personal data, of the different

actors. On the contrary, these actors can be involved at different stages of this

treatment and according to different degrees, so that the level of responsibility of each

of them must be assessed taking into account all the relevant circumstances of the case

case (see, to this 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 this directive only allow to consider the determination of the purposes

and means of the processing must be carried out by means of written guidelines or

instructions from the controller.

68. On the other hand, a natural or legal person who influences, for his own purposes,

on the processing of personal data and thereby participates in the determination

of the purposes and means of this processing, can be considered to be responsible

processing, within the meaning of Article 2(d) of Directive 95/46.

69. In addition, the joint responsibility of several actors for the same processing, in

under this provision, does not presuppose that each of them has access to the data to be

personal character concerned (see, to this effect, judgment of 5 June 2018, Wirtschaftsakademie

Schleswig-Holstein, C 210/16, EU:C:2018:388, paragraph 38). »

328. It therefore clearly appears to the Litigation Division that the defendant should not

necessarily process the personal data concerned itself, nor be

able to grant itself any access to this data, so that IAB Europe can

be considered a data controller109 with respect to a system

for which the defendant also invoices an annual fee of 1,200 euros to the

participating organizations110.

the CJEU of 5

109 Stop

June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/

Wirtschaftsakademie Schleswig-Holstein GmbH, C-210/16, ECLI: EU:C:2017:796, para. 35; judgment of the CJEU of July 10

2018, Tietosuojavaltuutettu and Jehovan todistajat - uskonnollinen yhdyskunta, C-25/17, ECLI:EU:C:2018:551, para. 69.

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

74

329. In addition, the impact or consequences of certain activities on the rights and freedoms of

data subjects may also be taken into account in determining the

responsibility of an organization. If it appears that an organization plays a decisive role in

the dissemination of personal data111 or that the processing operations

performed under the influence of this organization may substantially affect

fundamental rights to privacy and data protection

personnel112, this organization must be considered a data controller

Datas.

330. In this case, the Litigation Chamber concludes that the participating organisations, i.e.

say publishers and adtech providers, would not be able to reach the

objectives set by IAB Europe without the TCF. The system developed by IAB Europe therefore plays

a decisive role in the collection, processing and dissemination of preferences,

user consents and objections, regardless of whether the

defendant itself comes into contact with the aforementioned data.

B.2.2. - Determination of the purposes of the processing of personal data within

of the TCF

331. Determining the purposes of the processing is the first condition for identifying the

controller of personal data113. In addition, we consider

generally that the definition of the purposes of the processing takes precedence over that of the means

when it comes to establishing

responsibility of an organization. Incidentally, a

erroneous designation by a controller, such as a designation as

subcontractor contradicted by the factual situation, does not bind the jurisdiction or authority of

control115.

332. The Inspection Service specifies that the Transparency and Consent Framework in itself does not

does not constitute processing of personal data, but that it is a

set of Policies and technical specifications developed by IAB Europe and IAB Tech

Lab116. The Litigation Chamber agrees with the Inspection Service on this point.

111 Judgment of the CJEU of 13 May 2014, Google Spain SL c. Agencia Española de protección de Datos (AEPD) and others,

ECLI: EU:C:2014:317, para. 36.

112 Judgment of the CJEU of 13 May 2014, Google Spain SL c. Agencia Española de protección de Datos (AEPD) and others,

ECLI: EU:C:2014:317, para. 38.

113 Art. 4.7) GDPR; A. DELFORGE Title 8. The general obligations of the controller and the place of the subcontractor"

in The General Data Protection Regulation (RGPD/GDPR). In-depth analysis, Larcier, Brussels, 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 Title 8. The general obligations of the data controller and the place of the subcontractor" in Le

General Data Protection Regulation (RGPD/GDPR). In-depth analysis, Larcier, Brussels, 2018, para. 12.

115 C. de TERWANGNE, "Title 2. Key definitions and scope of the GDPR" in The General Protection Regulation

data (RGPD/GDPR). In-depth analysis, Larcier, Brussels, 2018, para. 9-12.

116 Technical analysis report from the Inspection Service, January 6, 2020 (Exhibit 53), p. 9.

333. However, the Litigation Chamber also noted that data of a nature

personnel are processed within the framework of the TCF, more particularly the preferences of the

users, which CMPs register through a user interface and store using the

TC String. In order to allow a standardized approach within the TCF, IAB Europe makes

use of both policy documents and technical specifications:

▪ The TCF Policies consist of rules of participation that apply to the

publishers, consent management platforms (CMP) and other providers

adtech.

▪ The TCF technical specifications, which provide a technical protocol with

which participating organizations can immediately exchange status

information provided to users and the choices of the persons concerned.

These technical specifications are closely linked to the TCF policy (policies) in order to

provide the technical functionality required to make the standard operational

TCF.

334. The defendant states in its pleadings that the treatment of these preferences,

in accordance with the rules imposed by the TCF on participating organisations, continues

the objective of allowing both publishers of websites and applications (publishers) and

ad tech partners who support ad targeting, delivery and measurement

and content (adtech providers) to obtain consent from users, to disclose

in a transparent manner the purposes of their processing and to establish a legal basis

valid for the processing of personal data for the purpose of providing between

other digital advertising117. This objective is also reflected in the TCF

Policies118:

“ii. The objective of the framework is to help players in the online ecosystem meet certain

requirements of the “privacy and electronic communications” directive (and, by extension,

of its successor, the future “privacy and electronic communications” regulation) and of the

General Data Protection Regulation, by providing a means of informing

users, among other things, of the storage and/or access to information on their devices,

the fact that their personal data are processed, the purposes for which they are

are processed, companies seeking to process their personal data to

these purposes, giving users choice about it, and notifying third parties, among other things,

what information has been disclosed to users and what their choices are. »

335. It is also clear from the documentation compiled by the defendant that the objectives of the

TC String are determined by IAB Europe:

117 Defendant's Response, para. 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).

76

"The main purpose of a TC String is to encapsulate and encode all the information

disclosed to a user and the expression of his preferences for the treatment of his

personal data under the GDPR. Using a management platform

consents (CMP), the information is captured in a coded and compact string

transferable by HTTP. This chain is used to communicate information about

transparency and consent to the entities, or “vendors”, which process the data to be

personal character of a user. Vendors decode a TC String to determine

whether they have the necessary legal bases to process the personal data of a

user for their purposes. » 119

336. Although the Litigation Chamber emphasizes 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 personal data contained in a bid request

as part of the OpenRTB, she finds that the TCF is being offered for the purpose of promoting

indirectly the use of OpenRTB. With this in mind, IAB Europe, in its capacity as

Managing Organization, serves as a real hinge between the TCF and the OpenRTB, which, by

elsewhere, was developed by IAB Tech Lab.

337. In support of its position, the Litigation Division refers to the inventory of purposes conceivable, which the participating organizations can pursue within the framework of the TCF. For example, TCF Policies for CMPs, publishers and other vendors respectively stipulate a mandatory list 120 with fixed and predefined purposes121, special purposes122, functionalities123 as well as special functionalities defined by IAB Europe:

▪ Purpose 1 — Store and/or access information on a device

▪ Purpose 2 — Select base advertisements

▪ Purpose 3 — Create a personalized ads profile

▪ Purpose 4 — Select personalized advertisements

▪ Purpose 5 — Create a custom content profile

▪ Purpose 6 — Select personalized content

▪ Purpose 7 — Measure ad performance

119 Free translation, Chain of transparency and consent with supplier list and CMP formats v2.0, August 2019 (Exhibit 35), p. 8.

120 IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 26 and following.

121 The term “Purpose” refers to one of the purposes defined for the processing of data, including data to be personal character of users, by participants in the Framework, which are defined in the TCF Policies or Specifications.

122 The term “Special Purpose” means one of the purposes defined for the processing of data, including data to be processed personal character of the users, by the participants in the Framework, which are defined in the TCF Policies or the Specifications for which Suppliers declare a legal basis in the GVL and for which Suppliers do not have no choice given by a CMP.

123 "Feature" means any of the personal data processing features used by participants in the Framework that are defined in the TCF Policies or Specifications used in the pursuit of one or more several objectives for which the user does not have the choice separately from the choice offered concerning the objectives for

which they are used.

77

▪ Purpose 8 — Measure content performance

▪ Purpose 9 — Apply market research to generate information about

the audience

▪ Purpose 10 — Develop and improve products

▪ Special Purpose 1 — Provide security, prevent fraud and debug

▪ Special Purpose 2 — Technically deliver advertisements or content.

▪ Feature 1 — Match and combine offline data sources

line

▪ Feature 2 — Link different devices

▪ Feature 3 — Receive and use device characteristics sent

automatically for identification

▪ Special Feature 1 — Use precise geolocation data

▪ Special Feature 2 — Active analysis of device characteristics for

identification.

338. The Litigation Chamber concludes that the purpose of the TC String, and in the broader sense of the

treatment of the TC String within the TCF as described in the TCF Policies, has been established

by IAB Europe.

B.2.3. - Determination of the means of processing personal data within

of the TCF

339. Determining the means of processing is the second cornerstone of accountability

treatment. With regard to the means of processing, the EDPB makes a distinction

between "essential" means and "non-essential" means. The choice of means not

essentials can, in principle, be left to a subcontractor without the liability of

the entity that determined the purposes is reduced124.

340. The “essential means” are closely linked to the purpose and scope of the processing and
are by nature reserved for the controller. Examples of essential means
relate to the type of personal data processed (“what data is
treated?), the duration of the processing (“how long are they processed?”), the
categories of recipients (“who has access to it?”) and categories of data subjects
(“Which personal data is processed?”). The "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
which can be left to the discretion of the subcontractor125.

124 EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 39-41.

125 EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 40.

341.
It is established by the Litigation Chamber, and also confirmed by the defendant126, that
the Transparency and Consent Framework provides a framework of binding rules for
participating organizations in handling user preferences. The
TCF participants are expected to agree to the Transparency and
IAB Europe Consent Framework (hereafter referred to as “Terms and Conditions”) 127 for
register. In doing so, the Litigation Chamber finds that IAB Europe does not only
monitor compliance with specifications and TCF Policies, as Managing
Organization. The defendant also defines the rules applicable to the
treatment of TC Strings under the TCF, and it imposes these rules on organizations
participants.

342. In the following paragraphs, the Litigation Division will examine the extent to which
Essential ways of processing the TC String are actually determined by
IAB Europe.

343. Generation, modification and reading of the TC String — First, the TCF Technical
Specifications128, the IAB Europe Transparency and Consent Framework Implementation
Guidelines (hereinafter “TCF Implementation Guidelines”)129 as well as the TCF Policies130
describe how CMPs are required to seek approval from users, must
generate a single TC String and can store the value of the TC String.
344. In addition, CMPs are obliged to register with IAB Europe in order to be able to generate
a TC String131 and they must comply with the technical specifications, developed by
IAB Europe in cooperation with IAB Tech Lab, regarding API132 with which CMPs
can generate the TC String and through which adtech providers and publishers
are able to read the TC String133. These specifications also attest to the fact that
The CMP API plays a vital role in the TCF, as it provides a standardized way to
parties, such as the publisher or an ad tech vendor, to access the preferences of the
users, which are managed by the CMP134. The Litigation Chamber notes that the use
of this API is mandatory to communicate between CMPs and providers.
126 Respondent's submissions of March 25, 2021, para. 35.
127 IAB Europe Transparency and Consent Framework Terms and Conditions (“Terms and Conditions”) (Exhibit 33)
128 Chain of Transparency and Consent with Global Supplier and CMP List Formats v2.0, August
2019 (Exhibit 35).
129 IAB Europe Transparency and Consent Framework TCF Implementation Guidelines, August 2019 (Exhibit 36).
130 IAB Europe TCF Policies v2019-08-21.3 (Exhibit 32); IAB Europe TCF Policies v2019-04-02.2c (Exhibit 38).
131 Technical analysis report from the Inspection Service, January 6, 2020 (Exhibit 53), p. 76.
132 An API is a programming interface that allows an entity to "plug" into an application in order to
to exchange data. An API is open and offered by the owner of the program. APIs are used in various
areas of digital marketing to enable, for example, automated gateways for data exchange
between programs such as Adwords, AdExchange and an agency or supplier. They can also be
used by adtech vendors, agencies or software vendors to automate campaigns

advertisers.

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.

79

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

346. In this regard, the Litigation Division refers to the “Wirtschaftsakademie” judgment, in which the Court of Justice ruled that the entity responsible for defining, and a fortiori for imposing, the parameters of data processing, thus participates in the determination of the purposes and of the means of this treatment and must therefore be considered as the person responsible for the treatment135.

347. Storage location — In their written evidence, the plaintiffs argue that IAB Europe is responsible for the management of the Internet domain "consensu.org", to which return so-called “globally scoped” consent cookies136 and which as such allows CMPs to view and modify shared TC Strings between several websites or applications.

348. On the other hand, IAB Europe indicates in its conclusions that, although it recorded the consensus.org domain, there is no storage of the TC String on the IAB Europe servers to which this consensus.org domain links. Indeed, IAB Europe delegates a sub-domain of consensus.org to each registered CMP137, which stores the TC String on the user's device at using a euconsent-v2 cookie and associates it with the consensus.org domain. According the defendant, it is therefore only the CMP which generates and stores the TC String and the own CMP servers that have access to the TC String.

349. In order to establish the responsibility of IAB Europe in the processing of TC Strings, it is necessary to determine to what extent delegating a subdomain to a CMP by IAB Europe implies that the defendant establishes at the very least the means (and the possible purposes) of this processing.

350. The TCF technical specifications provide that sharing the TC String with the CMPs must be done in two ways: either by storing the TC String in a storage system chosen by the CMP, if it is a consent specific to a service138, either by storing the TC String in a shared consent cookie with global scope, associated with the domain Internet consensus.org of IAB Europe139.

the CJEU of 5

135 Stop

June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v.

Wirtschaftsakademie Schleswig-Holstein GmbH, C-210/16, ECLI: EU:C:2017:796, para. 39: “Under these conditions, there is re

to judge that the administrator of a fan page on Facebook, such as Wirtschaftsakademie, by defining parameters

depending, in particular, on its target audience and the objectives of managing or promoting its activities, participates in the determination of the purposes and means of the processing of personal data of visitors to its fan page”.

136 Which contain the TC Strings.

137It concerns more particularly the subdomain <name of the CMP>.mgr.consensu.org. For example, for Onetrust, it this is https://cookies.onetrust.mgr.consensu.org/.

138 Concretely, this means that the user's consent is only valid for the website visited, and for the purposes accepted and approved suppliers.

139 Chain of Transparency and Consent with Global Supplier and CMP List Formats v2.0, August 2019 (Exhibit 35).

351. On the basis of the technical reports and the statements of the parties at the hearing, the Chamber Litigation concludes that the specific consent to the service is established by means of a

euconsent-v2 first-party cookie, and is therefore stored exclusively on the device of
the user. In this first scenario, the euconsent-v2 cookie in question will therefore not be
linked to the domain consensus.org, nor to the subdomain delegated to the CMP by IAB Europe.
352. However, in exceptional cases where user consent applies
also to other websites, so-called consent cookies within reach
global, CMPs are required to store the corresponding TC String on the device of
the user by means of a third-party cookie, associated with the domain consensu.org.140 Only CMPs
are able to read TC Strings on user devices.
353. In this second scenario, each CMP is then assigned a separate subdomain,
assigned by IAB Europe by DNS delegation, where the consent cookie and the TC String
are associated with the main consensus.org domain and its subdomains. Concretely,
this means that the scope of the globally scoped consent cookie includes both
the consensus.org domain and subdomains delegated to CMPs.
354. According to the defendant, the global consent was applied only to an extent
Limited and IAB Europe ceased using and supporting it after the hearing. Bedroom
Litigation takes note of this, but emphasizes that this feature also demonstrates
that the responsibility of IAB Europe goes beyond the simple design of a framework.
355. The Litigation Division further considers that the defendant establishes the means of
process the TC String as well as the euconsent-v2 cookie, both for consents
specific to the service than for consents with a global scope. The fact that the TCF
does not impose a specific mechanism for storing user consent in
the browser but simply recommends CMPs to use a first-party cookie
does not preclude finding that the defendant provides a list of possible mechanisms
to link 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 in particular the manner

standardized whose different parties involved in the TCF can consult the

user preferences, objections and consents141:

140 Technical analysis report from the Inspection Service, January 6, 2020 (Exhibit 53), p. 79.

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

81

356. Categories of recipients of the TC String — The Litigation Chamber also judges

that IAB Europe determines with whom user preferences should be shared,

in particular by providing a list of adtech suppliers registered with the TCF,

entitled Global Vendors List (GVL)142, as well as a list of approved CMPs (Global CMP List)143.

357. Documentation from IAB Europe shows that publishers wishing to use the TCF

are obliged to collaborate with a CMP registered with TCF144. In addition, the TCF Implementation

Guidelines state that CMPs are required to obtain consent and

possible objections for all the purposes and partners selected by the publisher,

although this selection can be extended to all adtech providers included in the

GVL145.

358. TC String Retention Period — Finally, the two versions of the TCF Policies

explicitly provide that participating CMPs and adtech providers must

keep the consent or objection record, which is stored in the TC

String, as long as the processing is in progress, and they are required to put it on the

available to the Managing Organization, i.e. the defendant, upon simple request

of this one146:

8. Record Keeping

142https://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. 26 and following.

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

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

82

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. »

359. The Litigation Chamber therefore considers that IAB Europe is responsible for defining the
criteria for determining retention periods for TC Strings.

360. It follows from the above that, in addition to the purposes, it is IAB Europe which actually determines
the means to generate, store and share the TC String by which the preferences,
user objections and consent are handled. The following items are
determinants according to the Litigation Chamber:

i.

IAB Europe defines how CMPs can collect consent or

user objections, generate a unique TC String and store the value of the

TCString;

ii.

IAB Europe, in collaboration with IAB Tech Lab147 has developed the technical

specifications of the API with which adtech providers, among others, can

access in a standardized way to user preferences, managed by the

CMP;

iii.

IAB Europe determines the location and method of storing cookies from

consent, whether service-specific or global in scope;

iv.

IAB Europe maintains lists of registered CMPs and adtech providers and

therefore determines to which recipients the data relating to the TC String is

potentially communicated;

147 IAB Europe worked with the IAB Tech Lab to determine the framework rules policies. IAB Europe has also

entrusted Tech Lab with the development and hosting of technical implementations and specifications of the TCF,

because of their technological expertise.

83

v.

IAB Europe determines the criteria according to which the retention periods of TCs

Strings can be established, as well as how organizations

participating in the TCF must make these TC Strings available to the Managing

Organization, that is to say the defendant.

361. Based on the above explanations, the Litigation Chamber considers that the

defendant must be considered responsible for the processing of the data

personal character as to the registration of the signal of consent, objections

and user preferences by means of the TC String, in accordance with the TCF

Policies and technical specifications of the Transparency and Consent Framework.

B.3. - Joint responsibility of publishers, CMPs and adtech providers with respect to

concerns the means and purposes of the processing of personal data in the

context of TCF and OpenRTB

362. The liability of IAB Europe does not exclude that there are other data controllers

data implementing the TCF and based on the OpenRTB protocol, endorsing

their own responsibility or shared responsibility for processing operations

personal data they provide.

B.3.1. - Joint processing responsibility

363. Article 26.1 of the GDPR provides that joint liability exists when “two

or more controllers jointly determine the purposes and means

of treatment”. The Court of Justice of the EU has clarified that "the existence of liability

joint does not necessarily result in equivalent liability, for a

same processing of personal data, of the different actors. On the contrary,

these actors can be involved at different stages of this processing and according to different

degrees, so that the level of responsibility of each of them must be assessed

taking into account all the relevant circumstances of the case”.

364. Again, the EDPB explained that the assessment of joint controllership

should be based on a factual rather than a formal analysis of the concrete impact on

purposes and means of processing.

365. First of all, the Litigation Chamber emphasizes that the existence of identical decisions

is not necessary to speak of joint processing responsibility; it is enough

that the defined purposes are complementary to each other150. The EDPB emphasizes

148 CJEU Judgment of 10 July 2018, Tietosuojavaltuutettu and Jehovan todistajat - uskonnollinen yhdyskunta, C-25/17,

ECLI:EU:C:2018:551, para. 66 and CJEU Judgment of July 29, 2019, Fashion ID GmbH & Co. KG, C-40/17, ECLI:EU:C:2019:6

para. 70.

149 EDPB - Guidelines 07/2020 on the concepts of data 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, para. 105: “Notwithstanding

the fact that the precise uses of the data for commercial purposes are not necessarily the same, both the

also that joint participation in the definition of means and ends can

take the form of a common decision, but also result from different decisions but

convergence of two or more entities concerning the purposes and the essential means

of data processing.

366. Decisions can be considered convergent if they are

complementary and necessary to processing in a way that confers influence

tangible on the determination of the purposes and means of the processing. The question to

to ask is whether the intended processing of personal data would be

impossible without the participation of all parties, or more precisely, if the activities of

processing carried out by each party are inseparable and indivisible.

367. Both in its submissions and during the hearing, IAB Europe pointed out that the TCF and the

OpenRTB protocol are completely independent of each other, in the sense that even

without participation in the TCF, adtech providers can freely process data to

personal character in the context of OpenRTB. On the other hand, the plaintiffs have

always refers to the inherent interconnection between OpenRTB and TCF, that the

defendant itself confirms — according to

the plaintiffs — in

TCFs

Implementation Guidelines152.

368. The Litigation Chamber finds that the defendant's argument cannot be followed,

given that the defendant indicates on several occasions in its pleadings that the

raison d'être of the TCF is precisely to put the processing of data in character

staff based on the OpenRTB protocol, among others, in compliance with the

applicable regulations, including the GDPR and the ePrivacy Directive. Although the

The Litigation Chamber understands that the TCF can also be used by

publishers for other applications153, in collaboration or not with the CMPs, it is

also certain that the TCF was never intended to be a stand-alone ecosystem and

independent.

369. On the contrary, the Litigation Chamber notes that the Transparency and Consent Framework

includes TCF Policies and technical specifications which should enable

publishers of websites and applications (publishers) as well as adtech partners who

support targeting, delivery and measurement of advertising and content

(adtech providers), to transparently disclose their processing purposes,

to establish a legal basis for the processing of personal data for the

defendant in the main proceedings that Facebook Ireland appear overall to pursue the same purpose in a manner which

seems mutually quite complementary. In the absence of identity, there is therefore a unity of finality: there is a finality

commercial and advertising. »

151 EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 54.

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 The TCF can thus also be used for non-marketing purposes, for example to measure audience,

performance, etc

provision of digital advertising, and to obtain consent or identify

user objections.

370. Accordingly, the Litigation Division finds that the decisions translated by IAB Europe

in the provisions of the TCF Policies and the technical specifications of the TCF, on the one hand,

and the means and ends determined by the participating organizations regarding

the processing — whether or not within the framework of OpenRTB — of character data

personal users, on the other hand, should be seen as decisions

convergent155. IAB Europe provides an ecosystem where consent,

objections and preferences of users are collected and exchanged not to

own or self-preservation purposes, but to facilitate further processing by

third parties (namely: publishers and adtech providers).

371. Consequently, the Litigation Chamber judges that IAB Europe and the organizations

respective participants must be considered as data controllers

spouses with respect to the collection and subsequent dissemination of consent,

objections and preferences of users, as well as for the related processing of their

personal data, without the responsibility of the CMPs and the suppliers

adtech participants does not reduce that of IAB Europe.

has. Consent Management Platforms (CMP)

372. CMPs ensure the technical implementation of consent banners by

which data subjects indicate their choices regarding the processing of

their personal data.

373. More specifically, CMPs have the function of storing consent, objections and

user preferences in the TC String, then store that value as

a euconsent-v2 cookie in the browsers used to visit the website, and finally

provide an API to adtech vendors so they can access the values of

consent, objection and preference for each individual user156.

374. CMPs wishing to register for the IAB Europe TCF v2.0 are required to put in place

standardized processing purposes and functionalities in their user interface,

in order to collect and store the data subject's preferences in this regard157. They

must also respect the applicable legal principles, as defined in the

TCF v2.0 from IAB Europe.

375. The Litigation Chamber has already established that the TC String in itself does not allow

directly identify people or devices. However, once the TC

154 Respondent's submissions of March 25, 2021, para. 33.

155 See para. 365-366.

156 C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, “Consent Management Platforms Under the GDPR: Proces

and/or Controllers? », in Privacy Technologies and Policy, APF 2021, LNCS, vol 12703, Springer, 2021, pp. 50-51.

157 IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 9 and following.

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 under the

form of a euconsent-v2.158 cookie.

376. To provide a CMP interface to users, publishers must implement code

JavaScript CMP on their website. This code is then loaded directly from the server

CMP or through the delegated subdomain. Following this HTTP(S) request, the publisher's server

and the CMP server have access to the IP address of the user who visits the website and sees

the CMP159 interface.

377. Access to this IP address allows the 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 this same IP address. On this basis, the Chamber

Litigation concludes that CMPs are able to process a large amount of data

of a personal nature.

378. The Litigation Chamber assesses the extent to which the CMPs act as

processors or as (joint) controllers in paragraphs

following.

379. According to the defendant, and as provided for in its TCF Policies, CMPs are in principle

considered as subcontractors. The Litigation Chamber does not share this

point of view for the following reasons. The main task of CMPs is to develop and

to provide interfaces that can have a direct impact on the choice of people

concerned. CMPs therefore play a key role, not only in the context of the TCF, but

also with regard to the processing of personal data in the context of

the OpenRTB. They are therefore required to comply with the principles of data protection

set out in Article 5.1 of the GDPR (lawfulness, fairness and transparency of data processing

personal).

380. Although the TCF Policies prohibit CMPs from giving preference to certain

adtech vendors on the Global Vendors List, and that they are therefore in principle required to

introduce users to all TCF-registered vendors, unless instructed otherwise

publishers161, some authors note that a certain number of CMPs do not respect

this requirement. Either because CMPs require publishers to supply

pre-selected, or because they refuse them the possibility of derogating from the complete list

adtech providers, proposed by default162.

158 See paras. 302 and following 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 Ibid., p. 5.

160 IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 9 and following.

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: Proces

and/or Controllers? », in Privacy Technologies and Policy, APF 2021, LNCS, vol 12703, Springer, 2021, pp. 50-51.

87□

381. It should also be noted that the CMPs have a wide margin of appreciation with regard to□ relates to the interface they offer to users. Indeed, the TCF Policies do not impose□ only minimum interface requirements to participating CMPs163, with the consequence□ that in practice, the interfaces and compliance with the principles of fairness and transparency□ can vary greatly depending on the CMP with which website publishers and□ applications collaborate164.□

382. The above findings lead the Litigation Division to conclude that the CMPs□ play an important role and therefore bear a (joint) responsibility165 with regard to□ the purposes and means of processing users' personal data□ as part of the TCF and the OpenRTB protocol.□

383. The Litigation Division observes, however, that this conclusion does not mean for□ as much as all CMPs must systematically be considered as□ controllers jointly with IAB Europe and the publishers, or that the□ scope of this joint responsibility is limitless. As explained□ earlier in this decision166, the list of CMPs implementing the TCF is exhaustive167□ due to mandatory registration and approval process with IAB□ Europe, as Managing Organization. The Litigation Chamber finds that the□ joint responsibility for control is established with respect to, respectively:□

has.□

the publisher of the site or application,□

b.□

the specific CMP set up by the publisher and providing the TCF interface to□ users,□

vs.□

IAB Europe, as Managing Organization.□

In this respect, the Litigation Chamber emphasizes that appropriate agreements must be put in place between the various joint controllers, in accordance with the requirements under Article 26 of the GDPR.

384. CMPs are in principle required by TCF Policies — developed and administered by the defendant — to present by default in their interface all of the TCF-registered adtech providers. To the extent CMPs implement TCFs 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 therefore jointly responsible for the

163 IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 61 and following.

164 Technical analysis report from the Inspection Service, January 6, 2020 (Exhibit 53), p. 99-103.

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

166 See para. 102; 341; 344; 356-360; and 374 of this decision.

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

transmission of personal data, including certain data contained 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 data with regard to the recipients of the personal data. Insofar as the CMPs do not respect the instructions imposed on them, they are themselves themselves fully responsible168, in accordance with article 28.10 GDPR.

386. Finally, when CMPs determine

the

list of recipients in accordance with

instructions from the publishers, the Litigation Chamber finds that the publishers bear

primary responsibility for the transfer of personal data to

suppliers, without prejudice to the responsibility of IAB Europe, without which the global list

of participating adtech providers would not exist in the first place.

b. Publishers

387. Publishers generally act as data controllers in the context of

context of the TCF, as they are expected to decide whether or not to cooperate with a registered CMP,

and are also able to determine which suppliers are authorized to provide

advertising on their website or in their application. Additionally, publishers can

exercise control over the legal basis for a specific processing purpose, and they

may exclude certain processing purposes.

388. Bid requests are sent by supply-side platforms, or

SSP), in their capacity as representatives of publishers, to demand-side platforms

(demand-side platforms, or DSPs), which represent adtech providers. The format and the

content (or "attributes") of these bid requests are determined in accordance with the technical

specifications of the OpenRTB protocol, independent of the TCF.

389. As confirmed by the reports of the Inspection Service, IAB Europe does not participate in the

determining the attributes of a specific bid request. These are mainly the

website and app publishers who decide which attributes to include in a bid

request and forward to adtech vendors.

390. A bid request contains at least one unique identifier for each bid request (Bid ID) and

a unique identifier for the auctioned advertising space (Item ID). Additionally, a bid

request usually contains information about the user's device, details of

the user, the website or the application, and technical details about the advertising space

(Print)170.

168 EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 150.

169 IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 21-22.

170 Technical analysis report from the Inspection Service, June 4, 2019 (Exhibit 24), p. 12-13.

391. Based on the foregoing, the Litigation Division finds that the bid request contains the most personal data, and that this data is not processed by the defendant, but mainly by publishers, CMPs and the different adtech providers who are in principle all bound to respect the values of the TC String, in accordance with the TCF Policies.

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 the app user. The Litigation Chamber is of the opinion that this can be considered not only as additional proof that the TC String is indeed a personal data, since it is information relating to a person physically identifiable171, but also as proof that the preferences stored in the TC String have a direct and significant impact on subsequent processing activities.

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

394. Consistent with its previous findings regarding CMPs,172 the Chamber

Litigation believes that publishers also act as responsible for the

processing of user preferences in a TC String as well as their data

of a personal nature addressed in a bid request.

395. In addition, the Litigation Division refers to Article 23.5 of the TCF Policies, which prohibits

publishers to modify the purposes of the processing, or to give the CMPs any instructions to

this effect.

396. Therefore, to the extent that publishers decide not to deviate from the list of

adtech providers offered by default and accept all processing purposes

proposed, the Litigation Chamber also considers that IAB Europe acts as

joint data controller with the publishers with respect to the

recipients of the TC String as well as the processing purposes for which the data

personal data of users will be processed.

vs. adtech suppliers

397. The Litigation Chamber has already found that IAB Europe is responsible for the

definition of the different processing purposes within the framework of the TCF174.

171 See paras. 291 and following 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), p. 22-23.

174 See para. 331 et seq. of this decision.

398. When registering for TCF v2.0, adtech providers must also choose the

intended processing purposes and possible legal bases, starting from a list

fixed and predetermined goals.

399. In this sense, the Litigation Chamber finds that adtech suppliers as well as the

defendant are jointly responsible for the processing that takes place in the

context of OpenRTB, for processing purposes and in accordance with preferences,

objections and consents collected within the framework of the TCF. This last aspect does not affect

however, not the role that adtech providers play in specifying the

purposes for which they intend to process the personal data

contained in a bid request, or with respect to further processing of data not

provided by the TCF175.

400. In addition, the Litigation Chamber specifies that, as for the CMPs, the suppliers

adtech are also required to register for the TCF in order to benefit from it. This means that the

joint control liability is limited to registered adtech providers176.

d. Assessment by the Litigation Chamber

401. This evidence-based analysis of the role of CMPs, publishers and adtech providers shows

that decisions relating to the determination of the purposes and means of the activities of

processing carried out by the defendant within the framework of the TCF (aimed at

processing activities carried out by the aforementioned participating organizations in

compliance with the GDPR and the ePrivacy Directive) complement the decisions relating to

purposes and means of processing activities carried out by organizations

participants in the framework of OpenRTB and should therefore be considered

as convergent decisions.

402. This leads the Litigation Division to conclude that the defendant and the CMPs,

participating publishers and adtech providers should be considered as

joint controllers with regard to the collection and dissemination

preferences, objections and consent of users, as well as for the

further processing of their personal data.

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

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

403. With regard to the lawfulness and fairness of the processing, the Litigation Division distinguishes between

two processing activities: on the one hand,

the actual capture of the signal of

175 WP171 - Opinion 2.2010 on online behavioral advertising, p. 10-11.

176 https://iabeurope.eu/vendor-list-tcf-v2-0/.

consent, objections and preferences of users in the TC String by the

CMP (a), and, on the other hand, the collection and dissemination of personal data of

users by participating organizations (b).

has. Registration of the signal of consent, objections and preferences of the

users by means of the TC String.

404. The Litigation Chamber notes that users are nowhere informed of the

legal basis for CMPs to process their personal and individual preferences

regarding the purposes and authorized adtech providers.

405. The defendant's underlying reasoning in this respect is that the TC String is not

personal data and that, therefore, no legal basis is

required for its processing.

406. As already established,

the Litigation Chamber does not share

the position of

the

defendant177. The Litigation Chamber has established that the generation and dissemination of

TC String do involve the processing of personal data.178 By

Consequently, this processing must in any case be based on one of the bases

legal treatment limits listed in Article 6 of the GDPR. For this reason,

the Litigation Chamber will examine the question of whether one of the legal bases of

Article 6 GDPR can be applied.

407. First of all, the Litigation Chamber finds that neither the TCF Policies nor the TCF

Implementation Guidelines do not mention an obligation for CMPs to obtain the
unequivocal consent of users, before saving their preferences in
a TC String, which is placed on users' devices by means of a cookie
euconsent-v2. In addition, users are never informed of the processing of their
preferences in the form of a TC String, nor of the parties with which their preferences
are shared, or the retention period of their preferences. The consent of
visitors being never requested, article 6.1.a does not apply de facto as a basis
legal for this treatment.

408. Similarly, the Litigation Chamber emphasizes that Article 6.1.b is not prima facie
applicable to the processing of user preferences and the TC String. In the majority
cases, even in the existence of a contractual relationship between the users and the
publishers, the data processing concerned by the TCF would not meet
the requirement of objective necessity for the provision of online services by publishers

177 See above B.1.1. – Presence of personal data in the TCF".

178 See B.1.2 above. - Processing of personal data in the TCF.

to the users concerned (in particular with regard to processing for the purposes of
personalization of content and advertising based on browsing behavior)179.

409. In the absence of any contractual relationship between the data subjects and the CMPs or
IAB Europe, and in the absence of unambiguous consent given by users for
placement of a euconsent-v2 cookie, the Litigation Chamber must examine whether
legitimate interest passes the CJEU's triple test and, if so, whether it could be used as a basis
legal (6.1.f GDPR) for this preliminary processing of user preferences by
the CMPs, in accordance with the means and objectives as defined by IAB Europe in
its TCF Policies and TCF Implementation Guidelines.

410. In order to be able to invoke Article 6.1.f GDPR as a legal basis for the processing of

personal data, the legitimate interest of the controller (or third parties),

closely linked to the concept of the purpose of the processing (even if it remains distinct from it),

be weighed against the interests or fundamental rights and freedoms of individuals

concerned. While "purpose" refers to the specific reason why

data is processed — in other words, the purpose or intent of the processing of the

data — the notion of "interest" is linked to the broader interest that a data controller

processing may have in the processing, or for the benefit that the controller

— or even a third party, who does not necessarily have to be qualified as a joint controller

with regard to data processing — could withdraw from the processing180.

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 for a controller to be able to

validly rely on this legal basis, “namely, first, the pursuit of a

legitimate interest by the controller or by the third party(ies) to whom the data

are communicated, secondly, the need for the processing of personal data

personnel for the achievement of the legitimate interest pursued and, thirdly, the condition

that the fundamental rights and freedoms of the person concerned by the protection of

data do not prevail” (Rigas judgment181).

412. In order to be able to invoke the ground of lawfulness of “legitimate interest” under Article 6.1.f

of the GDPR, the controller must demonstrate, in other words, that:

1)

the interests he pursues with the processing can be recognized as

legitimate (“purpose” criterion);

179 EDPB - Guidelines 2/2019 on the processing of personal data pursuant to article 6, paragraph

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 situation is different from the case pending b

the Court of Justice C-446/21, Maximilian Schrems vs. Facebook Ireland Ltd.

180 CJEU judgment of 11 December 2019, TK v. Asociația de Proprietari block M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064, para. 44.

181CJEU 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. 28-31. See also Judgment of the CJEU of December 11, 2019, TK v. Asociația de Proprietari block M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064, para. 40.

93

2)

the envisaged processing is necessary for the realization of these interests (criterion of

" need ") ; and

3)

the balancing of these interests with the fundamental interests, freedoms and rights

of the data subjects leans in favor of the controller or a

third party (“balancing” criterion).

413. With regard to the first condition, the Litigation Chamber considers that

recording users' consent and preferences in order to ensure and

to be able to demonstrate that they validly consented or did not oppose the

processing of their personal data for advertising purposes, may be

considered to be carried out in a legitimate interest.

414. The interest pursued by the defendant as data controller

can, in accordance with recital 47 of the GDPR, be considered legitimate in itself.

In particular, the ability to store user preferences182 is a

essential element of the TCF and the Litigation Chamber notes that this is done in the interest

legitimate of the defendant as well as of the third parties concerned, such as adtech suppliers

attendees.

415. Therefore, the first condition set out in Article 6.1.f of the GDPR is met.

416. To fulfill 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 it is necessary to

ask if the same result can be obtained by other means, without treatment of

personal data or without processing that is unnecessarily burdensome for the

persons concerned.

417. Given the objective of enabling both publishers of websites or

applications and participating adtech providers to communicate the purposes of their

processing in a transparent manner, to establish a valid legal basis for the processing

personal data in order to provide digital advertising, and to collect

consent — or to identify whether an objection has, if any, been made to the

processing of data based on their legitimate interest183 —, the Litigation Chamber

must check whether the personal data included in the TC String are

limited to what is strictly necessary to register the consent, the

specific user's objections and preferences.

418. This second condition can also be fulfilled by respecting the principle of

data minimization (article 5.1.c of the GDPR). The Litigation Chamber notes that the

182 Including obtaining valid consent before processing personal data, or allowing data subjects to

users to object to processing based on Article 6.1.f GDPR at the time of collection of personal data

personal.

183 IAB Europe Transparency & Consent Framework - Policies, Version 2020-11-18.3.2a, p. 5, https://iabeurope.eu/iab-

europe-transparency-consent-framework-policies/

information processed in a TC String184 is limited to data strictly

necessary to achieve the desired objective. Furthermore, on the basis of the documents in the file and the

defenses of the parties, the Litigation Division was not able to establish

that the TC String is kept indefinitely.

419. In order to verify whether the third condition of Article 6.1.f of the GDPR — the criterion of “implementation

balance" between the interests of the controller, on the one hand, and the freedoms and rights
fundamentals of the person concerned, on the other hand — can be fulfilled, the expectations
reasonable grounds of the data subject must be taken into account in accordance with the
recital 47 of the GDPR. In particular, it should be assessed whether the data subject "can
reasonably expect, at the time and in the context of data collection, to
personal character, that they are processed for a given purpose.
420. This is also what the Court underlines in its judgment “Asociația de Proprietari bloc M5A-
ScaraA”186, in which she states:
“Also relevant for the purposes of this balancing are the reasonable expectations of the
data subject that his or her personal data will not be processed
where, in the circumstances of the case, that person cannot reasonably
expect further processing of these. »
421. In this regard, the Litigation Chamber finds it remarkable that no option is offered
users to completely object to the processing of their preferences in the
TCF framework. Whichever they choose, the CMP will generate a TC String before binding it to the
User Unique ID of the user, through a euconsent-v2 cookie placed on the user's device
the person concerned.
422. In addition, since users are not informed of the installation of a cookie
euconsent-v2 on their device, whether or not they agree with the purposes and
adtech suppliers proposed by the CMP, and that in addition 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 fulfilled.
423. The seriousness of the violation of the rights and freedoms of the data subject is also a
essential element of the assessment under Article 6.1.f GDPR. The result of this
assessment depends on the particular circumstances of the specific case concerned187. In this
context, it is appropriate, according to the Court of Justice, to take account in particular of "the nature

possibly sensitive of this data, as well as the nature and concrete methods

the data processing in question, in particular the number of people who have access

184 See para. 300 and 301 of this decision.

185 Recital 47 GDPR.

186 CJEU judgment of 11 December 2019, TK v. Asociația de Proprietari block M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064,

58.

187 Ibid., para. 56.

to this data and the methods of access to the latter"188. In this context, the House

Litigation highlights the large number of participating organizations that have access to the

TC String, as well as the reduced control of data subjects over the nature and scope

the processing of their personal data by these organisations.

424. In the absence of a valid legal basis, the Litigation Division judges that the processing

data under the TCF in its current format, whereby CMPs

store user preferences in a TC String, does not conform to

GDPR Article 6.

425. It is therefore undeniable for the Litigation Chamber that IAB Europe, as

Managing Organization of the TCF, did not provide a legal basis for the treatment of

user preferences in the form of a TC String and therefore violated Article 6 of the

GDPR.

b. Collection and dissemination of personal data under the RTB

426. It is undisputed by any of the parties that the TCF aims to capture, by means of the interfaces

presented by the CMPs, the users' consent or their lack of objection to the

legitimate interests of participating adtech providers.

427. For the record, the Litigation Division emphasizes that these two bases concern the

processing activities that take place within the framework of the RTB, in accordance with the protocol

OpenRTB.

428. However, the Litigation Chamber judges that none of the bases proposed and implemented

implemented by the TCF cannot be legally invoked by the participants of the TCF. All

first, the Litigation Chamber considers that the consent of the persons concerned

obtained through the CMP is not valid (i) and that the (pre)contractual necessity is not

not applicable (ii). In addition, the Litigation Chamber considers that the legitimate interest does not

does not meet the CJEU's triple test (iii). Article 6 of the GDPR is therefore infringed.

(i) - Consent is not a valid basis for processing operations

in the OpenRTB as facilitated by the TCF

429. In order to ensure that publishers and adtech providers comply with the requirements

more stringent transparency and consent requirements under the GDPR with respect to

regarding the processing of personal data in the context of

OpenRTB (or RTB in general), CMPs provide a relatively

standardized allowing users to consent or oppose the transfer of their

personal data to hundreds of third parties at once, for

specific purposes.

188 CJEU judgment of 11 December 2019, TK v. Asociația de Proprietari block M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064,

57.

96

430. Based on the documents in this case, the Litigation Chamber understands that the

participants can pursue one or more purposes among

the 12 purposes

standards that the TCF makes available to participating adtech providers, and which

are offered to users through the CMP189.

431. However, the CMP system poses problems at several levels, with

consequence that the consent obtained by these CMPs (through the TCF), for

the processing carried out within the framework of the OpenRTB, is not legally valid

with regard to article 7 GDPR.

432. In order to be able to be used as a legitimate legal basis, consent under

Article 7 of the GDPR must meet strict conditions. However, for the reasons

set out below, the Litigation Chamber considers that the consent obtained by

CMPs and publishers in the current version of the TCF is insufficiently free,

specific, informed and unambiguous.

433. First of all, the Litigation Division finds that the processing purposes proposed

are not described clearly enough, and in some cases are even

misleading190. By way of example, the Litigation Division finds that the purposes 8

("Measure content performance") and 9 ("Apply market research to generate audience

insights")191 provide little or no guidance on the scope of the processing, the nature of the

personal data processed, or the retention period of the data to be

personal character collected as long as the user does not withdraw his consent.

434. In addition, based on the documents in the file, the Litigation Division understands that

the CMP user interface does not provide an overview of data categories to

personal character collected, which makes it impossible for users to give their

informed consent.

435. The Litigation Division also notes that the TCF makes it particularly difficult for

users to obtain more information about the identity of all those responsible for the

data processing to which they give their consent to process their data

for certain purposes before obtaining their consent. In particular, recipients for

which consent is collected are so numerous that users would need

disproportionately long for

read these

information, which means

their

consent can rarely be sufficiently informed.

436. In addition, the information CMPs provide to users remains too

general to reflect the specific processing operations of each supplier

adtech, which prevents the necessary granularity of consent.

189 For an overview of these TCF objectives, see paragraph 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), p. 34-36.

97

437. In addition, the Litigation Chamber considers that the enrichment of the data contained

in a bid request, using personal data already in the possession of the

adtech providers and relevant CMPs, implies that users cannot

be adequately informed, since the TCF does not provide in its current format that

participating organizations

indicate which personal data they

hold or what processing operations they already carry out with this data.

438. Finally, the Litigation Chamber finds that the consent, once obtained by the

CMP, cannot be removed by users as easily as given, as required

yet Article 7 of the GDPR. First of all, the Litigation Chamber observes that under

of the TCF Policies, adtech providers are required to comply with the signals of

consent of a user in real time192, while no measures are put in place

to ensure that adtech providers cannot continue processing on the

based on a previously received consent signal. Moreover, the TCF does not provide

no proactive transmission of updated consent signals to providers

adtech. In addition, adtech providers can in principle no longer access the data

of a personal nature

the user concerned after the latter has withdrawn his

consent, which also means that they cannot identify the user for

which the consent has been withdrawn as such, with the consequence that the

adtech providers will continue to process the user's personal data

in question193.

439. Indeed, the Litigation Chamber understands that the CMPs are at the intersection between

users and participating adtech providers, who receive their data at

personal character and then process them for their own purposes. Such a setup

therefore means that withdrawal of consent through a CMP will only take effect upon

from the moment the relevant adtech provider consults the new values in

the TC String modified via the CMP API. In other words, the withdrawal of consent

is never immediate and therefore cannot be considered effective.

440. Consequently, the Litigation Chamber concludes that Article 6.1.a of the GDPR does not

not a valid legal basis for the processing and dissemination of personal data

personal within the framework of the OpenRTB, insofar as this consent would have been

obtained in accordance with the TCF in its current format.

(ii) - The legitimate interest of the participating organizations does not outweigh the

protection of the fundamental rights and freedoms of the persons concerned.

441. The question therefore is to what extent the organizations participating in both the

TCF and OpenRTB (adtech providers) can legitimately rely on article 6.1.f

192 IAB Europe Transparency & Consent Framework Policies v2020-11-18.3.2.a (Exhibit 32), p.14

193 For more information, see: M. VEALE, FR. ZUIDERVEEN BORGESIUS, “Adtech and Real-Time Bidding under European D

Protection Law”, German Law Journal, 31 July 2021, p. 26.

GDPR for predefined processing purposes implementing targeted advertising

or profiling of users, as opposed to non-marketing purposes, such

as audience measurement and performance measurement.

442. As indicated above194, the assessment of legitimate interests must be carried out based on the three-step approach established by the Court of Justice. This appreciation must be performed by data controllers prior to implementation processing based on Article 6.1.f GDPR, as they determine the means and the purposes of the personal data processing activities envisaged and are therefore the only ones in a position to put in place appropriate safeguards to avoid a disproportionate impact on the people concerned. In the case where several controllers are jointly responsible, the principles of accountability and transparency require that balancing is done jointly by all data controllers involved in the treatment.

443. As stated by the Article 29 Working Party, the consequences, both positive and negative effects must be taken into account to assess the impact of the treatment, which must be necessary and proportionate to the achievement of the legitimate interests pursued by the data controllers or by a third party. These consequences may include "decisions or possible measures that will be taken subsequently by third parties and situations where the processing may lead to the exclusion of certain persons, to a discrimination against them, defamation or, more generally, situations which entail a risk of harm to reputation, bargaining power or autonomy of the data subject."195

444. With regard to the purpose test, in particular the question of whether the interests

pursued by publishers and adtech providers through data processing

of a personal nature can be recognized as legitimate, the Litigation Chamber

understands that participating organizations have an interest in collecting and processing

personal data of users in order to be able to offer them advertisements

tailored.

445. Based on the case law of the Court of Justice and the guidelines of the EDPB, the

Litigation Chamber considers that the notion of legitimate interest can have a broad scope,

Being heard that

interest

invoked by a data controller must be

sufficiently specific, existing, current and not hypothetical196.

194 See para. 411 et seq.

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-CE (WP217), p. 37.

196 CJEU judgment of 11 December 2019, TK c. Asociația de Proprietari block M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064,

para. 44.

446. In this respect, the Litigation Division can only note that, firstly, the

proposed processing purposes are described in general terms, so that it is not

easy for users to assess the extent to which the collection, dissemination and

processing of their personal data is necessary for the purposes

envisaged, insofar as these are understandable for the users.

447. To be relevant, a legitimate interest must comply with European and national law

applicable, be sufficiently specific and formulated clearly so that an implementation

balance is permitted, and represent a real and current interest. Therefore, the mere fact

to invoke a legitimate interest in the processing of personal data is not

not enough ; the outcome of the balancing test will determine whether Article 6.1.f GDPR can
to be invoked.

448. The TCF Policies do not provide for an obligation for CMPs to explain in clear terms
users the legitimate interests at stake. Instead, the specific requirements for
the Framework UIs in relation to the legitimate interests contained in the TCF Policies198
only require CMPs to provide an information layer
secondary, allowing users:
has. to obtain information on the fact that personal data is
processed, as well as the nature of the personal data processed (for
example, unique identifiers, browsing data);
b. to obtain information on the scope of processing based on legitimate interest and
the scope of any objection to such processing;
vs. to access the parameters in the CMP interface in order to oppose the processing of
their personal data based on a legitimate interest;
d. examine the list of processing purposes, including their standard name and their
full standard description, as defined in Appendix A of the TCF Policies, and of
provide users with a mechanism to see which adtech providers are dealing with
their data for each of the purposes on the basis of a legitimate interest;
e. to exercise their right of opposition, either with respect to each adtech supplier whose
the processing is based on the legitimate interest, either, separately, for each
purpose pursued by adtech providers on the basis of a legitimate interest;
f. consult the list of names of adtech suppliers, as well as their objectives and
their legal bases, and to access a link to the privacy policy.
confidentiality of each adtech supplier.

449. By way of example, the Litigation Division refers to the definitions of the purpose of
processing 5 (Create a personalized content profile), in appendix A of TCF Policies 199:

197 Ibid., p. 25.

198 IAB Europe Transparency & Consent Framework Policies v2020-11-18.3.2.a, pp.67-68.

199 IAB Europe Transparency & Consent Framework Policies v2020-11-18.3.2.a, p. 32.

100

450. Notwithstanding that the TCF Policies state that they establish requirements

language, design and other elements in the interface

user framework (Framework UI), which are intended to align with legal requirements

European regulations on privacy and data protection, the

The Litigation Chamber also notes that the general rules and conditions for

Framework UI also 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

Stacks200 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 in the TCF to explain more to the persons concerned, to

clear and user-friendly manner, both the legitimate interests pursued as well as the reasons

200 Stacks are, in essence, a combination of different treatment goals.

101

for which they believe that their interests are not superseded by the interests or

fundamental rights and freedoms of data subjects.

452. Although, in the context of this case, the Litigation Division does not rule

not on the question of whether an economic interest202 can be considered as a

legitimate interest within the meaning of Article 6.1.f of the GDPR, it considers that the lack of

specificity of the declared purposes has the consequence that the first condition of a

specific lawful treatment is not fulfilled by means of standardized descriptions of

purposes of the processing and the interests pursued, as imposed by the TCF Policies.

453. As part of the necessity test, aimed at determining whether the envisaged processing is

necessary for the achievement of the interests pursued, it is necessary to ask whether the interests

legitimate interests pursued by the processing of the data could not reasonably be

equally effectively achieved by other means, resulting in interference

lesser in the fundamental rights and freedoms of the persons concerned, in particular

their right to respect for their private life and their right to the protection of personal data

personnel, as guaranteed by Articles 7 and 8 of the Charter203.

454. The Court of Justice has also specified that the condition of necessity of the processing must be

examined under the data minimization principle set out in Article 5.1.c of the

GDPR204. In other words, it is necessary according to the EDPB to examine whether other means,

less invasive, are available to achieve the same goal.

455. In this case, the Litigation Chamber understands that no guarantee is provided for

ensure that the personal data collected and disseminated is limited to

information strictly necessary for the intended purposes.205

456. In the absence of measures which adequately demonstrate that no personal data

inappropriate is broadcast, the Litigation Chamber is forced to judge that the

second condition is not fulfilled.

457. As regards the balancing test, in particular the question of whether the

interests pursued by adtech providers outweigh the freedoms and rights

fundamentals of the persons concerned, the reasonable expectations of the persons

201 Article 29 Working Party - Opinion 06.2014 on the concept of legitimate interests of the data controller

under article 7 of directive 95-46-CE (WP217), p. 47.

202 Contrary to the interest pursued by capturing user choices in a TC String, as analyzed in

para. 404 and following.

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 Ibid., para. 48.

205 In this regard, some authors claim that there are alternatives to the RTB, in which only information

minimums on the user are communicated. See M. VEALE, FR. ZUIDERVEEN BORGESIUS, “Adtech and Real-Time Bidding

under European Data Protection Law”, German Law Journal, 31 July 2021, p. 19 and following. The authors mention in

particular the Adnostic browser plug-in, developed ten years ago, which builds a profile based on the behavior of

user navigation in order to target advertisements, the information leaving the user's device is minimal and the

behavioral targeting taking place exclusively in the user's browser. In addition, the authors refer to the

Google's system called Federated Learning of Cohorts (FLoC) for micro-targeting in Chrome.

concerned should also be taken into account, in accordance with recital 47

of the GDPR, in addition to the circumstances specific to the particular case206.

458. The criterion of the seriousness of the violation 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 of the

GDPR207. In this context, according to the Court of Justice, account should be taken in particular

of “the nature of the personal data in question, in particular the nature

possibly sensitive of this data, as well as the nature and concrete methods

the data processing in question, in particular the number of people who have access

to this data and the methods of access to the latter208”.

459. Once again, the Litigation Chamber notes, firstly, that due to the large

number of TCF partners likely to receive their personal data,

the data subjects cannot reasonably expect the processing

resulting from this transfer. Added to this is the huge amount of data that,

in accordance with the preferences entered as part of the TCF, are collected through

of a bid request and transmitted to adtech suppliers as part of the protocol

OpenRTB209.

460. Furthermore, the EDPB indicates that the legitimate interest does not constitute a sufficient legal basis

in the context of direct marketing implementing behavioral advertising210.

Similarly, the ICO concluded in a recent report that legitimate interest is not a basis for

legality in the context of the RTB (despite this many publishers base their

processing on this legal basis)211. In summary, in view of the foregoing, the Chamber

Litigation judges that the third condition imposed by article 6.1.f GDPR and the

case law of the Court is not satisfied in this case.

461. In light of the above considerations, the Litigation Chamber considers that

the legitimate interest of the participating organizations cannot be considered as a

adequate legal basis for the processing activities carried out under the protocol

OpenRTB, in accordance with user preferences and choices entered into the

TCF framework.

206 CJEU judgment of 11 December 2019, TK v. Asociația de Proprietari block M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064,

para. 58.

207 Ibid., para. 56.

208 CJEU judgment of 11 December 2019, TK v. Asociația de Proprietari block M5A-ScaraA, C-708/18, ECLI:EU:C:2019:1064,

para. 57.

209 Norsk Forbrukerrådet - “Out of Control. How consumers are exploited by the advertising industry in

line”, 14 January 2020, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/, p.

36-37; see also Recommendation CM/Rec(2021)8 of the Committee of Ministers of the Council of Europe to the States

members on the protection of individuals with regard to the automatic processing of personal data in the

frame

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 the purposes of direct marketing, behavioral advertising,□

brokerage of data, location-based advertising or tracking-based digital market research”.□

211 Information Commissioner's Office - "Update report□

https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf□

into adtech and real time bidding”, 20□

june 2019,□

november□

profiling,□

from□

3□

103□

(iii) - Contractual necessity is not a valid basis for the processing of□

personal data in the context of TCF and OpenRTB□

462. In accordance with the guidelines of the EDPB, the Litigation Chamber notes that,□

generally, the (pre)contractual necessity of the processing is not a legal basis□

applicable to behavioral advertising.□

463. In addition, the Litigation Division notes that the current version of the TCF does not mention□

nowhere Article 6.1.b GDPR as a possible legal basis for the processing of□

personal data within the TCF and OpenRTB.□

464. On the basis of the foregoing, the Litigation Chamber therefore concludes that the□

processing of personal data within the framework of 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 violation of the principle of lawfulness and fairness.□

B.4.2. - Obligation of transparency towards the persons concerned (Articles 12, 13 and 14 of the GDPR)

465. Complainants raise the issue of the lack of transparency, and more particularly the fact that the OpenRTB ecosystem is so large that it is impossible for people concerned to give informed consent to the processing of their personal data personal, or to object in an informed manner to the processing of their personal data personal on the basis of a legitimate interest.

466. The defendant, for its part, asserts that the TCF offers a solution for collecting the valid consent of users, when applicable, in accordance with the requirements set out in the GDPR and the ePrivacy Directive213.

467. The Litigation Chamber considers that the information provided under the current format of the TCF to data subjects, although for the purposes of processing their data at personal character within the framework of the OpenRTB, do not meet the requirements of transparency provided for by the GDPR214.

468. First of all, the Litigation Chamber indicates that IAB Europe can, in certain cases, request the "records of consent" that CMPs are required to keep, in accordance with to the TCF Policies215, but fails to inform data subjects of this processing potential by IAB Europe.

212 EDPB - Guidelines 2/2019 on the processing of personal data under article 6, paragraph 1(b) GDPR in the context of the provision of online services to data subjects, v2.0, 8 October 2019, p. 14 et seq., https://edpb.europa.eu.

213 IAB Europe TCF Policies v2019-08-21.3 (Exhibit 32); IAB Europe TCF Policies v2019-04-02.2c (Exhibit 38).

214 See para. 433 and following of this decision.

215 IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 11, 14 and 19.

469. Secondly, the Litigation Chamber considers that the way in which the information is

provided to data subjects, which has been established by IAB Europe, does not comply with the requirement of a “transparent, comprehensible and easily accessible form”216. The former Article 29 Working Party sets out in its guidelines on the transparency that “The requirement that the provision of information to data subjects and that communications addressed to them are carried out in a “concise” manner. and transparent” means that data controllers should present the information/communications effectively and succinctly to avoid drowning of information to the persons concerned”217. In addition, data subjects must be able to determine the scope and consequences of the processing in advance and not be later surprised by other ways of using their personal data personal218.

470. The Litigation Chamber considers that the approach adopted so far does not meet the conditions of transparency and fairness required by the GDPR. Some of the purposes of treatment announced are in fact expressed in a way that is too generic for the data subjects are properly informed of the exact scope and nature processing of their personal data. This is particularly problematic for purposes that rely on the consent of individuals concerned, because the consent must be specific and sufficiently informed to be valid as a legal basis.

471. The Litigation Division also refers to the examples of CMP specified in the technical report of the Inspection Service, and notes that the interface offered to users does not allow, among other things, to identify in a simple and clear manner the purposes processing associated with the authorization of a particular adtech provider or to identify adtech providers who will process their data for a specific purpose221.

472. In this regard, the Litigation Division underlines that the large number of third parties, namely

adtech suppliers who will receive and process personal data where applicable

personal of the users from the bid request, according to the preferences they have

seized, is not compatible with the condition of sufficiently informed consent, nor

with the broader transparency obligation under the GDPR.

216 Art. 12.1 GDPR.

217 WP260 - GDPR Transparency Guidance, paragraph 8.

218 WP260 - GDPR Transparency Guidance, para. 10.

219 See para. 4333 of this decision for examples as well as paras. 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,

p.p. 163-185.

220 See para. 429-440 et seq. of this decision.

221 Technical analysis report from the Inspection Service, January 6, 2020 (Exhibit 53), p. 99 et seq.

105

473. On the basis of the foregoing elements, the Litigation Division must therefore judge that the

TCF, in its current configuration, does not comply with the obligations arising from the principle

of transparency, in particular Articles 12, 13 and 14 GDPR.

B.4.3. - Liability (Art. 24 GDPR), data protection by design and by

default (art. 25 GDPR), integrity and confidentiality (art. 5.1.f GDPR), and security of processing

(Art. 32 GDPR)

has. Principle of liability and data protection by design and by default

474. Article 24.1 GDPR requires the controller to implement measures

appropriate technical and organizational arrangements, taking into account the nature, scope,

context and purposes of the processing as well as the risks, including the degree of probability and

of varying severity, for the rights and freedoms of natural persons, to ensure and be

able to demonstrate that the processing is carried out in accordance with the GDPR regulation.

These measures should also be reviewed and updated if necessary. This article

reflects the principle of "responsibility"" set out in Article 5.2 of the GDPR, according to which "the

controller is responsible for compliance with paragraph 1 (liability) and

can prove it". Article 24.2 of the GDPR provides that, when

are proportionate to the processing activities, the measures referred to in Article

24.1 of the GDPR below include the implementation of data protection policies

appropriate data by the controller.

475. Recital 74 of the GDPR adds that "there is a need to establish the liability of the controller

processing for any processing of personal data that it carries out itself

itself or which is carried out on its behalf. In particular, it is important that the head of the

processing is required to implement appropriate and effective measures and either

even to demonstrate the compliance of processing activities with this Regulation, including

including the effectiveness of the measures. These measures should take into account the nature,

scope, context and purposes of the processing as well as the risk it presents

for the rights and freedoms of natural persons. »

476. It is also the responsibility of the data controller, in accordance with Articles 24

(liability) and 25 GDPR (data protection by design and by default),

integrate the necessary compliance with the rules of the GDPR into its processing and procedures

(for example, ensuring the existence and effectiveness of procedures for handling

requests from data subjects, and relating to the verification of the integrity and

conformity of the TC String).

b. The contours of the safety obligation

477. In accordance with Article 32 GDPR, the controller is responsible for

guarantee the security of the processing, "taking into account the state of knowledge, the costs of

implementation and the nature, scope, context and purposes of the processing as well as

as risks, the degree of likelihood and severity of which vary, for the rights and freedoms

natural persons". The Litigation Chamber notes, however, a lack of

compliance with the obligation to ensure the security of the processing on the part of the defendant,

obligation which is part of the principle of responsibility. This gap is addressed in the

following points.

478. This breach of the obligation to ensure the security of the processing constitutes a point

fundamental to this Decision and the penalties it imposes. The absence of measures

technical and organizational aiming to guarantee the integrity of the TC String is considered

as a serious offence.

479. According to Article 5.1f GDPR, personal data must be processed in a manner

to ensure appropriate data security, including protection against processing

unauthorized or unlawful and against accidental loss, destruction or damage,

using appropriate technical or organizational measures. In the absence of measures

appropriate to secure the personal data of the persons concerned,

the effectiveness of respect for the fundamental rights to privacy and to the protection of

personal data cannot be guaranteed, particularly given the role

crucial role played by information and communication technologies in our society.

480. As indicated in the previous section, the absence of an obligation to ensure the security of the

treatment constitutes an important point of the decision222. Considering the very large

number of TC Strings generated each day as part of the TCF, it is essential that

all the rules governing participation in the TCF are observed and respected by

all parties involved, under the supervision of IAB Europe as Managing

Organization. The Litigation Chamber recalls that the combined reading of Articles 32

(security of processing), as well as 5.2 and 24 GDPR (principle of liability) imposes on the

controller to demonstrate its compliance with Article 32, by taking

appropriate technical and organizational measures, in a transparent and

traceable.

481. The Litigation Chamber also recalls the requirement of Article 25 GDPR (protection
data by design and by default), which imposes on the controller
to integrate the necessary compliance with the rules of the GDPR upstream of its actions.

482. It should also be noted that the security principle, with its various
components of data integrity, confidentiality and availability, is set out in
articles 5.1.f and 32 of the GDPR and is now regulated in the GDPR in the same way as
the fundamental principles of lawfulness, transparency and fairness.

222 See para. 448 and following of this decision.

107

483. IAB Europe offers the TCF to make the OpenRTB protocol GDPR compliant. In
in other words, the objective of the TCF is to guarantee that the processing of data to
personal character under the OpenRTB protocol take place in accordance with the
GDPR as well as the ePrivacy Directive. Therefore, IAB Europe, as Managing
Organization of the TCF and joint controller of the processing operations carried out
in this context223, must take organizational and technical measures to guarantee
that participants comply with at least the TCF Policies.

484. Although in the current TCF system of IAB Europe, adtech providers receive the
consent signals as part of an HTTP(S) request or via the APIs of
sailors, some authors believe that the measures in place under the TCF are
insufficient to guarantee the integrity of consent signals (in particular their
validity) and to ensure that an adtech provider actually received them (rather than
generated itself)224.

485. However, in the absence of validation by IAB Europe, it becomes theoretically possible for
CMPs to tamper with or modify the signal to generate a euconsent-v2 cookie and so
reproduce a "false consent" of users for all purposes and for all

adtech providers. This case is also explicitly provided for by 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 Division takes note of the fact that the possibility of falsification or

modification of the TC String by the CMPs is provided for in the TCF Policies document of the

defendant, which establishes the bases of 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”, whereby audits

organizations participating in the TCF (listed on the Global Vendors List) will take place226. The

Litigation Chamber encourages all initiatives emanating from the defendant, who

are intended to ensure compliance with the obligation to process personal data in

under the TCF in a secure manner. However, given the lack of control

systematic by the defendant of the respect of the TCF rules by the organizations

participants, and given the significant impact of such violations (notably, the

223 See above, title B.2. - Liability of IAB Europe for processing operations in Transparency and Consent

framework.

224 See on this subject, for example C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, “Consent Management Pl

Under the GDPR: Processors and/or Controllers? », in Privacy Technologies and Policy, APF 2021, LNCS, vol 12703,

Springer, 2021, p. 64.

225 Transparency and 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/

falsification or modification of the TC String), the Litigation Chamber considers that

this introduction of the TCF Vendor Compliance Program is insufficient to put the
defendant in compliance with the security obligation.
488. In particular, the Litigation Chamber relies on the fact that the sanctions regime of this
new program, provided by the defendant in the event of non-compliance with the rules of the TCF,
is permissive and not dissuasive. Indeed, an adtech supplier can claim responsibility
of a violation up to three times, without any sanction, before benefiting from a
28 days to comply. Only in the event of non-compliance after
the expiration of 28 days the adtech vendor will be suspended from the Global Vendors List.
He can also be reintroduced in the list if he complies with the rules afterwards. the
program also provides that an adtech provider may commit an offense
up to four times, before proceeding with his immediate suspension for a brief
14 day period, until the supplier comes into compliance. The “TCF Vendor
Compliance Programme” is therefore not a sufficient measure to ensure the
security of the processing of personal data carried out within the framework of the TCF.
489. The Litigation Chamber also observes that no measure other than the "TCF Vendor
Compliance Programme" is intended by the defendant to monitor or prevent the
tampering with or modifying the TC String.
490. With regard to the Complainants' allegation that IAB Europe is also in breach
Articles 44 to 49 of the GDPR, the Litigation Chamber recognizes, in view of the scope of the TCF
— which involves a large number of participating organizations — that it is clear that the
personal data included in the TC Strings will be transferred at some point
given outside the EEA by the CMPs, and that the defendant acts as responsible
processing in this respect (see paras. 356-357). However, the Litigation Chamber notes
that the Inspection Service did not include in its report an assessment of a transfer
concrete international data. For this reason, the Litigation Chamber concludes that it
there is a violation of the GDPR, but given the absence of proof of an international transfer

systematic, as well as the scope and nature thereof, the Litigation Chamber
considers that it is not in a position to sanction the defendant for a violation of the
articles 44 to 49 of the GDPR. Notwithstanding the foregoing, the Litigation Division judges
also that these international transfers of personal data, the case
applicable, should be evaluated first by publishers and CMPs implementing
works the TCF. The Litigation Chamber finds that publishers are responsible and
liable to take the necessary measures to prevent the personal data
personal data collected through their website and/or application are not transferred
outside the EEA without adequate international transfer mechanisms.
491. However, the Litigation Division is also of the opinion that the defendant should
facilitate the due diligence incumbent on publishers and CMPs, by
109
e.g. requiring adtech providers to clearly indicate whether they are localized
outside the EEA or if they plan to transfer personal data at a later date
personnel outside the EEA through their subcontractors. Furthermore, the
Litigation Chamber notes that, contrary to its obligation under the
principles of liability and data protection by design and by default,
IAB Europe has no mechanism in place to ensure that publishers and
Participating CMPs have adequate mechanisms in place for transfers
potential international partners of the TC String, as provided for in Articles 44 to 49 of the GDPR,
both at the time of its creation and during the transmission of the TC String to the suppliers
adtech participants. The preamble to the TCF Policies simply states 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
considers that this does not meet the requirements of Articles 24 and 25 of the GDPR.
492. The Litigation Division notes, for the record, that it is not certain that, given the

its current architecture and support for the OpenRTB protocol, the TCF can be

reconciled with the GDPR.

493. In this sense, the responsibility of IAB Europe is engaged from the moment when the organization

designs and makes available a consent or objection management system for

users, but does not take the necessary steps to ensure compliance,

the integrity and validity of such consent or objection.

494. The Litigation Chamber therefore notes that, within the framework of its security obligations

and integrity,

he

responsibility of IAB Europe to take effective measures, both

organizational and technical, to guarantee and be able to demonstrate the integrity of the signal

preference transmitted by CMPs to adtech suppliers.

B.4.4 - Other alleged violations of the GDPR

has. Purpose limitation and data minimization (Art. 5.1.b and 5.1.c GDPR)

495. Although in this decision, the Litigation Chamber has already concluded that the transactions

processing methods based on the OpenRTB protocol do not comply with the principles

fundamentals of purpose limitation and data minimization227 (therefore

that no guarantee is provided to ensure that the personal data

collected and disseminated within the framework of the OpenRTB are limited to information strictly

necessary for the purposes pursued), the Litigation Chamber emphasizes that the plaintiffs

have explicitly stated in their conclusions that they limit the scope of their claims

processing operations within the TCF. The Inspection Service also clarified

in its report that IAB Europe does not act as a data controller

227 See para. 455-456 of this decision

data for processing operations that take place entirely within the framework of

the OpenRTB.

496. Given these details, the Litigation Chamber concludes that, given the limited quantity

data relating to a user which is stored in a TC String before being

saved using a euconsent-v2 cookie, there is no violation of the principles of

Purpose limitation and data minimization in the context of the TCF.

497. Although larger amounts of personal data are processed

at a later stage, including special categories of personal data

personal, this is not the case in the context of the TCF. Within the framework of the TCF, there is therefore no

no violation of the principles of purpose limitation and data minimization.

b. Limitation of storage (Art. 5.1.e GDPR)

498. With regard to the principle of limitation of storage and on the basis of the report of the

Inspection Service, the Litigation Chamber considers that there is not sufficient evidence

as the TC String and associated storage of users' personal data

are stored for an unauthorized period, in violation of Article 5.1.e of the GDPR.

499. Consequently, the Litigation Chamber concludes that no violation of Article 5.1.e of the

GDPR could not be established.

vs. Integrity and confidentiality (Art. 5.1.f GDPR)

500. As already explained above228, the Litigation Chamber considers that the current version

of the TCF offers insufficient safeguards to prevent the values included in a

TC String are modified in an unauthorized manner, with the consequence that the

personal data of a data subject aggregated in a bid request

may be processed for improper purposes, in violation of the principle of integrity, and/or may

end up with bad adtech suppliers or adtech suppliers refused by

the user, in violation of the principle of confidentiality. The Litigation Chamber therefore judges

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 Department determined in its report, as
preliminary, that the Belgian Data Protection Authority was not competent for the
first and that IAB Tech Lab does not act as a data controller for the
second229.
228 See para. 477 et seq. of this decision.
229 Investigation report of the Inspection Service, p. 8-11.

502. The Litigation Division notes that the Inspection Service points out the absence of rules
appropriate 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 analyzes of the Service
of Inspection show that the TC String itself does not contain any information
which can be linked to the taxonomy of the websites visited, where, for example, categories
special personal data may be involved.
503. Consequently, the Litigation Chamber finds that this allegation is unfounded and that it
cannot be concluded that the defendant violated Article 9 of the GDPR.
e. Exercise of the rights of data subjects (Articles 15 to 22 of the GDPR)
504. First of all, the Inspection Service notes in its report that certain complainants have
state of the impossibility for the persons concerned to assert their rights, even if
the investigation carried out by the Inspection Service was unable to confirm these allegations.
Given the absence of proof of any infringement, the Litigation Chamber
limits its reasoning to general conclusions relating to the exercise of the rights of

persons concerned.

505. Secondly, the Litigation Chamber takes into consideration the scope of the conclusions written submissions from the complainants, in which they specifically limited their grievances to the processing of the personal data of the complainants by the defendant in the particular framework of the TCF230. Consequently, the Litigation Chamber will not assess the circumstances in which data subjects can exercise their rights regarding the processing of personal data contained in requests of offers, with respect to adtech providers, given that this processing takes place entirely under the OpenRTB protocol.

506. With regard to the current version of the TCF, the Litigation Chamber notes however that the TCF does not appear to facilitate the exercise of the rights of data subjects, in the as the CMP interface cannot be easily recalled at any time by users, so as to allow them to modify their preferences and find the identity of the adtech providers with whom their personal data has been shared by means of a bid request, in accordance with the OpenRTB protocol. In this regard, the Litigation Chamber emphasizes the importance of implementing and correct application of interface requirements as defined in the TCF Policies, so as to allow data subjects to effectively exercise their rights vis-à-vis each of the joint controllers, and notes that the Shared responsibility in this regard lies primarily with CMPs and publishers.

230 Plaintiffs' submissions of February 18, 2021, p. 2.

In these circumstances, however, the Litigation Chamber is not in a position to find a breach of Articles 15 - 22 GDPR.

f. Register of processing activities (Art. 30 GDPR)

507. The Inspection Service notes in its report that IAB Europe does not keep a record of its

processing activities. The defendant considers, first of all, that it can rely on

the exception provided for in Article 30.5 of the GDPR and that it is therefore not subject to the obligation

to maintain such records. During the investigation, the defendant nevertheless

added to the documents in the file a summary of its processing activities231.

508. The Litigation Chamber notes first of all that the register submitted by the defendant

so provided does not contain any activity relating to the TCF, with the exception of the management of

members, including

administration of the TCF. Unlike

the assertion of

the

defendant, namely that the records do not need to include the activities of

processing in the context of the TCF, the Litigation Chamber is of the opinion that the registers

must at a minimum include access to signals of consent, objections and

user 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 Managing Organization, to access

to “records of consent”. The Litigation Chamber also emphasizes that the character

incidental to this access to user preferences has not been demonstrated or raised

by the defendant. The stable relationship between IAB Europe, in its capacity as Managing

Organization, and all organizations participating in the TCF ecosystem, must also

be taken into account. Given the large number of participating organizations and

the defendant's intention to monitor the compliance of the various CMPs and other

adtech234 vendors in more depth in the future, IAB Europe should

also include this processing in its processing activity logs.

510. Consequently, the Litigation Division considers that the non-accessory nature of the

processing and the violation of Article 30.1 of the GDPR noted by the Inspection Service

are sufficiently proven.

g. Data protection impact assessment (Art. 35 GDPR)

511. The Litigation Chamber notes first of all that the defendant does not dispute that the

TCF can also be used for RTB purposes.

512. The defendant's argument that the TCF can be used for other purposes, unrelated

to direct marketing, and that the OpenRTB can also operate separately from the TCF

231 Response from IAB Europe to the investigation of February 10, 2020 (Exhibit 57), p. 23.

232 IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 38), p. 6.

233 IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 14.

234 See Hearing of June 11, 2021.

is therefore not relevant for the examination of the necessity or not of an impact assessment on the

Data protection.

513. Moreover, the correlation between the TCF and the RTB implies that the preferences that

users enter using the CMP interface will necessarily have an impact on

how their personal data will subsequently be processed by the

adtech providers under the RTB, in accordance with the OpenRTB protocol.

514. The Litigation Division also refers to decision No. 01/2019 of the General Secretariat

Belgian ODA235, in which the General Secretariat has drawn up a list of treatments for

which a data protection impact assessment is required.

515. It is indisputable for the Litigation Division that the TCF was developed, among other things,

for the RTB system, in which the online behavior of users is observed,

collected, recorded or influenced in a systematic and automated way, including to

advertising purposes. Nor is it disputed that under the RTB the data

are widely collected from third parties (Data Management Platforms, or DMPs) in order to

analyze or predict the economic situation, health, preferences or interests

personal data, the reliability or the behavior, location or movements of

natural persons237.

516. Given the large number of data subjects who come into contact with the

websites and applications implementing the TCF, as well as the growing number

of organizations participating in the TCF, on the one hand, and the impact of the TCF on the treatment

large scale of personal data under the RTB, on the other hand, the

Litigation Chamber finds that, in accordance with

Decision No 01/2019,

the

defendant is indeed subject to the obligation to carry out an impact analysis on the

data protection, pursuant to Article 35 of the GDPR. Therefore, there is

violation of Article 35 GDPR.

h. Appointment of the Data Protection Officer (Art. 37 GDPR)

517. Article 37 of the GDPR provides for the obligation to appoint a data protection officer

(DPD) in cases where:

i.

ii.

the processing is carried out by a public authority or a public body; Where

a controller or processor is primarily responsible for the

processing operations which, due to their nature, scope and/or

purposes, require regular and systematic monitoring on a large scale of

persons concerned; Where

235 Decision of the General Secretariat n° 01/2019 of 16

ODAhttps://www.gegevensbeschermingsautoriteit.be/publications/beslissing-nr.-01-2019-van-16-januari-2019.pdf.

236 General Secretariat Decision No. 01/2019 of 16 January 2019, para. 6.8).

237 General Secretariat Decision No. 01/2019 of 16 January 2019, para. 6.3).

January 2019, available at

the site

internet of

114

iii.

the core activities of the controller or processor consist of

into large-scale processing of special categories of data to

personal character referred to in Article 9 of the GDPR and personal data

personnel relating to criminal convictions and offenses referred to in Article

10 GDPR.

518. The Litigation Division has already concluded that the defendant processes personal data

personnel due to the fact that IAB Europe, in its capacity as Managing Organization, may

have access to TC Strings and records of consent238.

519. The former Article 29 Working Party indicates that processing activities which are

necessary to achieve the objectives of the controller or processor

can be considered basic activities within the meaning of Article 37 of the GDPR. The

Litigation Chamber considers that, given the importance of the TCF for the

defendant, of the declared objectives of the TCF as well as the associated processing of data to

personal character in its capacity as Managing Organization, the processing within the framework of the

TCF is part of the core business of IAB Europe.

520. With regard to the notion of “large-scale processing”, the Working Party “Article

29” specifies that the following elements must be taken into account in particular:

i.

the number of people involved - either as a specific number or

as a proportion of the relevant population;

the amount of data and/or range of different data processed;

the duration or permanence of the data processing;

the geographic scope of the processing activity.

ii.

iii.

iv.

In this case, the Litigation Chamber finds that the TCF is offered in different

Member States ; that the TCF inherently requires that personal data

users are treated as a TC String as long as it is

necessary to be able to demonstrate that the consent was obtained in accordance with the

TCF Policies; and that the personal data processed is further shared

with many adtech vendors. The Litigation Chamber concludes that the TCF

involves large-scale processing of personal data.

521. With regard to the criterion of regular and systematic observation, WP29 interprets the

term "regular" in one or more of the following ways:

i.

something that happens continuously or at specific times during

a certain period of time;

ii.

something that happens on a recurring or repetitive basis at times

fixed; Where

238 See para. 358 and 468 of this decision.

115

iii.

something that happens constantly or periodically.

The Litigation Chamber considers that the contractual obligation for suppliers

adtech and the CMPs to provide the defendant with “records of consent”, in

its capacity as Managing Organization, at the simple request of IAB Europe, falls under point (i).

There is therefore a regular observation of data relating to identifiable users.

522. The term “systematic” must be understood in one or more of the meanings

following:

i.

ii.

iii.

something that happens according to a system;

predisposed, organized or methodical;

something that happens as part of a general fundraising program

data ; Where

iv.

an action carried out within the framework of a strategy.

523. Once again, the Litigation Division considers that the processing of TC Strings or

records of consent by the defendant in the current version of the TCF meets at least

to the first three criteria. Consequently, the Litigation Chamber judges that the TCF must

be considered regular and systematic user observation

identifiable.

524. Based on the foregoing, the Litigation Chamber concludes that IAB Europe

should have appointed a DPO, in accordance with Article 37 of the GDPR. Therefore, there is

violation of Article 37 GDPR.

116

C. Penalty

525. On a preliminary basis, and as developed below, the Litigation Chamber notes that the

this decision on the TCF does not directly address deficiencies in the broader framework

of the OpenRTB. However, the Litigation Chamber draws attention to the risks

importance that OpenRTB poses to the fundamental rights and freedoms of people

concerned, in particular due to the large amount of personal data

concerned, profiling activities, prediction of behavior and

resulting monitoring (see A.3.1). Insofar as the TCF is the tool on which

OpenRTB relies to justify its GDPR compliance, the TC String plays a central role

in the current OpenRTB protocol architecture

526. Under article 100 LCA, the Litigation Chamber has the power to:

1° dismiss the complaint without follow-up;

2° order the dismissal;

3° order a suspension of the pronouncement;

4° to propose a transaction;

5° issue warnings or reprimands;

6° order to comply with the data subject's requests to exercise

his rights;

7° order that the person concerned be informed of the security problem;

8° order the freezing, limitation or temporary or permanent prohibition of the

treatment ;

9° order compliance of the processing;

10° order the rectification, restriction or erasure of the data and the

notification of these to the recipients of the data;

11° order the withdrawal of accreditation from certification bodies;

12° impose periodic penalty payments;

13° to impose administrative fines;

14° order the suspension of cross-border data flows to another State

or an international body;

15° forward the file to the public prosecutor's office in Brussels, which

informs him of the follow-up given to the file;

16° decide, on a case-by-case basis, to publish its decisions on the Authority's website

data protection.

527. As to the administrative fine that may be imposed under Article 83 of the GDPR and

of articles 100, 13° and 101 LCA, article 83 of the GDPR provides:

“1. Each supervisory authority shall ensure that the administrative fines imposed in

under this article for breaches of this Regulation referred to in paragraphs 4,

5 and 6 are, in each case, effective, proportionate and dissuasive.

117

Depending on the specific characteristics of each case, administrative fines are imposed

in addition to or instead of the measures referred to in points (a) to (h) of Article 58(2), and

j). To decide whether to impose an administrative fine and to decide the amount

of the administrative fine, due account shall be taken, in each case, of the

following elements:

has)

the nature, gravity and duration of the breach, taking into account the nature, scope

or the purpose of the processing concerned, as well as the number of persons

concerned affected and the level of damage they have suffered;

b)

whether the breach was committed willfully or negligently;

vs)

d)

e)

f)

any action taken by the controller or processor to

mitigate the damage suffered by the persons concerned;

the degree of responsibility of the controller or processor, account

given the technical and organizational measures they have implemented in

under sections 25 and 32;

any relevant breach previously committed by

processor or processor;

the person in charge of

the degree of cooperation established with the supervisory authority with a view to remedying the

violation and to mitigate any adverse effects;

g)

the categories of personal data affected by the breach;

h)

the manner in which the supervisory authority became aware of the breach, in particular

whether, and to what extent, the controller or processor has notified the

breach ;

i)

i)

where measures referred to in Article 58(2) have previously been

ordered against the controller or processor concerned

for the same purpose, compliance with these measures;

the application of codes of conduct approved pursuant to Article 40 or

certification mechanisms approved under Article 42; and

k) any other aggravating or mitigating circumstance applicable to the circumstances of

the species, such as the financial advantages obtained or the losses avoided,

directly or indirectly, as a result of the breach”.

528. Recital 150 of the GDPR239 makes an additional distinction depending on whether the

offender is a business or not. In the first hypothesis, the criterion (amount

fixed or percentage) to reach the highest fine should be applied. When,

on the other hand, the author of the infringement is not a company, it is necessary to take into account

the economic situation of the author and the general level of income in the Member State

concerned. This is to avoid the imposition of fines which could be disproportionate.

239 Recital 150 of the GDPR: “[...] When administrative fines are imposed on a company, this term must, at

For this purpose, be understood as a business in accordance with Articles 101 and 102 of the Treaty on the Operation of

the European Union. When administrative fines are imposed on persons who are not a company,

the supervisory authority should take into account, when considering what the appropriate amount of the fine would be, the level

general income in the Member State as well as the economic situation of the person concerned. ...]”.

118

529. It is important to contextualize the Respondent's breaches in order to identify the

most appropriate corrective actions. In this context, the Litigation Chamber

take into account all the circumstances of the case, including — to the extent that it

detailed below — of the reaction presented by the defendant to the sanctions

considered and communicated through the sanction form240. In this regard, the

Litigation Chamber specifies that

the form she sent mentions

expressly that this does not imply a reopening of the debates. Its only purpose is to

obtain the defendant's reaction to the penalties provided for.

530. While measures such as a compliance order or a ban on

further processing may end a

offense

identified, fines

administrative procedures, as defined in recital 148 of the GDPR, are imposed in the event of

serious breaches, in addition to or instead of the appropriate measures that are necessary

to remedy the violation.

531. The Litigation Chamber also wishes to recall that it is its sovereign responsibility,

as an independent administrative authority — in compliance with the relevant articles

of the GDPR and the LCA — to determine the corrective measure(s) and sanction(s)

appropriate(s). This stems from article 83 of the GDPR, but also from the Court of Markets which

underlined the existence of a wide margin of maneuver in its case-law, inter alia

in its judgment of July 7, 2021.241

532. The Litigation Chamber notes that the plaintiffs made various requests for

sanctions against the defendant. However, it is not for the complainants to

ask the Litigation Chamber to order a corrective measure or a sanction

particular, and it is not the responsibility of the Litigation Chamber to justify its refusal of one

requests made by the complainants. These considerations nevertheless leave

intact the obligation incumbent on the Litigation Chamber to justify the choice of measures

and sanctions it deems appropriate (from the list of measures and sanctions made available to it

provision by Article 58 of the GDPR and Article 100 of the LCA) to condemn the

defendant.

533. In this case, the Litigation Chamber notes that the plaintiffs ask the Chamber

Litigation to take the following measures and sanctions. These proposals are

integrated below for information (free translation):

“1) Pursuant to Article 100, §1, 8° of the LCA:

has.

prohibit IAB Europe from processing the TC String in the TCF;

240 See para. 534 as well as 272 et seq.

241 Court of Appeal of Brussels, section of the Court of Markets, 19th chamber A, section of market affairs, 2021/AR/320,

p. 37-47.

242 Market Court, 1 December 2021, FOD Financiën c. GBA, no. 2021/AR/1044, para. 25

119

b.

prohibit IAB Europe from processing in the TCF any personal data

personnel associated with the processing of the TC String, such as IP addresses, websites

visited and the applications used;

vs. order IAB Europe to permanently remove its website and other communication channels

public communication of all documents, files and records which, from

in any way induce or oblige a third party to carry out such processing;

2) Pursuant to Article 100, §1, 10° of the LCA, order IAB Europe to erase

definitively all TC Strings and other personal data already processed in

as part of the TCF of all its computer systems, files and data carriers, as well as

computer systems, files and data carriers of the subcontractors contracted by

IAB Europe;

3) Pursuant to Article 100, §1, 10° of the LCA, order IAB Europe to inform all

recipients of the personal data processed in the TCF of the imposed order

by the Litigation Division, including:

has.

b.

the prohibition of the processing of the TC String in the TCF;

the prohibition of the processing in the TCF of all personal data

associated with TC String processing, such as IP addresses, websites visited and

applications used;

the order for the permanent deletion of all TC Strings and other data to

vs.

personal character already processed under the TCF of all systems

computers, files and data carriers;

and this, in a clearly visible and legible way in a box in bold at the top of the home page

from the IAB Europe website www.iabeurope.eu in the usual font and size up to 6

months after a judgment of the Markets Court has become final, if applicable

in accordance with Article 108 LCA, or by e-mail, in both cases with a

hyperlink to the English version of the decision of the Litigation Chamber on the website

ODA;

4) Pursuant to Article 100, §1, 12° LCA on behalf of IAB Europe order the confiscation

a penalty payment of 25,000 euros per calendar day started for delay in the execution of any measure

imposed in the interlocutory decision of the Litigation Chamber from the expiry

seven calendar days after the interlocutory decision of the Litigation Chamber. »

534. A sanction form was sent to the defendant on October 11, 2021. IAB Europe

submitted its response on 1 November 2021243. This response was taken into account in the

following paragraphs.

243 See heading A.10. – Sanction form, European cooperation procedure, and publication of the decision, supra.

120

C.1. - Violations

535. The Litigation Division found that the defendant had violated the following articles:

▪ Articles 5.1.a and 6 of the GDPR — The current TCF does not provide a legal basis for the

handling user preferences in the form of a TC String. Furthermore, the

Litigation Chamber notes that the TCF proposes two legal bases for the

processing of personal data by participating adtech providers,

but finds that none of them can be used. First of all,

the

consent of data subjects is currently not given in a manner

sufficiently specific, informed and granular. Second, the interests of

data subjects outweigh the legitimate interest of the participating organizations

to the TCF, given the large-scale processing of user preferences

(collected under the TCF) as part of the OpenRTB protocol and the impact this may□
have on these. Since none of the grounds of lawfulness set out in Article 6 of the□
GDPR does not apply to this processing, as explained above244, the defendant□
violates Articles 5.1.a and 6 GDPR.□
Taking note of the fact that the defendant itself no longer has factual or□
technique on the TC Strings once these have been generated by the CMPs and□
stored on users' devices245, the Litigation Chamber finds that it□
cannot impose on the defendant the subsequent deletion of all TC Strings□
generated so far. Specifically, it is the responsibility of CMPs and publishers who□
implement TCF246 to take the appropriate measures, in accordance with the□
articles 24 and 25 of the GDPR, ensuring that the personal data which□
were collected in violation of Articles 5 and 6 of the GDPR are no longer processed and□
removed accordingly. To the extent that IAB Europe still stores□
TC Strings from consent cookies with global scope, which are no longer□
supported,□
the Litigation Chamber also considers that□
measures□
necessary must be taken by the defendant to guarantee the erasure□
permanent storage of those personal data which are no longer necessary.□
▪ Articles 12, 13, and 14 GDPR — As developed above (see B.4.2. - Obligation to□
transparency towards data subjects (Articles 12, 13 and 14 of the GDPR), the way□
whose information is provided to data subjects does not meet□
the requirement of a "transparent, understandable and easily accessible manner".□
Users of a website or application participating in the TCF do not receive□
sufficient information on the categories of personal data□
244 B.4.1 - Lawfulness and fairness of processing (Art. 5.1.a and 6 of the GDPR)□

245 In accordance with the Mandatory Policies and the technical specifications established and imposed on TCF participants by IAB Europe.

246 In addition, the Litigation Chamber emphasizes the fact that none of the CMPs and suppliers took part in this procedure.

121

collected about them, and are not able to determine in advance the scope and the consequences of the treatment. The information given to users is too general to reflect the specific treatment of each adtech provider, which also prevents the granularity — and therefore the validity — of the consent received for the processing carried out within the framework of the OpenRTB protocol. The people concerned are unable to determine in advance the scope and consequences of the processing, 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 above247, based on the articles 5.1.f and 32 GDPR, the controller is required to ensure the security of the processing and the integrity of the personal data processed. Bedroom Litigation recalls that the combined reading of Articles 5.1.f and 32, as well as 5.2 and 24 GDPR (principle of accountability) requires the controller to demonstrate its compliance with article 32, by implementing technical measures and organizational arrangements, in a transparent and traceable manner. As part of the current TCF system, adtech providers receive a consent signal without that no technical or organizational measure can guarantee that this signal of consent is valid or that an adtech provider actually received it (rather than generated). In the absence of systematic and automated control systems for CMP and Participating Adtech Providers by Defendant, Integrity of TC

String is not sufficiently secure, since it is possible for CMPs to falsify the
signal in order to generate a euconsent-v2 cookie and thus reproduce a "false
consent" of users for all purposes and for all types of partners. As
indicated above248, this hypothesis is moreover specifically covered by the
TCF terms of use. The Litigation Chamber therefore finds that IAB
Europe, in its capacity as Managing Organization, has designed and provides a system of
management of consent, but does not take the necessary measures to ensure the
validity,
integrity and
the conformity of the preferences and the consent of the
users.
The Litigation Chamber also notes that the current version of the TCF does not facilitate
not the exercise of the rights of the data subject, in particular taking into account the
relationship of joint responsibility for processing between the publisher, the CMP set up
and the defendant. The Litigation Chamber also points out that the GDPR requires
that the rights of data subjects can be exercised vis-à-vis each of the
joint controllers of the TCF so as to comply with Articles 24 and 25 of the GDPR.
247 See heading B.4.3. - Responsibility (art. 24 GDPR), data protection by design and by default (art. 25 GDPR),
integrity and confidentiality (art. 5.1.f GDPR), and processing security (art. 32 GDPR)
248 See para. 485 of this decision.

In view of the foregoing, the Litigation Division finds that the defendant has
breached its obligations of security of processing, integrity of personal data
personal and data protection by design and by default (Articles 24, 25,
5.1.f and 32 GDPR).
▪ Article 30 GDPR — As developed above249, the Litigation Chamber cannot

follow the defendant's argument that it believes it can benefit from the

exceptions to the obligation to keep records of its processing activities, such as

provided for in article 30.5 GDPR. Since the record of processing activities

of the defendant does not contain any treatment relating to the TCF, apart from the management of

members and administration of the TCF, while IAB Europe is able to access

to the records of consent as Managing Organization, the Litigation Chamber

finds the breach of Article 30 of the GDPR on the part of the defendant.

▪ Article 35 GDPR — Given the large number of data subjects who

come into contact with websites and applications implementing the TCF, as well as

that the organizations participating in the TCF, on the one hand, and the impact of the TCF on the

large-scale processing of personal data through the protocol

OpenRTB, on the other hand, the Litigation Chamber finds that IAB Europe has not

carried out a full data protection impact assessment (DPIA)

to the processing of personal data within the TCF, and therefore violated Article

35 GDPR. The Litigation Chamber notes that the TCF was developed, among other things,

for the RTB system, in which the online behavior of users is observed,

collected, recorded or influenced in a systematic and automated manner, including

advertising purposes. It is also undisputed that within the RTB, data is

widely collected from third parties (DMP) in order to analyze or predict the situation

economic, health, personal preferences or interests, reliability or

behaviour, location or movements of natural persons.

▪ Article 37 GDPR— Due to

large-scale, regular and

system of identifiable users involved in the TCF, and given the role of

the defendant, more specifically in its capacity as Managing Organization, the Chambre

Litigation judges that IAB Europe should have appointed a delegate for the protection of

data (DPD). By not doing so, the defendant violates Article 37 of the GDPR.

C.2. - Penalties

536. Consequently, the Litigation Division condemns the defendant:

I.

To make the TCF compliant with the obligations of legality, fairness and transparency

(articles 5.1.a and 6 GDPR), establishing a legal basis for the processing as well

249 See para. 507 et seq. of this decision.

that the sharing of user preferences within the framework of the TCF, in the form

a TC String and a euconsent-v2 cookie placed on users' devices

to this end. These obligations also imply that any data of a

personnel collected so far by means of a TC String within the framework of the

global consents, which are no longer supported by IAB

Europe, must be deleted by the defendant without undue delay. Furthermore, the

Litigation Chamber orders the defendant to prohibit the use of

legitimate interest as a legal basis for processing by organizations

participating in the TCF in its current format, through the conditions

of using the TCF.

II.

To make the TCF compliant with the obligations of transparency and information (Articles

12, 13 and 14 of the GDPR), requiring that CMPs registered with the TCF

adopt a harmonized and GDPR-compliant approach to

with regard to

information to be provided to users via their interface. This information, which

relate to the categories of data collected, the purposes of their collection and the

legal bases applicable to the processing, must be precise, concise and

understandable in order to prevent users from being surprised by the processing

subsequent processing of their personal data by parties other than the

publishers or IAB Europe.

III.

To ensure compliance of the TCF with integrity and security obligations, as well as

that data protection by design and by default (dedicated to

articles 5.1.f and 32 GDPR, and 25 GDPR). In this regard, the Litigation Chamber

orders to include technical and organizational control measures

effective in facilitating the exercise of the rights of data subjects and in

guarantee the integrity of the TC String, given the possibility, in the current state

of the system, to falsify the signal. An example of measures to be put in place under

of Article 32 of the GDPR is a strict verification process for organizations

participating in the TCF. The Litigation Chamber reminds the defendant, as well

than to other joint controllers, their obligation to take the

necessary arrangements to ensure, inter alia, that

the people

concerned can effectively exercise their rights. Finally, as part of

Article 25 of the GDPR, the defendant is obliged, via its terms of use,

prohibit organizations participating in the current version of the TCF from activating a

consent by default, as well as to base the lawfulness of the processing activities

envisaged on the legitimate interest.

IV.

To ensure the compliance of the register of processing activities carried out in the

framework of the TCF, and in particular concerning the processing of preferences and

user consent in the form of a TC String and the placement of a

euconsent-v2 cookie on their devices.

v.

To carry out a data protection impact assessment (DPIA),

covering both personal data processing activities in the

title of the TCF, and the impact of these activities on the further processing on the basis of the

OpenRTB protocol.

VI.

To appoint a Data Protection Officer (DPO), responsible, among other things, for

ensure the compliance of personal data processing activities in the

framework of the TCF, in accordance with articles 37 to 39 of the GDPR.

537. These compliance measures must be carried out within a maximum period of six

months after the validation of an action plan by the Belgian Data Protection Authority,

which will be submitted to the Litigation Chamber within two months of this decision.

On the basis of article 100 § 1, 12° of the LCA, a penalty payment of 5,000 EUR per day will be due

in the event of non-compliance with the aforementioned deadlines.

538. In addition to this compliance injunction, the Litigation Chamber considers that a

administrative fine is justified in this case for the following reasons, analyzed on the

basis of Article 83.2 GDPR.

539. The principles of legality, fairness, transparency and security are part of the essence of the

GDPR, and violations of these rights are subject to the highest fines,

in accordance with

Article 83.5 GDPR. In this regard,

failure to respect the principles

fundamentals of data protection must be sanctioned by fines at the

proportionate amount, depending on the circumstances of the case. In this sense, one can refer

the guidelines on the application and setting of administrative fines, according to

which:

“Fines are an important tool that supervisors should use

in the appropriate circumstances. Supervisors are encouraged to adopt

a well-considered and balanced approach when applying measures

remedies in order to react to the violation in a manner that is both effective and dissuasive

proportionate. This is not to see fines as a last resort or to

fear of imposing them, but, on the other hand, they should not be used in such a way either.

way that their effectiveness would be reduced. »250

540. In point (a), Article 83.2 mentions “the nature, gravity and duration of the violation,

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 harm they suffered”.

250 Article 29 Working Party - Guidelines on the application and setting of administrative fines for the purposes of

regulation 2016/679 (WP 253), p. 7.

125

541. With regard to the nature and seriousness of the breaches, the Litigation Division notes

that the principles of lawfulness (articles 5.1.a and 6 GDPR), transparency (articles 12 to 14 GDPR)

as well as security (articles 5.1.f and 32 GDPR) are fundamental principles of the regime

protection put in place 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, namely the transition from a regime based on

prior declarations and authorizations by the supervisory authority to a greater

accountability and responsibility of the controller. Compliance with its obligations

by the latter and its ability to demonstrate it are therefore all the more important.

542. A valid legal basis and transparent information are essential elements of the

fundamental right to data protection. With regard to transparency, this

principle constitutes a “portal” making it possible to reinforce the control of the persons

concerned on their personal data as well as the exercise of other rights

granted to data subjects by the GDPR, such as the right to object and the right

erasure. Violations of these principles constitute serious breaches, which

may be subject to the highest administrative fines under the GDPR

543. Violation of Article 25, relating to the obligation of data protection from the design stage

and by default, as well as Article 30, relating to the keeping of a register of the activities of

processing, also constitute significant offences, particularly in view of

the extent of processing operations and the impact on the privacy of complainants as well as

than other users confronted with websites or applications highlighting

works the TCF.

544. With regard to the nature and purpose of the processing, and more particularly the nature of the

data, the Litigation Chamber notes that the TC String, as an expression of the

user preferences regarding processing purposes and providers

adtech potential highlighted by the CMP interface, constitutes the cornerstone of the

TCF. Although the scope of this decision is the TCF and the TC String, well

that the sanction imposed on the defendant concerns only this framework, the compliance

of the OpenRTB protocol with the GDPR is evaluated as part of a holistic analysis of the

TCF and its interaction with the first. Since the current version of the TCF is

the tool on which the OpenRTB relies to justify its compliance with the GDPR, and since the

defendant facilitates membership in and use of OpenRTB by a significant number

of participating organizations, the Litigation Chamber observes that IAB Europe plays a

pivotal role with respect to OpenRTB, without being a data controller

data in this context.

545. With regard to the scope of the contested processing and the number of persons

concerned, the Litigation Division finds that the TCF (in its current format), as it

was developed by the defendant (representing major players in the

online behavioral advertising251), offers a unique service on the market. The scope of
TCF is therefore essential, given the growing number of partners who have joined.
With regard to the level of harm suffered by the persons concerned, the Chamber
Litigation stresses once again that the TC String plays a central role in
the current architecture of the OpenRTB protocol. Therefore, the TC String supports a system
presenting significant risks that OpenRTB poses to the rights and freedoms
fundamentals of the persons concerned, in particular because of the large amount of
personal data concerned, profiling activities, prediction of the
behavior and subsequent monitoring (see A.3.1).
546. With regard to the duration of the offence, the Litigation Chamber notes that the TCF
has been proposed by the defendant since April 25, 2018 as a mechanism allowing
to get
user consent to
with regard to processing purposes
predetermined, and to transfer their personal data to participants in the
TCF, including adtech providers. Notwithstanding the different iterations of the framework, which
was upgraded to the second version of the TCF on August 21, 2019, and considering the
systemic deficiencies of the TCF with regard to the GDPR, the Litigation Chamber finds
that the shortcomings have existed at least since May 2018, with regard to the validity of the
collected consent and placement of a String TC without a valid legal basis, and
since August 2019 for the use of legitimate interest as a legal basis in order to process
the personal data of the persons concerned.
547. Article 83.2.b GDPR requires DPA to take into account the intentional or
negligent of the offence. Noting that the defendant, in its capacity as Managing
Organization, was aware252 of the risks associated with non-compliance with the TCF, in particular

which concerns the integrity of the TC String and the encapsulated choices and preferences of
users, and given the impact of the TC String on subsequent processing in
within the framework of OpenRTB, the Litigation Chamber considers that IAB Europe has demonstrated
negligence in establishing measures governing the implementation of the version
current TCF.

548. In point (c), Article 83.2 GDPR refers to potential actions taken by the controller
processing 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 persons concerned (namely the
processing of their personal data independently of their choices, or in
lack of a valid legal basis).

251 See para. 36.

252 See para. 485

549. Article 83.2d of the GDPR concerns the degree of responsibility of the controller
or of the subcontractor, taking into account the technical and organizational measures that they have
implemented under Articles 25 and 32.

550. Even if the Litigation Division does not take into account in this decision the
developments after the closure of the procedure in June 2021, it notes that
the defendant announced during the hearing253 its intention to introduce a "TCF Vendor
Compliance Programme" in September 2021, through which audits of organizations
participating in the TCF (appearing on the Global Vendors List) will be set up.

551. The Litigation Chamber encourages all measures aimed at ensuring compliance
with the GDPR. However, as explained in paras. 487-488, given the absence
systematic control by the defendant of compliance with the rules of the TCF by the
participating organizations at the time of lodging the complaints, and taking into account

the significant impact of such violations (for example in the event of tampering or
modification of the TC String), the Litigation Chamber considers that the announcement of this
initiative to increase compliance with one of his obligations as responsible for the
processing of the TCF and consisting of audits of adtech suppliers listed on the Global
Vendors List demonstrates that the TCF did not comply with the security obligations of the
defendant, including the obligation to minimize the damage suffered by the persons
concerned. No other action was communicated by the defendant to the Chamber.
Litigation in this regard.

552. Moreover, the Litigation Division is no longer in a position to examine the nature of this
program and, in any case, this new program does not change the nature of the
GDPR breaches that occurred up to the close of proceedings in June 2021.

553. In light of Article 83.2.e of the GDPR, the Litigation Chamber notes the absence, at
time of this decision, any final decisions of other supervisory authorities
jurisdictions, concerning previous relevant infringements by the defendant in
relationship with the TCF.

554. Article 83.2.f of the GDPR concerns the degree of cooperation established with the authority, with a view to
to remedy the violation and to mitigate any adverse effects thereof. In this regard, the
Litigation Chamber does not share the conclusion of the Inspection Service that
the defendant did not cooperate sufficiently with the first, apart from the supply and
delivery of the register of processing activities carried out by IAB Europe.

555. With regard to the categories of personal data concerned by
the offense (article 83.2.g of the GDPR), the Litigation Chamber acknowledges that the data to be
personal character contained in and processed by means of the TC String are in

And confirmed by

253

https://iabeurope.eu/blog/iab-europe-launches-new-tcf-vendor-compliance-programme/.

the defendant by a public announcement on its website,

August 26, 2021

:

128

adequacy with the principle of minimization of data, taking into account their nature.

Notwithstanding the foregoing, the Litigation Division reiterates its position that the

TCF plays a central role in supporting processing operations as part of the

OpenRTB protocol. Consequently, the Litigation Chamber concludes that it cannot be

excludes that both special categories and regular categories of data to be

personal — processed through a bid request with the TC String attached

— may be affected by offenses committed under the TCF.

556. With regard to Article 83.2.h of the GDPR, the Litigation Chamber notes that this criterion

is not relevant here.

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 adherence to approved codes of conduct or

approved certification mechanisms. In this context, the Litigation Chamber notes

that IAB Europe has already been in contact with the Belgian Data Protection Authority

concerning the drafting and adoption of a code of conduct (when the procedure

was already underway). The Litigation Chamber also underlines the lack of monitoring of the

defendant in this regard since June 2020, without further explanation on its part.

559. Finally, Article 83.2.k of the GDPR covers any other aggravating or mitigating circumstance

applicable to the circumstances of the case, such as the financial advantages obtained or the

losses avoided, directly or indirectly, as a result of the breach. Bedroom

Litigation did not retain specific elements likely to modify the amount

of the fine.

560. To determine the amount of the administrative fine, Articles 83.3 to 83.7 of the GDPR

use the term "company" which, on the basis of recital 150 of the GDPR and as

confirmed by the Article 29 Working Party and the EDPB254, must be interpreted

in accordance with Articles 101 and 102 TFEU. Based on the case law of the CJEU,

the notion of undertaking in Articles 101 and 102 TFEU refers to an entity

single economic entity, even if this economic entity is legally constituted by

several natural or legal persons.255

561. To assess whether several entities form a single economic entity, it is necessary to

take into account the ability of each entity to make free decisions. It suits

also to examine whether or not a governing body (the parent company) exercises an influence

decisive on the other entity (the amount of the participation, the links at the personnel level or

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 May 25, 2018; as well as the decision

binding 1/2021, para. 292, of the EDPB.

255 Judgment of the CJEU of 23 April 1991. Klaus Höfner and Fritz Elser v Macrotron GmbH, C-41/90, ECLI:EU:C:1991:161,

paragraph 21, and judgment of the CJEU of 14 December 2006, Confederación Española de Empresarios de Estaciones de

Servicio, C-217/05, ECLI:EU:C:2006:784, paragraph 40. 40

of the organization, the instructions and the existence of work contracts are examples

of criteria).

562. The Litigation Chamber could not find any indication of a decisive influence of IAB Inc.

on the defendant IAB Europe, or a limitation of its freedom of decision with regard to

of IAB Inc.

563. This was also developed by the defendant in its response to the complaint form.

sanction, in which IAB Europe asserts that IAB Inc. has no interest in the

defendant nor any right of inspection over the deployment of IAB Europe's activities. The

defendant indicated that IAB Inc. (headquartered in the United States) licenses

of the "IAB" brand to other organizations and remains an entirely separate entity

and independent of IAB Europe.

564. The Litigation Chamber therefore decides to rely solely on the financial income

of IAB Europe as a reference for the calculation of the administrative fine, instead of the figure

Annual Business of IAB Inc.

565. In this regard, the Litigation Chamber notes that the annual gross profits of the

respondent amounted to EUR 2,471,467 in 2020256. In the alternative, the Chamber

Litigation also observes that participating organizations are required to pay

an annual fee of EUR 1,200 to the defendant when they registered for the TCF257.

Considering the total number of adtech providers registered with the TCF, which increased by

significantly, going from 420 on May 25, 2020 to 744 on June 7, 2021, the Chamber

Contentious therefore notes that a large part of IAB Europe's income is generated

through the granting of licenses for the use of the TCF. More specifically, IAB Europe would carry out a

gross profit of at least EUR 981,600 for 2021 with the only annual contribution of

TCF participants — including adtech providers and CMPs258.

566. Under Article 83.4, breaches of Articles 25, 30, 32, 35 and 37 of the GDPR may

amount to up to EUR 10,000,000 or, in the case of a company, up to 2% of the turnover

total global annual revenue for the previous fiscal year.

567. Under Article 83.5 GDPR, breaches of Articles 5.1.a, 5.1.f, 6, and 12 to 14 GDPR

may amount to up to EUR 20,000,000 or, in the case of a company, up to 4% of the

total worldwide annual revenue for the previous financial year. The maximum amount of

the fine in this case, as provided for in article 83.5, is therefore EUR 20,000,000.

256See the 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 Totaling 74 CMP on June 7, 2021: https://iabeurope.eu/cmp-list/. The actual profit is likely to be higher,

given the ever-increasing number of TCF participants.

130

568. As regards, inter alia, violations of a fundamental right enshrined in Article 8 of the Charter of Fundamental Rights of the European Union, the assessment of their gravity on the basis of Article 83.2.a GDPR will be done independently.

569. On the basis of the elements developed above, of 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 aforementioned offenses justify imposing to the defendant a compliance order accompanied by a fine administrative charge of 250,000 EUR (article 100, § 1, 13° and 101 of the LCA), as a penalty effective, proportionate and dissuasive under Article 83 GDPR. To determine what amount, the Litigation Chamber took into account the total annual turnover of the defendant, which amounted to EUR 2,471,467 in 2020259.

570. The amount of EUR 250,000 remains, in view of the above, proportionate to the offenses that have been established by the Litigation Chamber. This amount is also significantly lower than the maximum amount of EUR 20,000,000 provided for in Article 83.5 of the GDPR.

571. The Litigation Division is of the opinion that a lower fine would not respond, in the species, to the criteria required by section 83.1. of the GDPR, according to which the fine administrative action must not only be proportionate, but also effective and dissuasive. These elements derive from the principle of sincere cooperation described in recital 13 of the GDPR (in accordance with Article 4.3 of the Treaty on European Union).

572. Given the importance of transparency regarding the decision-making process of the

Litigation Chamber and in accordance with article 100, §1, 16° of the LCA, this decision

is published on the website of the Data Protection Authority260. In view of

prior publicity surrounding this matter, as well as the general interest to the public and

the significant number of people concerned and organizations involved, the Chamber

Litigation has decided not to delete the direct identification data of the parties

and the persons mentioned, whether natural or legal persons.

259 See the annual accounts 21/12/2020, available at https://cri.nbb.be/bc9/web/catalog?execution=e1s1.

260 See para. 287.

131

FOR THESE REASONS,

the Litigation Chamber of the Data Protection Authority decides, after deliberation:

- to order the defendant, in accordance with article 100, paragraph 1, point 9, of the LCA, in

with a view to bringing the processing of personal data under the TCF into

compliance with the provisions of the GDPR:

has. to provide a valid legal basis for the processing and dissemination of the preferences of

users under the TCF, in the form of a TC String and a cookie euconsent-

v2, as well as prohibiting, through the TCF Terms of Use, the use

legitimate interests as the basis of lawfulness for the processing of personal data

by organizations participating in the TCF in its current form, in accordance with the

articles 5.1.a and 6 of the GDPR;

b. to ensure effective technical and organizational control measures in order to

guarantee the integrity and confidentiality of the TC String, in accordance with articles 5.1.f, 24,

25 and 32 GDPR;

vs. to maintain a strict audit of organizations adhering to the TCF in order to ensure that the

participating organizations meet the requirements of the GDPR, in accordance with the

articles 5.1.f, 24, 25 and 32 of the GDPR;

d. to take technical and organizational measures to prevent the

consent is checked by default in the interfaces of the CMPs as well as to prevent

the automatic authorization of participating adtech providers basing their operations

of processing on the legitimate interest, in accordance with articles 24 and 25 of the GDPR;

e. compel CMPs to adopt a uniform and GDPR-compliant approach to

information they submit to users, in accordance with Articles 12 to 14 and

24 GDPR;

f. update the current register of processing activities, including the processing of

personal data in the context of the TCF by IAB Europe, in accordance with article 30

GDPR;

132

g. to carry out a data protection impact assessment (DPIA) with regard to

regarding the processing activities carried out within the framework of the TCF and their

impact on the processing activities carried out under the protocol

OpenRTB, as well as adapting this AIPD to future versions or modifications of the

current version of the TCF, in accordance with Article 35 of the GDPR;

h. to appoint a data protection officer (DPO) in accordance with the

articles 37 to 39 of the GDPR.

These compliance measures must be implemented within a maximum period

six months after the validation of an action plan by the Belgian Data Protection Authority

data, which will be submitted to the Litigation Chamber within two months of this

decision. In accordance with article 100 § 1, 12° of the LCA, a penalty payment of 5,000 EUR

per day will be due in the event of non-compliance with the aforementioned deadlines.

- to impose an administrative fine of EUR 250,000 on the defendant pursuant to

section 101 of the ACL.

This decision may be appealed to the Court of Markets, in accordance with

Article 108, § 1 of the LCA, within thirty days of its notification, with

the Data Protection Authority as defendant.

(Sr.) Hielke HIJMANS

President of the Litigation Chamber

133