1/58

Litigation chamber

Decision on the merits 85/2022 of 25 May 2022

File number: DOS-2020-03432

Re: Use of cookies on the media websites of Knack and Le Vif (Roularta Media

group)

The Litigation Chamber of the Data Protection Authority, made up of Mr Hielke Hijmans,

Chairman, and Messrs. Christophe Boeraeve and Frank De Smet, members;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 relating to the protec

of natural persons with regard to the processing of personal data and to the free movement

of this data, and repealing Directive 95/46/EC (General Data Protection Regulation), here-

after GDPR;

Considering the law of December 3, 2017 creating the Data Protection Authority (hereinafter LCA);

Having regard to the law of 30 July 2018 relating to the protection of natural persons with regard to the processing of

personal data, hereinafter LTD;

Having regard to the internal regulations as approved by the House of Representatives on December 20, 2018

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

Considering the documents in the file;

made the following decision regarding:

.

.

The defendant:

Roularta Media Group, a public limited company under Belgian law, having its registered office

.

.

registered office at 8800 Roeselare, Meiboom, 33, and registered with the Banque-Carrefour des

.□

.□

Companies under the number 0434.278.896, represented by Maître Tom De□

Cordier, having his practice at 1170 Watermael-Boitsfort, Chaussée de La Hulpe□

178 (CMS).□

Decision on the merits 85/2022 - 2/58□

I. Facts and procedure□

I.1. Investigation by the Inspection Service□

1. On January 16, 2019, the Management Board of the Data Protection Authority ("DPA") decides,□

on the basis of Article 63, 1° of the LCA read in the light of Article 57, paragraph 1, points a) and h) of the GDPR,□

to submit a file to the Inspection Service in the context of the use of cookies on the sites□

Belgian media website.□

2. More specifically, it was decided to carry out a survey of the most popular Belgian news media.□

frequently viewed:1□

1□

2□

3□

4□

5□

6□

7□

8□

9□

HLN□

DPG Media nv□

http://hln.be/□

Het Nieuwsblad□

mediahuis□

http://nieuwsblad.be/□

TRV□

Sudinfo□

The DH□

TRV□

http://deredactie.be/□

Rossel Group□

http://sudinfo.be/□

IPM Group SA□

http://dhnet.be/□

From Standaard□

mediahuis□

http://standaard.be/□

RTBF□

RTBF□

Gazet van Antwerpen Mediahuis□

http://rtbf.be□

http://gva.be/□

RTL□

RTL Group□

http://RTL.be□

10 Importance□

from□

mediahuis□

http://hbvl.be/□

Limburg□

11□

The evening□

12 7 out of 7□

13 The Free□

Rossel Group□

http://lesoir.be/□

DPG Media nv□

http://7sur7.be/□

IPM Group SA□

http://lalibre.be/□

14 DeMorgen□

DPG Media nv□

http://demorgen.be/□

15 De Tijd□

16□

the future□

17 VTM□

MEDIAFIN NV□

http://tijd.be/□

Nethys.sa□

http://lavenir.net/□

DPG Media nv□

http://vtm.be□

NL□

NL

NL

FR

FR

NL

FR

NL

FR

NL

FR

FR

FR

NL

NL

FR

NL

18 Sudpresse

Editions

Rossel Group

http://www.sudpressedigital.be/ EN

Foxgloves

19 Knack

Roularta Media

http://knack.be/

group

20 The Snitch

Roularta Media

http://levif.be/

group

NL

FR

1 According to figures from the Center for Information on the Media (CIM) from 2019.

Decision on the merits 85/2022 - 3/58

3. The above-mentioned survey concerned the verification of the basic principles of the GDPR and the Directive

e-Privacy in the context of the use of cookies and, more specifically:

-

-

the accessibility and clarity of information about cookies;

compliance with obtaining user consent for the placement of cookies that

are not strictly necessary;

-

the placement (or not) of cookies that are not strictly necessary before obtaining

user consent;

-

the possibility for the user to configure his acceptance of cookies (i.e. the

possibility of differentiating the choices at a more general level), in particular to refuse

cookies for profiling for advertising purposes.

The study was based on the following principles:

-

Further browsing is no longer accepted, as it contradicts the GDPR;

- In order to comply with the requirement of consent, which implies freedom of choice, the possibility

to configure cookies must exist and clear information must be provided on

the purposes of the categories of cookies;

- For websites currently operating with a setting, the effectiveness of this

configuration must be checked at the technical level.

4. The investigation by the Inspection Service for the websites www.knack.be and www.levif.be ended on 7

October 2020 and the file is submitted by the Inspector General to the President of the Chamber

litigation, in accordance with art. 91, §1 and §2 ACL.

5. The Inspection Service's investigation reports contain the following findings:

1. Placement of cookies that are not strictly necessary before obtaining the

consent (potential breach of GDPR Article 6.1(a)):

▪ Article 6.1 a) GDPR and Article 129 of the Electronic Communications Act

(ECL) stipulate that the consent of the persons concerned is required for

the installation of cookies, except those that are strictly necessary;

▪ The technical analysis of the Inspection Service shows that cookies are installed

before the data subject was able to give their consent (66 cookies for

Knack and 60 cookies for Le Vif). These include third-party cookies (48 for

Knack, 44 for Le Vif). The technical report would also show that

many analytical cookies and marketing cookies have been saved.



▪ For the Knack and Le Vif sites, only two cookies were considered strictly

required.

2. Statistical cookies are placed without consent (potential violation of

Article 6.1 a) GDPR):

▪ The cookie settings screen demonstrates that on the Knack and Le

Vif, Roularta Media Group considers statistical cookies as cookies

not subject to consent. They are indeed always active by default and do not

can be disabled;

▪ First-party “statistical” cookies do not necessarily fall under the

the exception of "strictly necessary cookies" provided for in Article 5.3, paragraph

2, of the ePrivacy Directive. The Litigation Chamber ruled in a decision as to

at bottom 12/2019 of December 17, 2019 that statistical cookies cannot be

considered as cookies strictly necessary for the provision of a service

requested by a subscriber, within the meaning of article 129, paragraph 2 LCE. She judged that the

notion of “necessary” must be interpreted in accordance with the objectives of

protection of European data protection law, in the sense that this

exception can only be invoked in the interest of the persons concerned (the

website visitors) and not in the exclusive interest of the service provider

of information. Although website operators consider these cookies to be

essential to the provision of their service, they are not absolutely

necessary to provide the information service requested by the site visitor

web.2

▪ However, in the same decision, the Litigation Chamber did not exclude the

possibility that, under certain conditions, certain statistical cookies may

actually be cookies strictly necessary for the provision of a service

requested by the person concerned, for example to detect a problem of

navigation. However, this is not the issue in this case.3

3. Pre-ticked boxes for partners (potential violation of Articles 4.11, 6.1 a) and 7.1

GDPR):

▪ The GDPR requires an “unequivocal statement or active act” (Article 4.11

GDPR), which means that any presumed consent based on a mode of action

more implicit on the part of the person concerned does not comply with the standards

GDPR consent. The Inspection Service relies on the Planet49 judgment which

CC,

2

https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-12-2019.pdf,

3Ibid.

Decision

12/2019

as to

bottom

from

to

17

december

2019,

Decision on the merits 85/2022 - 5/58

clarified that

Article 2. F

(definition of consent) and

section 5.3

(consent for cookies) of the ePrivacy Directive must be read

in conjunction with Article 4.11 and Article 6.1(a) of the GDPR.4 The Court of Justice has

then held that the consent was not validly given when the

storage of information by means of cookies or access to information already

stored on the website user's end device by means of cookies is

authorized by means of selection boxes checked by default that the user must

uncheck if he refuses to give his consent;5

▪ The technical analysis shows that the cookies of the partner companies are

enabled by default;

▪ The Inspection Service also notes that the defendant did not

complied with the obligation under Article 7.1 of the GDPR to prove that the person

data subject has given consent to the placing of cookies which are not

strictly necessary.

4. Disclaimer for third-party cookies (potential violation of Articles

5.2 a) and 7.1 GDPR):

▪ According to the Inspection Service, Roularta Media Group is trying to discharge the

responsibility for third-party cookies placed when visiting the Knack and Le Vif sites;

▪ For example, the cookie policy states that Roularta Media Group

is not responsible for cookies placed and managed by third parties (for example, for

allow the sharing of information via social networks). The policy in

regarding cookies also indicates that Roularta Media Group has no control

on certain cookies used on its website.

▪ Regarding this aspect,

the Inspection Service refers to

the stop

Wirtschaftsakademie of the Court of Justice in which it was held that the

owner of a website is responsible for the treatment of cookies that his site

web installs or reads.6 At the very least, it participates in defining the purposes and

4 Judgment of the Court of Justice of 1 October 2019, C-673/17, ECLI:EU:C:2019:801, Planet49 (hereinafter: “Planet49 judgme

65: “In view of the foregoing, the answer to the first question under points a) and c) must be that Articles 2, under f), and 5, para

3 of Directive 2002/58, read in conjunction with Article 2(h) of Directive 95/46, and with Articles 4(11) and 6,

paragraph 1(a) of Regulation 2016/679 must be interpreted as meaning that the consent referred to in these provisions does not

been validly given when the storage of information by means of cookies or the access to information already stored on

the terminal device of the user of a website is authorized by means of cookies by means of a selection box checked by default

that this user must uncheck if he wishes to refuse his consent. »

5 Ibid.

6 Judgment of the Court of Justice of 5 June 2018, C-210/16, ECLI:EU:C:2018:388, Wirtschaftsakademie, par. 39: “Under these

should be considered as the manager of a fan page on Facebook, such as Wirtschaftsakademie, by defining settings in

depending, in particular, on its target audience and the objectives of managing or promoting its activities, participates in the defi

purposes and means of processing the personal data of visitors to its fan page. To this end, this manager must

be considered, in casu, as responsible in the Union, jointly with Facebook Ireland, for such processing within the meaning of Arti

(d) of Directive 95/46. »



means of processing the personal data of visitors to its site

web by allowing third-party applications on its website or the distribution of

third-party content in the advertising spaces of its website.7

▪ Next, the Inspection Service refers to the principle of liability in article 5.2

of the GDPR, according to which the controller is responsible for ensuring compliance

principles relating to the processing of personal data and must be

able to demonstrate compliance with these principles.

▪ This practice used by Roularta Media Group should also be considered

as a violation of Article 7.1 of the GDPR, because a data controller must

demonstrate that the data subject has given consent for the

placement of all cookies that are not strictly necessary.

5. Incorrect and insufficient information (potential violation of Articles 4.11, 12.1, 13

and 14 GDPR).

▪ Roularta Media Group's cookie policy contains

provisions that do not comply with the GDPR. For example, the policy in

cookie policy speaks of implied consent for cookies via access

to the websites of Roularta Media Group, which contradicts the need

an expression of the will by a clear statement or a positive action in

pursuant to Article 4.11 of the GDPR. It also indicates that no consent□

specific is required for the sharing of data collected through the□

cookies, which is contrary to the specific nature of consent for a□

data processing under Article 4.11 of the GDPR;□

▪ The cookie policy would also lack clarity as to the□

need to use third-party cookies due to technical problems that last□

for more than a year ;□

▪ The Inspection Service also observes that the names of the types of cookies in□

the cookie policy does not correspond to the names of the categories□

cookies in the cookie setting tool, which does not improve the□

comprehensibility;□

▪ In addition, the cookie policy does not contain information about cookies.□

cookie storage periods. The cookie policy would indeed□

reference to an unlimited storage period for cookies;□

7 Ibid.□

Decision on the merits 85/2022 - 7/58□

▪ The cookie policy indicates that the partners use the “IAB□

Europe Transparency & Consent Framework", which ensures that third parties□

comply with the GDPR. However, of the 449 partners listed on the sites of□

Knack and du Vif, 312 have not or no longer been validated by the IAB;□

▪ The fact that the user must consult the policies of the 449 vendors (“vendors”)□

to find out what these companies are doing with their data and to decide□

informed consent to give consent on this basis is more□

than illusory and unenforceable. In addition, this is likely to lead to the placement□

even more cookies when visiting links to these partners;□

▪ Finally, it should be noted that cookies are not individually documented, which□

does not allow the user to control what is done with their data.

6. Unjustified cookie storage periods (potential violation of Article 5.1 e) of the

GDPR):

▪ The Inspection Service refers to article 5.1 e) GDPR, which stipulates that cookies do not

may be stored longer than necessary to achieve the purpose.

This retention period cannot therefore be indefinite. Information

collected and stored in a cookie and the information collected as a result of the

reading a cookie should be deleted when no longer needed

for the intended purposes. A cookie exempt from the requirement of consent must have a

lifetime directly related to the purpose for which it is used and must be

configured to expire as soon as it is no longer needed, taking into account the

reasonable expectations of the user. Cookies that are not subject to

the obligation of consent should therefore generally expire at the end of the

browser session, or even before8;

▪ The technical analysis report demonstrates that the effective storage periods

are unreasonably long and cookies have a lifespan of

several years. The cookie policy refers to a period of

storage which is in principle unlimited.

7. Non-compliance with the withdrawal of consent (potential violation of article 7.3 of the GDPR):

▪ Article 7.3 of the GDPR stipulates that the data subject has the right to withdraw his

consent at any time;

▪ The technical analysis shows that the withdrawal of consent is not effective. He

technical analysis of the Knack site shows that the number of cookies does not decrease

8See “The lifetime of cookies” and

https://www.gegevensbeschermingsautoriteit.be/burger/thema-s/internet/cookies.

the “Questions” of the thematic file “Cookies” on

the website of

ODA,

Decision on the merits 85/2022 - 8/58

not after returning to minimal choices. The Inspection Service finds that

when he withdraws his consent again, there is no change in the

amount of cookies downloaded, on the contrary, the number of cookies increases.9

The technical analysis of Le Vif's website shows that it is impossible to

operate the cookie management tool after the initial consent has been

given.

6. On November 6, 2020, the Litigation Chamber requests additional information from the

Inspection service on the basis of article 94, 2° and 96, § 2 LCA concerning examination reports

technical.

7. On November 30, 2020, the additional investigation ends and the Inspection Service provides a

additional investigation report to the Litigation Chamber.

I.2. The procedure before the Litigation Chamber

8. On December 21, 2020, the Litigation Chamber decides on the basis of article 98 LCA that the file

is ready for substantive consideration.

9. On December 21, 2020, the defendant is informed by registered mail of this

decision, as well as the inspection report and the inventory of documents in the file transmitted by the

Inspection service at the Litigation Chamber. The defendant is also informed of the

deadlines for presenting its means of defense in accordance with article 99 LCA. The reception time

of the defendant's response has been set for February 9, 2021.

10. On January 6, 2021, the Litigation Chamber received a letter from counsel for the defendant.

In the aforementioned letter, the defendant requests a copy of the file (art. 95, § 2, 3°

LCA) and asks to be heard by the Litigation Chamber in accordance with article 98 LCA,

in order to be able to present his defenses orally.

11. On January 18, 2021, the Litigation Chamber transfers a copy of the file to the defendant.

12. On February 9, 2021, the Litigation Chamber receives the conclusion of the response from the party

defendant. A summary of the pleas and arguments put forward by the party is given below.

defendant in this conclusion.

13. In its submission in response, the Respondent first points out that certain

inaccuracies were noted during the DPA review.

▪ Reason 1: The investigation was not conducted in accordance with the applicable rules of the art.

9 See page 46 of the De Knack Inspection Report: “Between step 24 “all” and step 26 “minimum”, the number of cookies does n

not ".



oh

Essential elements are missing during manual cookie scans, namely the

list of URLs visited and specific requests regarding the placement of

Cookies. It is therefore impossible for Roularta Media Group to check which URLs

were visited during the search and if these URLs were restricted to Roularta and if

cookies were already present or placed during each scenario of

consent.

o Cookiebot and Onetrust were used as classification mechanisms (no

of the two only provides information and methodology on the method of

classification

used).

o In addition, the Inspection Service used a free version of both mechanisms,

this

who

not

contributes

not

at

the

credibility

of

investigation.

o Finally, the classifications of OneTrust and Cookiebot have conflicts, and

the study does not specify anywhere how these are resolved when the mechanisms

are applied to Roularta cookies.

oh

Unclear terminology: “no technique”, “further browsing”, “CMP”,

"cookie wall", "permanent banner", "non-permanent banner".

o Non-professional tooling: WEC and Cookie Manager are github repositories

immature by any software development standard. Although the WEC carries the

SEPP approval label, this standard was developed solely by Robert

Riemann, IT Policy Officer of the European Data Protection Supervisor

(EDPS), and is not actively maintained, judging by the number of pull requests

and recent ongoing issues. Cookie Manager was also developed by

an individual (Rob Wu) who has no specific training in compliance

privacy or security.

▪ Way 2: the document uses sources/tools that are not official

o The sources of the classification of cookies cannot be verified, and the

documented sources are unreliable. Both OneTrust and Cookiebot have

developed their own cookie classification databases which help

controllers to begin their understanding of cookies during the implementation

work of a CMP.

o For OneTrust, classifications are based on ICC guidelines at the

UK, which are no longer available, and supplemented with "a layer of

simple rules that allow clearer decisions in certain scenarios

Decision on the merits 85/2022 - 10/58

with borderline cases, and a methodology to classify best practices

when additional information about the use of certain cookies does not

are not otherwise available.

o As for Cookiebot: property of the Swedish company Cybot, it only indicates

that the company maintains a global repository of cookies without mentioning the

methodology and sources.

o The credibility of these classifications is further affected by the fact that the Researcher

uses free versions of Cookiebot and OneTrust which aim to encourage

users to purchase a full subscription.

o Reference to the gdpr.eu website for the definition of cookies strictly

required: site belonging to the Swiss company Proton Technologies AG. the

Service Inspection could also refer to the appropriate legislation.

o Third-party cookie ratio: The Inspection Service asserts that the relationship between

first and third party cookies in the context of strictly necessary cookies

serves as a proxy for a potential breach. This while there is absolutely no

causal link between the purpose of a cookie and domain ownership.

o Manual cookies do not contain timestamps. Therefore, Roularta

cannot verify whether these cookies have actually been placed in order and what

cookies were added after a specific consent setting.

14. The defendant then addresses the findings of the Inspection Service:

▪ Observation 1: Placement of cookies that are not strictly necessary before

obtaining consent.

o Roularta states in its conclusions that it cannot check which cookies have□

were actually placed at the time of the findings. She indicates that due to a□

lack of technical knowledge at Roularta, implementation of OneTrust□

was faulty. Cookies placed by advertisers should□

normally follow the consent that has been transmitted through the IAB TCF.□

According to Roularta, however, it is very difficult to constantly monitor whether all□

IAB vendors abide by the IAB TCF agreements.□

o Roularta indicates that in 2021 all information and content sites will be□

grouped under a single Roularta domain, making it much easier to control□

this issue.□

▪ Observation 2: statistical cookies without consent□

Decision on the merits 85/2022 - 11/58□

o According to Roularta,□

the placement of statistical cookies before□

obtaining the□

consent is compatible with art. 6.1 a) GDPR. This is due to the fact that the□

placement of these statistical cookies is intended to collect statistics of□

database gathered on the use of its websites, which is necessary for the□

website business model:□

▪ reliable visit figures verified by the CIM (Centre d'Information sur□

the Media) must be made available to advertisers;□

▪ on the other hand, newsrooms must be able to measure the results□

articles published online in order to be able to carry out evaluations and□

constant adaptations.□

o The defending party refers to the fact that the aggregated data does not fall□

not within the scope of the GDPR.□

o In addition, the APD had not yet published official guidelines on the obligation

to obtain consent for the placement of statistical cookies. The part

defendant then refers to the position of the CNIL (French authority) and the AP

(Dutch authority) regarding statistical cookies. She argues that she

had

inspired its practice in terms of statistical cookies on

them

recommendations of the CNIL and the AP. According to his own interpretations, the

Roularta's practice regarding statistical cookies was compliant with the LCE and

to GDPR.

▪ Observation 3: pre-ticked boxes for partners

o Roularta considers the use of pre-ticked boxes as consent

valid.

o OneTrust Consent Management Platform partner companies were

defined as "active" by default, but Roularta clarifies that this does not mean

that cookies have been installed by these partner companies. It was therefore not

not to consent to the placement of cookies, but to consent that a certain

number of partner companies have access to the data for one or more purposes. By

example, if the data subject does not accept advertising cookies, these

partner companies could not place advertising cookies.

o Roularta considers, in the light of the case law of the Court of Justice in the judgment

Planet49, that the practice whereby cookies from partner companies are

set by default to "active" constitutes valid consent within the meaning of the

articles 4.11 and 6.1.a of the GDPR.



o Roularta points out that they have moved to the Didoma Consent Management Platform in

March 2020, and that from now on, none of the partner companies is□

automatically set to "active" and the user always has to make a choice□

asset.□

▪ Observation 4: disclaimer for third-party cookies□

o Roularta declares that it is not responsible for the processing of cookies placed by□

third parties under the IAB TCF.□

o The defendant relies on the IAB Europe study for its argument:□

"Belgium's Data Protection Authority found IAB Europe's Transparency and□

Consent Framework does not meet several standards under the EU General Data□

Protection Regulation, TechCrunch reports. The DPA determined the framework□

fails to comply with the GDPR's principles of transparency, fairness and□

accountability. IAB Europe said in response it “respectfully disagree[s] with the□

[Belgian DPA]’s apparent interpretation of the law, pursuant to which IAB Europe is□

a data controller□

in the context of publishers’□

implementation of the TCF□

[Transparency & Consent Framework (TCF)”.□

o Next, the defendant indicates that, in the event that the ODA reaches□

a different conclusion, its practices nevertheless comply with Article 5.2 of the□

GDPR. The obligation of justification means "(I) the need for a person responsible for the□

processing to take appropriate and effective measures to implement□

data protection principles...”. No guidelines have been published□

by the DPA to clarify what is meant by minimum appropriate measures□

and efficient. Furthermore, Roularta has chosen to use the IAB Framework which is described□

as “the most sophisticated and scrutinized model of GDPR-compliance for□

digital advertising in the world”.□

o Roularta clarifies that this disclaimer was not intended to

disempower, but rather to indicate that it is not able to block the

cookies placed by third parties.

o Regarding elements II and III of Article 5.2 of the GDPR: “(ii) the need to

be able to demonstrate, upon request, that appropriate and effective measures have been

taken. The controller must therefore be able to provide proof

of item (i) above”.

The defending party admits that the mention of the cookie policy

that "Roularta Media Group is not responsible for the cookies placed and

managed by third parties, including those used to enable the sharing of information



via social networks" and that "Roularta Media Group has no control over

certain cookies used on its website" was worded in such a way

unfortunate. The defendant specifies that the intention was not so much to

transfer liability than to state that Roularta is not technically

capable of blocking cookies placed by certain third parties (in this case:

advertisers).

Advertisers and agencies can, when running a campaign

advertising on one of Roularta's sites, launch cookies or scripts through the

through this campaign which are not known in advance by Roularta.

Roularta states in its conclusions that the reference in the policy on

cookies in question have been deleted because, since the introduction of the IAB TCF

Framework, it can be assumed that IAB vendors will no longer place cookies or

scripts in accordance with this framework, unless consent has been obtained

for cookies and that the vendor in question has been approved in the list of

partner companies.

▪ Observation 5: incorrect and faulty information

With regard to the mention "...the lack of clarity of the policy in terms of

cookies regarding the need to use third-party cookies is due to

technical problems " :

o Position of Roularta: At the time of the finding by the DPA, this problem had already

been resolved, but it was still in the respect for life policy

private. When the cookie policy was updated on June 23

2020, this reference has been deleted. More specifically, the problem was that

Knack had been using a new registration system since November 2018.

This registration system used functional cookies so that

users do not have to identify themselves each time. Technically, this cookie

was a third-party cookie. There seemed to be an issue for users who

refused third-party cookies by default (they had to log in each time).

This issue was raised with the recording system provider in

to find a quick solution. A solution was sought, but this

turned out to be more difficult than expected. They had to find a way for the

people who only accept first-party cookies remain connected to the

website.

Regarding the mismatch of cookie names in the policy of

cookies, on the one hand, and categories of cookies in the configuration tool

cookies, on the other hand:

Decision on the merits 85/2022 - 14/58

o Position of Roularta

: Roularta had no choice but to use the

unclear wording used by the IAB TCF on its consent tool (under

penalty of exclusion from the TCF).

On the fact that the cookie policy does not contain

information about storage periods:

o See the statement of the defense on finding 6.

On the mention in the consent management tool concerning the use

of the “IAB Europe Transparency & Consent Framework”:

o The mention and brief explanation were for the sole purpose of creating transparency

and to inform the user of how Roularta intends to control

the use of cookies, i.e. by adhering to an internationally recognized standard

recognized in the world of digital advertising.

On the fact that the user of the website must consult the policy in terms of

cookies from 449 vendors in order to get an idea of what happens to its

data :

o An obligation imposed on it by the IAB TCF.

About not documenting cookies individually:

o Corrected in the meantime with an update to the cookie policy.

▪ Observation 6: unjustified cookie storage periods

o The defendant underlines here again the absence of precise directives

as to the lifespan of cookies.

o She argues that this makes it very difficult for companies (1) to understand

what is the lifespan when cookies "cannot be stored anymore

longer than the time required to achieve the intended objective" and (2)

to adapt their practices to comply with the ODA.

o The Inspection Service also incorrectly stated that no information on the

retention period of cookies could not be found in the policy of

protection of privacy (exhibit 8): “The retention period varies from cookie

cookies, in general cookies are stored until the user

delete cookies (...)". Paragraph 11 of the Privacy Policy

privacy (Exhibit 8) actually contains two types of information about the duration of

conservation of cookies: (i) the fact that the duration varies from one cookie to another; (ii) the

fact that the user can deactivate cookies, which entails a duration of

Decision on the merits 85/2022 - 15/58

zero retention (since cookies are not active). It is therefore incorrect

to state that Roularta has a shelf life which is in principle unlimited. He is

true that no concrete information could be found on the duration of

storage of cookies, but the Inspection Service goes too far in assimilating this

duration to an unlimited duration.

o The defendant also refers to a protection policy

of privacy adapted on June 23, 2020, where we now find a

detailed description of the retention period.

▪ Observation 7: Non-compliance with withdrawal of consent

o This was due to technical issues with the use of the cookie tool

OneTrust. The issue was resolved by implementing the Consent

Management Platform Didomi.

oh

Withdrawing should be as easy as giving consent: Roularta

provides a simple and easily accessible tool, without reducing the level of

service.

o Furthermore, Roularta cannot effectively remove a particular cookie from

device, this must be done by the person concerned.

o In summary, the consequence of withdrawing consent is: “the blocking and

subsequent deletion of cookies in the user's browser, plus

no data processing will take place”. Cookies will always be installed

on the user's device, but they will be inactive and no longer

functional.

15. On December 6, 2021, the defendant was informed that the hearing would take place on December 17

2021.

16. On December 17, 2021, the defendant is heard by the Litigation Chamber.

17. On December 23, 2021, the minutes of the hearing are sent to the members of the council of the

defendant.

18. On January 6, 2022, the Litigation Chamber received the Respondent's comments on

the minutes, which she included in her deliberations.

19. On April 20, 2022, the Litigation Chamber notified the defendant of its intention to

proceed with the imposition of an administrative fine, as well as the amount thereof, in order to give

the defending party the possibility of defending itself before the sanction is actually

imposed.

20. On May 11, 2022, the Litigation Chamber received the respondent's response to the

to impose an administrative fine, as well as the amount thereof.

Decision on the merits 85/2022 - 16/58

II. Motivation

II.1.

Competence of the Data Protection Authority

21. Pursuant to Article 4, §1 LCA, the Data Protection Authority “is responsible for the

control of compliance with the fundamental principles of personal data protection

personnel, within the framework of this law and the laws containing provisions relating to the

protection of the processing of personal data. » The wording of the explanatory memorandum

of the ACL demonstrates that DPA competence should be interpreted very broadly:

“The Data Protection Authority acts within the framework of legislation containing

provisions relating to the processing of personal data, such as, for

example, the law regulating a National Registry, the law establishing and organizing

of a Crossroads Bank for Social Security, the law creating a Bank-

Crossroads of Companies, etc. »10

It can be deduced from the foregoing that the intention of the legislator was to confer on the APDS a

general and horizontal competence for the protection of personal data.

The DPA therefore not only has supervisory powers with regard to the GDPR, but also

with respect to other legislation concerning the processing of personal data.

22. With regard to the use of cookies, reference should be made in this respect to the Directive

European 2002/58/EC of July 12, 2002 concerning the processing of personal data

personnel and the protection of privacy in the electronic communications sector

("ePrivacy Directive"), which has been partially transposed into Belgian law by the Law

Electronic communications

(LCE). Article 5, paragraph 3 of

the ePrivacy Directive is

particularly relevant here, as converted at the time in (former) Article 129 of the LCE (cf.

below). The first provision quoted reads as follows:

"Member States shall ensure that the storage of information or access to

information stored in the terminal equipment of a subscriber or user is not

permitted only on condition that the subscriber or user concerned has given his consent,

after having received clear and complete information in compliance with the Directive

95/46/EC, among others on the purposes of the processing. This provision does not preclude

to storage or technical access aimed exclusively at carrying out or facilitating the

transmission of a communication by

the way of a communications network

10 Belgian Chamber of Representatives, Draft law establishing the data protection authority, 23 August 2017, DOC

54 2648/001, 13.

electronic data, or, if strictly necessary, for the supply of a service of the company of

information expressly requested by the subscriber or user. »

23. With regard to the jurisdiction of the Litigation Chamber regarding the ePrivacy Directive and

the LCE, the Litigation Chamber refers to its previous decisions 12/2019 of December 17

2019, 19/2021 of February 12, 2021, 24/2021 of February 19, 2021 and 11/2022 of January 21, 2022.

24. The Litigation Chamber further emphasizes that, as an organ of the DPA, it is competent to

decide on the legal validity of personal data processing activities

pursuant to Article 4, §1 of the LCA, as well as Article 55 GDPR, and this in the light of Article 8 of

the Charter of Fundamental Rights of the European Union.

25. Furthermore, at the time of the findings of the Inspection Service, under Belgian law, the Belgian Institute of

posts and telecommunications (BIPT) was the competent authority for the law on communications

(ECL), including article 129 of this law, which implements article 5, paragraph 3, of the directive

ePrivacy. However,

the concept of consent under

the ePrivacy Directive is

inextricably linked to consent requirements under the GDPR, which has also been

clarified in consent guidelines by WP29 as the legal predecessor of the

European Data Protection Board (hereafter: “EDPS”).11

26. Furthermore, particular reference should be made in this regard to EDPS Opinion 5/2019 on the interaction

between the ePrivacy Directive and the General Data Protection Regulation, in which the

EDPS states:

“Data protection authorities are competent to enforce the GDPR.

The mere fact that a subsection of the processing falls within the scope of the

ePrivacy Directive does not limit the competence of data protection authorities in

GDPR”.12

27. In the aforementioned Opinion, the EDPS states that the provisions of the ePrivacy Directive “clarify and

effectively supplement the GDPR with regard to the processing of personal data

personnel in the electronic communications sector13, in order to ensure compliance with

Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Article 5, paragraph 3, of

the ePrivacy Directive is cited as an example of such a “specification provision”.14

11 EDPS, Guidelines 5/2020 on consent under Regulation 2016/679, 4 May 2020, among others paragraph 7.

12 EDPS Opinion 5/2019 on the interaction between the ePrivacy Directive and the General Data Protection Regulation, in parti

regarding the tasks and competences of data protection authorities, 12 March 2019, marginal no. 69.

13 Ibid, marginal no. 38.

14 Ibid, marginal no. 41.



28. The fact that the provisions of the ePrivacy Directive - as well as its transposition provisions -

should be considered as clarifying and supplementing the provisions of the GDPR is also

explicitly confirmed in the explanatory memorandum to the LCE bill:

“Section 2 of Chapter III of Title IV is mainly devoted to the transposition of the

Directive 2002/58/EC of 12 July 2002 of the European Parliament and of the Council concerning

the processing of personal data and the protection of privacy in the

electronic communications sector ("Privacy and Communications Directive

Electronic”, hereinafter “Privacy Directive” for short). The provisions of this section

establish in certain places a specific privacy protection regime, adapted

to the characteristics and needs of the electronic communications sector. In

other places, the provisions of this section should be considered as

supplementing the provisions of the law of 8 December 1992 relating to the protection of life

with regard to the processing of personal data (hereinafter "Privacy Law")

abbreviated). » 15(proper underscore)

29. In its Planet49 judgment, the Court of Justice also ruled that the collection of cookies is

assimilated to the processing of personal data.16The Court confirmed in the judgment

cited above that the purpose of Article 5, paragraph 3, of the ePrivacy Directive is to "protect the user against

an interference with his private life, whether or not it relates to personal data".17 In

Furthermore, the Court of Justice held that Article 5, paragraph 3, of the ePrivacy Directive must be interpreted

in light of the GDPR, and in particular Articles 4.11, 6.1.a) (consent requirement) and 13

GDPR (disclosures).

30. In this regard, the Litigation Chamber also highlights the proposed ePrivacy Regulation which

indicates that monitoring and compliance with the Regulation will be entrusted to the supervisory authorities

responsible for monitoring Regulation (EU) 2016/679.18

31. Finally, the Litigation Chamber recalls that since the entry into force of the law of 21 December 2021

transposing

the European Electronic Communications Code and amending various

electronic communications provisions on 10 January 2022, the DPA is now

competent under Belgian law to control the provisions relating to the placement and use of

cookies (i.e. "storing information or obtaining access to information already

stored in the terminal equipment of a subscriber or user"). The aforementioned law has

amended the ECA, among others. More specifically, article 256 of the law of December 21, 2021 provides

the repeal of article 129 LCE and the transfer of this provision to the law of July 30, 2018

15 Draft law on electronic communications, PC parl. Chamber, DOC 51 1425/001, p. 73. The present article 129 is the article

138 in the bill.

16 Planet49 judgment, § 45.

17 Planet49 judgment, § 45.

18 Article 18, Proposal for a Regulation of the European Parliament and of the Council on privacy and data protection

personal data in electronic communications and repealing Directive 2002/58/EC, COM/2017/010 final.

(LTD).19 Article 10/2 of the LTD will now read as follows:

“In application of article 125, § 1, 1°, of the law of June 13, 2005 relating to communications

electronically and without prejudice to the application of the regulations and this law, the storage

information or obtaining access to information already stored in the equipment

terminals of a subscriber or user is authorized only on condition that

:

1° the subscriber or user concerned receives, in accordance with the conditions laid down in the

regulation and in this law, clear and precise information concerning the objectives of the

treatment

and

his

rights

on

the

base

from

settlement

and

of

this

law

;

2° the subscriber or the end user has given his consent after having been informed

in accordance

to

1°.

Paragraph 1 does not apply to the technical recording of information or access to

information stored in the terminal equipment of a subscriber or an end user having

for the sole purpose of effecting the sending of a communication via a communications network

or to provide a service expressly requested by the subscriber or end user

when strictly necessary for this purpose. »

Since the DPA has the residual power to control the provisions of the LTD, this confirms the

material authority of the DPA regarding the placement and use of cookies.

32. However, the Litigation Chamber points out that, given the fact that this amendment dates

According to the conclusion of the arguments in this case, the legislative framework as it existed in the

time of (the opening of) the procedure before the DPA will continue to be taken into account in casu.

33. In all cases, the DPA is therefore competent - also in the legal situation that prevailed at the

time of the findings of the Inspection Service - to decide on the legal validity of a

consent given for the placement of cookies. In this sense, the DPA is also competent

to exercise its supervisory powers with respect to any other terms and conditions imposed

by the GDPR in activities involving the processing of personal data - such as

obligations of transparency and information (Article 12 et seq. GDPR).20

II.2. Introduction to the general principles of the use of cookies

19Law of 21 December 2021 transposing the European Electronic Communications Code and amending various

electronic communications provisions, M.B. 31 December 2021.

20 For a comparison of the scope of this supervisory power, see also the judgment of the Court of Justice of the EU of 15 June

2021, C-645/19, ECLI:EU:C:2021:483, paragraph 74.



34. Before addressing the conclusions contained in the investigation report, the Litigation Chamber

considers it useful to recall the general principles concerning the use of cookies and other means

tracing.21

35. The term “tracking means” includes cookies and HTTP variables, which can be placed

through web beacons or web pixels, flash cookies, access to information from

API (Local Area Network) terminal and information from APIs (LocalStorage, IndexedDB,

advertising identifiers like IDFA or Android ID, GPS access, etc.), or any other identifier

generated by software or an operating system (serial number, MAC address,

single terminal (UDI)), or a set of data used for a unique fingerprint of the terminal

(for example, via fingerprints).

36. Cookies and other means of tracking can be distinguished according to different criteria, such as

the purpose they serve, the area in which they are placed or their lifespan.

37. Cookies can be used for various purposes (for example, to support communication on

the network, for audience measurement, for marketing and/or behavioral advertising purposes,

authentication purposes, etc.).

38. They can be used, among other things, to support communication via the network (cookies of

connection), to measure the audience of a website (visitor number cookies, also

called “analytical cookies” or “statistical cookies”), for marketing and/or advertising based

on behavior, for authentication purposes, for website security, for the load

balancing, for customizing the user interface or to allow the use of a

media player (flash cookies).

39. Cookies can also be distinguished according to the domain by which they are placed on

your device. "First party" cookies are placed directly in the address bar of the

browser by the registered domain. In other words, these are cookies placed directly by

the owner of the website you are visiting. “Third party” cookies are placed by a domain

different from the domain you are visiting. This is the case when the website incorporates elements

from other websites, such as images, social media "plug-ins" (e.g.,

the Facebook "Like" button) or advertisements. When these elements are recovered by the

browser or other software from other websites, these websites may also place

cookies, which can then be read by the websites that placed them. These "third party cookies"

allow these third parties to track the behavior of Internet users over time and over many

websites and to create profiles of individuals based on this data (profiling), in order to

21 See also in this respect the thematic page of the website of the Data Protection Authority, available at the following address

: https://www.gegevensbeschermingsautoriteit.be/burger/thema-s/internet/cookies.



to be able, for example, to offer more precise and targeted marketing in the future during the

navigation of these Internet users thus followed.

40. Cookies can be distinguished according to their lifespan. In this context, a

distinction is made between “session cookies” and “persistent cookies”. Cookies from

session are automatically deleted when you close your browser, while

“persistent cookies” remain stored on your device (computer, smartphone, tablet, etc.)

until a predetermined expiry date (which can be expressed in minutes, days or years,

depending on the case).

41. Furthermore, from a legal point of view, a distinction must be made between, on the one hand, the means

of tracing that require the prior consent of the user and, on the other hand, those for

which consent is not required.

42. According to Article 129 of the LCE, there are two situations in which the prior consent of the

data subject is not required for placing or reading cookies:22

1) when the sole purpose of the cookie is to transmit a communication over a network

electronic communication (for example, cookies for load balancing); and

2) when the cookie is strictly necessary for the provision of an explicitly requested service

by the subscriber or end user (for example, cookies allowing the storage of the shopping cart

or cookies used to ensure the security of a banking application).

43. The installation of other cookies and means of tracking requires the prior consent of

the user, in accordance with article 129 of the ECA.

44. These include cookies or other means of tracking that allow the display of

(personalized) advertisements or regarding sharing functions on social networks. In

the absence of valid consent, these non-strictly necessary cookies cannot be

placed or read on the user's device.

45. The Litigation Chamber recalls that, to comply with the GDPR, said consent must be

informed, specific and free, and that the user must be able to withdraw it as easily as it was given

(see also below, title II.5.6).

22 Insofar as it is relevant, article 129 of the LCE reads as follows: “The storage of information or obtaining access to

information already stored in the terminal equipment of a subscriber or user is permitted only on condition

that [...] 2° the subscriber or the end user has given his consent after having been informed in accordance with 1°. The 1st parag

does not apply to the technical recording of information or access to information stored in the equipment

terminals of a subscriber or an end user whose sole purpose is to carry out the sending of a communication via a network of

electronic communications or to provide a service expressly requested by the subscriber or end user when this is

strictly necessary for this purpose”. (the Litigation Chamber emphasises)

Decision on the merits 85/2022 - 22/58

II.3.

As to the supposed absence of guidelines

46. In its response submission, the Respondent points out that cookie compliance is

a technical and complex subject that requires both technical and legal expertise. She does

argue that ODA would not have provided sufficient support to businesses to enable them

correctly apply the regulations in force.

47. More specifically, the defendant argues that, at the time of the findings of the Service

of Inspection in this file, the APD had not published guidelines on the use of cookies. This

contrary to the French supervisory authority (CNIL).

48. The Litigation Chamber recalls that at the level of the European Union, as well as at the Belgian level,

opinions and positions of the authorities already existed concerning cookies within the framework of the directive

ePrivacy many years before May 25, 2018.23 At European level, the Article

29 issued an opinion in 2012 on exceptions to consent to cookies.24 At the Belgian level, the

DPA's predecessor, the Commission for the Protection of Privacy ("CPVP"), has already published

guidelines on the use of cookies in 2015.25 In addition, at the time of the Service's findings

Inspection, there were, and still are, a large number of guidelines and advice directly

related to the situation of cookies in this case, such as the directives concerning a

legally valid consent.26

49. It is indeed true that the legal situation, as well as the technical possibilities with and for

cookies, have changed since the entry into force of the GDPR. The Litigation Chamber has already rendered its

first decision on cookies in 2019, which was also published on the website of the Authority of

Data Protection.27

50. Although the Litigation Chamber clearly recognizes that the EDPS and the DPA themselves have the

power, as a supervisory authority, to formulate and publish opinions and directives in

with regard to the protection of personal data, the Litigation Chamber emphasizes

however, that this falls within the range of tasks and powers of these institutions, and does not

does not constitute an obligation in itself.28 Indeed, authorities cannot be expected to

monitors that they take a proactive stance on every (changed) aspect of processing

7

via

June

available

2012, WP194,

23 In accordance with Article 99 of the GDPR, the Regulation has been in force since this date.

24 WP29, Opinion 04/2012 on Cookie Consent Exemption (“Opinion 4/2012 on the repeal of the consent requirement for

Cookies "),

https://ec.europa.eu/justice/article-29/documentation/opinion-

recommendation/files/2012/wp194_en.pdf.

25CPVP, Spontaneous recommendation on the use of cookies n° 01/2015.

26 At the time of the findings, the following guidelines, among others, were relevant: WP29, Guidelines on Consent under

of Regulation 2016/679, WP259 rev.01, as reiterated by the European Data Protection Board of May 25, 2018:

EDPS,

:

https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

27 Litigation Chamber Data Protection Authority, Decision 12/2019 of December 17, 2019, available via:

https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-12-2019.pdf.

28 Resp. Articles 70 (e) and 58 (3) (b) GDPR.

Endorsement

available

1/2018,

via

:



personal data in a digitized society, where the absence of such positioning

would prevent any application.

51. This is the reason why the European legislator has effectively chosen to base the

responsibility for the processing of personal data on the controller,

without reservation in

lack of clarity regarding certain technical situations.29 This

accountability for processing also includes demonstrating that data subjects

concerned have given legally valid consent, as well as the adequate follow-up of the

consequences of his dismissal, which is very relevant in this case.30

52. In the present case, it is the defendant, as manager of the websites in question, which

chooses a particular structure for the placement of cookies by a particular provider (choice

particular "means") in order, in particular, to obtain advertising revenue by this means (choice

of a certain “purpose”). Due to the defendant's choice of a particular management of

its websites, it is the complexity of the defendant's processing activities in themselves.

even that requires proper - and admittedly technically complex - examination and analysis

subsequent to a de facto situation. Thus, the alleged absence of concrete guidelines in the context

present cannot constitute a useful argument against a violation of the legislation on the protection

Datas.

II.4. Regarding the alleged inaccuracies during the investigation

53. The defendant first argues that the investigation by the Inspection Service was not

carried out according to the rules of the art. In summary, the defendant claims that:

-

there are discrepancies between the results obtained by the automated analysis and the analysis

cookie manual;

-

there is a lack of documentation on the classification of cookies by Onetrust and

Cookiebot;

-

-

unclear terminology is used in the investigation report;

unprofessional tooling is used.

54. Secondly, the defendant asserts that the Inspection Service used sources and

tools that are not official.

29 Articles 5, paragraph 2, 24 and 25 GDPR;

30 Compare for information: E.M. FRENZEL, “DS-GVO Art. 5. Grundsätze für die Verarbeitung personenbezogener Daten” in

Boris P Paal and Daniel Pauly (eds), Datenschutz-Grundverordenung Bundesdatenschutzgesetz (CH Beck 2021), (85)106, rn. 5

55. The Litigation Division firstly indicates that, in accordance with Article 72 LCA, the inspector
general and the inspectors can “carry out any investigation, any control and any hearing, as well as
that collect any information they consider useful in order to ensure that the fundamental principles
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
staff, are effectively respected".
56. Article 67 LCA stipulates that “Investigation measures may give rise to a report of
statement of offence. This report has probative force until proven otherwise. The service
Inspection carried out several investigative operations, the results of which it recorded in detail in
reports.
57. The findings of the Inspection Service are administrative acts subject to the substantial obligation
reasons and, for this reason, must be supported by "reasons acceptable in law and in
made and which must therefore be verifiable. 31 As part of the substantial obligation to state reasons,
on the other hand, it is not required that these grounds be explicitly mentioned in the act
administrative itself. In other words, it is not required that the Inspection Service justify
formally all aspects - for example by describing in detail the language of
programming used and with which it deploys survey tools, technical terminology, etc. -
of his findings.
58. It is only in the context of “decisions of individual scope”, such as this one by the Chamber
litigation, that the legal and factual considerations underlying the decision must
be (explicitly) set out in the decision itself, and in an adequate manner.32 The
the Belgian legislator has moreover explicitly limited the control of the investigative acts of the Service
Inspection, leaving it to the Inspector General and his inspectors to ensure "that the means
they employ are appropriate and necessary. (art. 64, §2 LCA). It therefore does not belong to the
Litigation Chamber to control the choices made for certain means of investigation, when they
apparently fall within the remit of the Inspection Service, and when the principles of good

general administration were apparently respected.33

59. Regarding discrepancies between manual and automated cookie analysis

relied on by the defendant, the Litigation Chamber emphasizes that the differences

mentioned above are explained by the fact that, in the case of manual analysis, either processing

were done manually, or “maximum” consent was granted

in the cookie banner, which resulted in the placement of additional cookies. Nevertheless,

31 I. Opdebeek & S. De Somer, Algemeen Bestuursrecht (2nd edition), 2019, 435, par. 944.

32 Article 3 Law of 29 July 1991 relating to the explicit justification of administrative acts, see also the judgment of the Court of A

Brussels (Cour des Marchés section) of October 9, 2019, 2019/AR/1006: "The main reason for the obligation to state reasons [..

is that the person concerned must be able to find in the decision which concerns him the reasons for which it was taken [...]".

33 See also, mutatis mutandis, the judgment of the Brussels Court of Appeal (Cour des Marchés section) of 7 July 2021, 2021/A

21: “It [the Court of Markets] is not competent to rule on the decisions taken by the Inspection Service [...]”.



this is not possible with automated cookie analysis - performed via Website Evidence

Collector (WEC) - which cannot grant consent and through which, therefore,

only cookies that have been placed without consent are detected.

60. It should also be noted in this respect that this was expressly stated in the report

of technical investigation drawn up by the Inspection Service.34

61. With regard to cookies placed without consent, it should be noted that the different

methods actually produced virtually the same results.

62. In this respect, it should also be pointed out that it is in no way technically possible to

detect cookies that have not been placed. If the detection of cookies had been carried out from

negligent manner - quod non - this could only have resulted in cookies

actually placed are not detected by the tool, which could therefore only have benefited the

defendant.

63. In addition, the Litigation Division points out that, with regard to the argument of the party

defendant that it is not possible to check whether the cache memory has been emptied or not and

whether or not temporary internet files were present during the investigation, this cannot be

relevant only for manual survey via Cookie Manager, but does not apply to survey

automatically via the WEC (which always starts the investigation as if the browser had not

yet been manipulated in any way in this sense). Always during this last

automatic investigation, cookies that were not strictly necessary were detected on

websites reviewed.

64. With regard to the argument raised by the Respondent concerning the alleged lack of

professionalism of the tools used, in particular the Website Evidence Collector, the Chamber

litigation recalls first of all that, in accordance with article 64, §2 LCA, the inspector general and

inspectors, when exercising the powers referred to in Chapter 6, ensure that the tools they

use are appropriate and necessary. This is the case whether the tool used is ad hoc software or

no, a beta version or not.

65. Furthermore, it should be noted that the changes made to the WEC tool between versions 0.3.1

and 1.0.0 only concern "features" and "bug fixes", i.e. improvements to the

benefit of the researcher, so that the tool does not crash, freeze or generate messages

of error. In other words, if the WEC version 0.3.1 has detected a cookie, it means that the tool has

worked. It is indeed impossible for such an instrument to accidentally detect a cookie

non-existent due to a malfunction.

34 See for example the Knack website technical investigation report, p. 4 (“3. Analysis”): “First of all, all websites, including

that of “Knack”, were examined automatically by the WEC. Thereafter, the different choices presented, provided by the website

concerning cookies, have been manually tracked from “minimum” consent to “maximum” consent (...)”.



66. Finally, the Litigation Chamber emphasizes that the defendant does not demonstrate in any way

that it is able, as data controller, to make a complete inventory of the

placed cookies. At no time during the proceedings did the defendant present its own

inventory of cookies used on the websites concerned. On the contrary, the defendant has

argues at the hearing that the IAB is in a dominant position and that its requirements are therefore

imposed, so to speak, and that the publishers are not able to control all these cookies.

The defendant added during the hearing that the inventory of cookies should ideally

be done several times a day as the situation is constantly changing. However, the fact that a

supplier is in a dominant position - for example, a monopolistic position or

oligopolistic in the online advertising market - cannot, in itself, free the person responsible for the

dealing with its responsibilities.

II.4.

The IAB Transparency and Consent Framework ("IAB TCF")

67. The Litigation Chamber refers to its decision 21/2022 of February 2, 2022.35

68. The Litigation Chamber stated in this decision: "IAB Europe is a federation which

represented

the sector of

digital advertising and marketing at the level

European. It includes both corporate members and national associations, with

members of their own company. Indirectly, IAB Europe represents approximately 5,000

companies,

including both large companies and national members"36.

69. IAB Europe itself described its operation as follows: "In its current form, the TCF is

a

standard

of

good

practice

intersectoral

who

makes it easier for the digital advertising industry to comply with certain

regulations

european

in respect of privacy and data protection and to give individuals more

transparency and control over their personal data. This is in particular a "framework"

in which companies operate independently and which helps them to comply with the basic

of the GDPR for the processing of personal data and the ePrivacy directive,

which requires that

the user gives consent for

storage and

the access to

information about a user's device. »37

35 Available at: https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-21-2022.pdf.

36 Ibid, para. 36.

37 Ibid., para. 39.

Decision on the merits 85/2022 - 27/58

70. In the conclusion to the Response and during the Hearing, the Respondent stated that it

can only allow advertisements on its website if they comply with the IAB TCF.

71. The Litigation Chamber first notes that the defendant does not provide any evidence

evidence to support the argument set out above. The Litigation Chamber finds

also that the operators of websites of other media and similar media do not use

not the IAB TCF. In any case, the defending party is not obliged to use the TCF of

the IAB.

72. The Litigation Chamber recalls that the defendant, as manager of the sites

Internet in question and as controller within the meaning of Article 4(7) of the GDPR

personal data of users of said websites on the basis of the duty of

responsibility provided for in Article 5, paragraph 2 j° 24, of the GDPR, is responsible for compliance with the provisions

of the GDPR for the processing in question and the provision of proof thereof.

II.5.

Violations noted

II.5.1. Lack of valid consent (Article 6, paragraph 1, point a) of the GDPR j°,

article 129 LCE).

II.5.1.1.

The placement of cookies that are not strictly necessary before

obtaining consent - finding 1 Service Inspection

73. Article 6, paragraph 1 of the GDPR stipulates that the processing of personal data is only lawful

if it is based on one of the grounds for processing referred to in this provision.

74. With regard to the processing of personal data through the placement of cookies,

Art. 6 para. 1 GDPR should be read in conjunction with (former) Art. 129 ECA

(currently article 10/2 of the LTD), because this article clarifies and complements the provisions of the GDPR.38

75. The aforementioned article therefore stipulates that

installation and/or

the

reading cookies requires

the

consent of the data subject, unless cookies are strictly necessary for 1)

carry out the transmission of a communication via an electronic communications network or

2) provide a service explicitly requested by the user.

76. In its Planet judgment49, the Court of Justice ruled that the term “consent” appearing in Article

5, paragraph 3, of Directive 2002/58 (transposition into Belgian law via former article 129 LCE, now

Article 10/2 LTD) refers to “consent of a data subject” as defined and

specified in Directive 95/46 (i.e. the legal predecessor of the GDPR).39 The EDPS indicates

38 EDPS Opinion 5/2019 on the interaction between the ePrivacy Directive and the General Data Protection Regulation, in parti

regarding the tasks and powers of data protection authorities, 12 March 2019, marginal no. 38.

39 Judgment of the Court of Justice of 1 October 2019, C-673/17, ECLI:EU:C:2019:801, Planet49, paragraph 50.



in this respect in its Directives 05/2020 of May 4, 2020 on consent: “The EDPB notes

that the requirements for consent under the GDPR are not considered to be an ‘additional

obligation’, but rather as preconditions for lawful processing. Therefore, the GDPR conditions for

obtaining valid consent are applicable in situations falling within the scope of the e-Privacy

Directive”.40

77. The Litigation Chamber recalls that Article 4, point 11 GDPR defines valid “consent”

as follows: "any expression of will freely consented, specific, informed and not

ambiguous

by

which

the data subject accepts, by a declaration or by a clear positive act, that data to be

personal character concerning him or her are the subject of processing".

78. The technical analyzes of the Inspection Service show that cookies were installed before

to request the consent of the interested party (66 cookies for the Knack website and 60 cookies

for Le Vif website). These include third-party cookies (48 for the Knack site and 44 for the

Vivid). Although in principle it cannot be excluded that third-party cookies are also strictly

necessary for the operation of the website, the legal distinction with a first party may

be a parameter in the evaluation of the strictly necessary character of a cookie.41 In addition, the

defendant does not demonstrate at all that these cookies are strictly necessary.

79. In this regard, the Litigation Chamber refers to Opinion No. 10/2012 of the former Commission of the

Protection of Privacy (predecessor of the ODA) on the bill containing various provisions

relating to electronic communication. She indicated that the cookies exempted from the obligation to

consent are mainly certain "first party cookies". The Commission pointed out that it

in this case, these are cookies placed by the user himself, which memorize, among other things, the

language settings and personal proposals in an online store (for example,

customer identification and the virtual basket). 42 In addition, the aforementioned notice indicates that some cookies do not

are clearly not covered by the disclosure exemption. These are the forms of

most intrusive and recent cookies (such as "supercookies" or "evercookies").

The Commission has indicated that these are mainly "third party" cookies on which the

different responsible parties give very little or no information, and who

require special expertise and software to be able to remove them.43 In this opinion, it was

40 EDPS, Guidelines 05/2020 on Consent under Regulation 2016/679, 4 May 2020, p. 6 (No. 7). Free translation: “The EDPS n

GDPR consent requirements should not be viewed as an “additional obligation”, but

rather as conditions for lawful processing. GDPR requirements for obtaining valid consent

therefore apply in situations falling within the scope of the ePrivacy Directive. »

41 Compare: WP29, Opinion 04/2012 on Cookie Consent Exemption, 7 June 2012, p. 5: “[…]’third party’ cookies are usually not

necessary’ to the user visiting a website since these cookies are usually related to a service that is distinct from the one that has

‘explicitly requested’ by the user.” ; free translation by the Litigation Chamber: “third-party cookies are generally not

strictly necessary for the user who visits a website because these cookies are generally linked to a separate service from the on

been explicitly requested by the user. »

42 Opinion No. 10/2012 of March 21, 2012 on the bill containing various provisions relating to electronic communications (CO-

A-2012-009), § 51.

43 Opinion No. 10/2012, § 52.



also clearly asked the legislator to provide additional clarifications to

Article 129 of the LCE on the types of cookies that specifically require consent. 44

The legislator did not provide any details on this subject.

80. The Article 29 Data Protection Working Party stated in its opinion 04/2012 on the exemption from the obligation of consent for cookies that: "third-party cookies", moreover, are only generally not "strictly necessary" to visit the website, as these cookies are generally linked to a service other than that which the user has “expressly requested”.45 The Data Protection Group Article 29 indicates "that it must be determined according to the purpose, the specific implementation or specific processing whether or not a cookie can be exempted of the obligation of consent”.

81. Consent must in principle be obtained for all cookies, unless the cookies are "functional" or "strictly necessary", according to the criteria set out in article 129 LCE (see above). It is up to the defending party, in accordance with its duty of responsibility, to prove that the cookies are strictly necessary and that, for this reason, the consent is not required.

82. The Inspection Service's investigation report shows that only two cookies were judged strictly necessary on the Knack and Le Vif websites. Only these two cookies should therefore, in principle, be placed without the consent of the person concerned. In this regard, the House litigation reiterates that the defendant does not advance any argument to justify that the other cookies detected by the Inspection Service are (also) considered as strictly necessary.

83. For the description of "strictly necessary cookies", the Inspection Service relied on a definition included on the website www.gdpr.eu46, which defines strictly necessary cookies as following :

“Strictly necessary cookies - These cookies are essential for you to browse the website and use its features, such as accessing secure areas of the site. Cookies that allow web shops to hold your items in your cart while you are shopping online are an example of strictly necessary cookies. These cookies will generally be first-party session cookies. While it is

not required to obtain consent for these cookies, what they do and why they are necessary□

should□

be□

explained□

to□

tea□

user”.□

(eigen□

onderlijning)□

In English: "Strictly Necessary Cookies - These cookies are essential for you to□

44 Opinion No. 10/2012, § 64.□

45 Data Protection Group Article 29, Opinion No. 04/2012 on the removal of the consent requirement for cookies,□

p.60.□

46 A website funded by the EU under the Horizon 2020 Framework Programme.□



can surf the website and use its features, such as visiting areas□

site security. Cookies that allow online shops to put items□

in the shopping cart during online shopping are examples of cookies strictly□

required. These cookies will generally be first party cookies. Although he does□

is not necessary to obtain consent for these cookies, you must explain to□

user what they do and why they are needed. (free translation and underlining□

by the Litigation Chamber)□

The Litigation Chamber points out that the above definition was used to clarify the□

findings of the Inspection Service. The same can be inferred in se from the statutory provision□

strictly speaking, article 129 LCE.□

84. For the Knack and Le Vif sites, two cookies have been deemed strictly necessary:□

Sightings□

knock□

OptanonConsent□

OptanonConsent□

PHPSESSID□

PHPSESSID□

In order to classify the different cookies, the Inspection Service took into account the information□

related to the specific cookie on the website, cookiebot report or manual survey.47□

85. The Litigation Chamber points out that the Respondent itself indicates in its□

answer conclusion that due to a lack of technical knowledge, the cookie tool□

OneTrust used at the time was implemented in a flawed way. The defendant□

adds the cookies that would have been placed. During the hearing of the defendant, it is□

also appeared that it admits that non-strictly necessary cookies have□

actually placed without obtaining the consent of the persons concerned.□

86. Based on the foregoing, the Litigation Division finds that the Respondent has violated□

Article 6, paragraph 1, point a) of the GDPR j° article 129 LCE.□

II.5.1.2. Placement of statistical cookies without consent - finding 2□

Inspection Service□

87. The technical analysis report of the Inspection Service demonstrates that statistical cookies are□

placed before obtaining consent. The cookie setting tool used by the party□

47 For the classification of the different cookies, see p. 15-29 in Knack's technical report.□



defendant at the time demonstrates that statistical cookies are always configured as□

active and cannot be disabled.□

88. The Litigation Chamber wishes to specify that under article 129 LCE, which is a complement and□

a clarification of the provisions of the GDPR, it turns out that the placing and/or reading of cookies□

requires the consent of the data subject, unless the cookies are strictly

necessary to carry out the transmission of a communication via a communications network

electronically or provide a service explicitly requested by

the user. Bedroom

litigation will clarify its position regarding the placement of statistical cookies below.

89. In substantive decision 12/2019, the Litigation Chamber defined statistical cookies

as "the collection of information about the technical data of the exchange or the use of the

website (pages visited, average duration of visit, etc.) in order to improve its functioning

[i.e. to know the use of the website]. The data thus collected by the site are in

principle aggregated and processed anonymously, but may also be processed to other

purposes".48

In the case in question, statistical cookies were also placed without the consent

prior to the data subject. The Litigation Chamber then ruled "that in the current state of the

law, there is no consent exception for "first-party analytical cookies".

party", so that the consent prior to the placement of such cookies is effectively

required".49 In its decision on the merits 12/2019, the Litigation Chamber also

referred in this respect to an opinion of the predecessor of the DPA (CPVP) according to which "it is up to the

legislator to clarify the issue of the non-exemption of user consent in the

framework of origin analysis cookies".

According to the Litigation Chamber, the placement of "first-party statistical cookies" does not

nor could it be based on the legitimate interest of the owner of the website, taking into account the

reading of article 5, paragraph 3, of the ePrivacy directive.

90. Still at European level, the Article 29 Working Party has already taken a position on the obligation to

consent for statistical cookies in 2012. It is clear that Task Force 29 considers

that "first party analytical cookies" are not exempt from the requirement of

consent as they are not strictly necessary to provide a function explicitly

requested by the user or subscriber. Indeed, according to the Article 29 Working Party, the user

can access all the functions offered by the website without any problem, even when these

cookies are disabled.50 He then added that “first-party analytical cookies are

48 DPA, Decision on the merits 12/2019 of 17 December 2019, p. 31.

49 DPA, Decision on the merits 12/2019 of 17 December 2019, p. 31.

50 Data Protection Group Article 29, Opinion 04/2012 on the exemption from the requirement of consent for cookies, 7 June

2012, 00879/12/NL, p. 11.



however unlikely to pose a privacy risk if strictly

limited to aggregate statistics for the website operator and used by websites that

already provide clear information about these cookies in their privacy policy

privacy and provide appropriate privacy safeguards.”51 The Group

Article 29 adds: "In the event of a revision of Article 5, paragraph 3, of Directive 2002/58/EC, it

agrees that the European legislator considers adding a third exemption criterion for

cookies strictly limited to first party cookies for anonymous statistical purposes and

aggregated”.

91. In summary, in its decision on the merits 12/2019, the DPA considered that the placement of "cookies

first-party analytics” requires, in principle, the prior consent of the person

concerned.

92. In its defence, the defendant states that statistical cookies are installed in the

sole purpose of collecting basic aggregate statistics on the use of its websites. In his

cookie policy, it also stated the following about statistical cookies

:

“Analytical and statistical cookies are always downloaded, they are used to have

a completely anonymous overview of how the website is used and which pages are visited with

frequency. This information is necessary, among other things, for the Internet study of the CIM and

are used for traffic and profile analysis so that we can tailor our work

even more closely to your needs. »52

93. The Litigation Chamber recalls that

when statistical cookies are placed on

the terminal equipment of an Internet user, it will always be possible to identify them by means of addresses

IP and other identifiers.53 Indeed, in its consistent case law, the Court of Justice has always

used a very broad definition of both “personal data” and the concept

"identifiability". She indicated that "as soon as information can, because of its content,

its purpose or its effects, be linked to a natural person identified or identifiable by

means that can reasonably be used54, that the information from which the person

51However, it should be noted that the process of data aggregation may in itself constitute data processing to

personal character which must comply with data protection legislation, regardless of whether this process

actually leads to statistical data, see also recital 162 of the GDPR: "[...] The statistical purpose implies

that the result of the processing for statistical purposes does not consist of personal data, but of aggregated data

[...]” (proper underscore)

52 Exhibit 15 of the defendant's book of exhibits.

53 See Recital 30 GDPR; Article 4, point 1 of the GDPR also explicitly mentions "an online identifier".

54 Judgment of the CJEU C-434/16 of 20 December 2017, Nowak t. Data Protection Commissioner, ECLI:EU:C:2017:994,

paragraph 35.



data subject can be identified either wholly owned by the same controller or

partly by another entity, it should be considered as personal data”.55

94. Based on the technical report of the Service Inspection for the Knack website (p. 15-29), the

Litigation Chamber found that for most statistical cookies, the manager of the

website has either a unique identification number or an IP address when reading

Cookies. It makes sense, because it's the only way for the website to know how many times it is visited.

by the same user.

95. With regard to the IP address, the Litigation Chamber states that it is clear that it can

enable a natural person to be identified. An IP address has already been recognized by the Court of

Justice as personal data under the GDPR.56 Since the installation

and the reading of a statistical cookie on the user's terminal equipment also provide

to the website operator the IP address, it is also possible for the controller

to identify the user. It is therefore the processing of information of an identifiable person (for example

an online identifier, cf. art. 4, point 1) GDPR).

96. With regard to the registration of a unique identification number, the Litigation Chamber

refers to substantive decision 12/2019 where a position has already been taken on the qualification of a

unique identification number. In this case, the Litigation Chamber ruled that the awarding of a

unique identification number is a form of pseudonymisation within the meaning of Article 4(5) of the

GDPR.57 The Article 29 Data Protection Group has also already expressed an opinion on the

meaning of the notion of “pseudonymised data”.58 He specifies that pseudonymisation

is to hide a

identify. The identity of individuals may be concealed by

the

pseudonymization in such a way that re-identification becomes impossible, for example by a

one-way encryption, resulting in in se anonymized data.59 The data

traceable pseudonymized information can be considered information about a person

indirectly identifiable and are therefore personal data within the meaning of the GDPR.60 If the

data can be traced back to the person concerned by using a pseudonym,

55 Judgment of the CJEU C-582/14 of October 19, 2016, Patrick Breyer t. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, p

Judgment C-434/16 of December 20, 2017, Nowak t. Data Protection Commissioner, ECLI:EU:C:2017:994, para. 31: see also F

ZUIDERVEEN BORGESIUS, “Singling out people without knowing their names – Behavioral targeting, pseudonymous data, and

Data Protection regulation”, Computer Law & Security Review, vol. 32-2, 2016, p. 256-271; and FR. ZUIDERVEEN BORGESIUS

Breyer Case of the CJEU – IP Addresses and the Personal Data Definition", EDPL, 1/2017, pp. 130-137.

56 Judgment of the CJEU C-582/14 of October 19, 2016, Patrick Breyer t. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, p

57 According to Article 4.1.5. GDPR, "pseudonymisation" is defined as "the processing of personal data of

such that they can no longer be assigned to a specific data subject without recourse to information

additional information, provided that this additional information is kept separately and subject to measures

technical and organizational to ensure that personal data is not assigned to a person

identified or identifiable physical".

58Data Protection Group Article 29, Opinion 4/2007 on

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_nl.pdf.

59 Ibid., p. 18-19.

60 Ibid., p. 19.

the concept of personal data,

Decision on the merits 85/2022 - 34/58

so that his identity can be established, data protection rules apply.61

based on the constant case law of the Court of Justice, the Litigation Chamber notes that it is

possible to identify a data subject by combining the unique identification number with

other information obtained or not obtained from third parties.62 In this case, the identification number

unique must be considered as personal data within the meaning of the GDPR.

97. Given the above findings and the broad interpretation of the notion of data

of a personal nature, as confirmed by the case law of the Court of Justice of the EU, the

Litigation Chamber concludes that, with regard to statistical cookies (where the IP address of a

user is also always available), prior consent is indeed required

pursuant to Article 6, paragraph 1, point a) of the GDPR in conjunction with the national implementation of Article

5, paragraph 3, of the ePrivacy Directive. This is effectively the processing of information from a

identifiable natural person, so the rules of the GDPR undoubtedly apply. absence

of such consent on the defendant's website for statistical cookies

identified by the Inspection Service therefore constitutes a violation of Article 6, paragraph 1, point a), juncto

Article 129 of the ECA.

II.5.2. Pre-ticked boxes for partners (Articles 4, point 11), 6, paragraph 1, point a)

and 7, paragraph 1 GDPR) - finding 3 Inspection Service

Inspection Service findings:

98. The Inspection report shows that for Knack and Le Vif, 449 "partners" or "vendors"

receive consent by default through pre-ticked boxes. This also emerges from

screenshots of websites featured in Knack and Le Vif technical reports:

61 The Court of Justice stated in the Breyer judgment that "in order to determine whether a person is identifiable, it is necessary

account of all the means likely to be reasonably used, either by the controller or by any other

person, to identify that person" (§42).

62 Judgment of the CJEU C-582/14 of October 19, 2016, Patrick Breyer t. Bundesrepublik Deutschland, ECLI:EU:C:2016:779, p



99. The Inspection Service asserts that the GDPR requires an "unequivocal declaration or active act"

(Article 4, point 11) GDPR), which means that any presumed consent based on a mode of action

more implicit on the part of the data subject does not comply with the standards of consent

of the GDPR. The Inspection Service relies on the Planet49 judgment, which specified that Article 2, point f)

(definition of consent) and article 5, paragraph 3 (consent to cookies) of the directive

ePrivacy should be read in conjunction with Article 4(11) and Article 6(1)(a) of the

GDPR. The Court of Justice then ruled that the consent was not validly given when

the storage of information by means of cookies or the access to information already stored on

the user's terminal device of the website through cookies is enabled by means of boxes

selection checked by default that the user must uncheck if he refuses to give his

consent. The Inspection Service also finds that the defendant did not respect

nor the obligation provided for in Article 7, paragraph 1 of the GDPR which requires him to prove that the person

data subject has given consent to the placement of cookies which are not strictly

required.

Defendant's position:

100. The defendant argues that the Inspection Service's third finding is incorrect. She

admits that the partner companies of the OneTrust Consent Management Platform were

defined as "active" by default, but that this did not mean that cookies were

automatically installed by these third-party partner companies. According to the defendant, it

was not actually a question of consenting to the placement of cookies, but rather of indicating which

IAB vendors could use a consent for one or more purposes, provided that this



consent is given. This would only be the case if the data subject accepts cookies

corresponding in the cookie management tool. The defendant therefore considers, in the light

of the case law of the Court of Justice in the Planet judgment49, that the practice according to which

cookies from partner companies are set by default to "active" constitutes a

valid consent within the meaning of Articles 4.11 and 6.1.a of the GDPR.

101. The Litigation Chamber notes that the Respondent indicates in its submissions that it has

adjusted its practice regarding this aspect by implementing a new Didomi Consent

Management Platform in March 2020. Currently, none of the partner companies are

automatically set to "active" and the user must now make an active choice.

Position of the Litigation Chamber:

102. In this section, the Litigation Division will address the criteria for valid consent.

Article 4(11) GDPR defines the "consent" of the data subject as "any

expression of free, specific, informed and unambiguous will by which the data subject

accepts, by a declaration or by a clear positive act, that personal data the

concerning are subject to processing".

103. Article 7 GDPR contains the conditions applicable to consent:

1. In cases where processing is based on consent, the controller

is able to demonstrate that the data subject has given consent to the□

processing of personal data concerning him.□

2. If the consent of the data subject is given in the context of a declaration□

in writing which also concerns other matters, the request for consent is□

presented in a form which clearly distinguishes it from these other matters, in a□

comprehensible and easily accessible form, and formulated in clear and simple terms.□

No part of this statement that constitutes a violation of these rules is□

binding.□

3. The data subject has the right to withdraw consent at any time. Withdrawal□

of consent does not compromise the lawfulness of processing based on consent□

made before this withdrawal. The person concerned is informed of this before giving his□

consent. Withdrawing is as easy as giving consent.□

4. When determining whether consent is freely given, consideration should be given to□

greater account of the question of knowing, inter alia, whether the performance of a contract,□

including the provision of a service, is subject to consent to the processing of□

personal data which is not necessary for the performance of this contract.□

Decision on the merits 85/2022 - 37/58□

104. Furthermore, Article 5, paragraph 3 of the ePrivacy Directive, as transposed by Article 129 of the LCE□

at the time of the investigation by the Inspection Service, lays down the condition that the user "has given his□

consent" for the placement and consultation of cookies on its terminal equipment,□

except for the technical recording of information or the provision of a service□

expressly requested by the subscriber or end user and when the placement of a cookie is□

strictly necessary for this purpose.□

105. Recital 17 of the ePrivacy Directive specifies that for the application of this directive, the notion□

of "consent" shall have the same meaning as "consent of the person□

data subject", as defined and specified in the GDPR.63□

106. In the Planet judgment49, the Court of Justice of the European Union clarified the requirement of consent for the placement of cookies following the entry into force of the GDPR. She indicated that explicit active consent is required: “active consent” is therefore indisputably required according to the correct interpretation of the GDPR.64 Indeed, recital 32 indicates that: “Consent should be given by a clear affirmative act by which the data subject expresses in a free, specific, informed and unequivocal manner its agreement to the processing of personal data relating to him, for example by means of a written declaration, including electronically, or an oral statement. This could be done in particular by ticking a box when consulting a website, by opting for certain parameters techniques for information society services or by means of another declaration or other behavior which clearly indicates in this context that the data subject agrees to the proposed processing of his personal data. There can therefore be no have consent in case of silence, boxes checked by default or inactivity. the consent given should apply to all processing activities having the same purposes. Where the processing serves more than one purpose, consent should be given for all of them. If the consent of the data subject is given following of a request submitted electronically, this request must be clear and concise and not must not unnecessarily disrupt the use of the service for which it is granted. " (bedroom underlines).

107. On the basis of these considerations, the Litigation Division finds that the consent referred to in articles 2, point f) and 5, paragraph 3 of Directive 2002/58, transposed in article 129 of the LCE at the time of the findings, read in conjunction with Articles 4, paragraph 11 and 6, paragraph 1 point a) of the GDPR, is not not validly given by a box checked by default that the user must uncheck to refuse to give consent (in this case, it is therefore a question of giving consent to the partners

63 The GDPR replacing Directive 95/46/EC.

64 Judgment of the Court of Justice of 1 October 2019, C-673/17, ECLI:EU:C:2019:801, Planet49, paragraph 73.

for one or more purposes for which consent must be given in another

window).65

108. In concrete terms, this means that the data subject must receive information about the

how to express your wishes in terms of cookies, and on how to accept "all

cookies", "some cookies" or "no cookies".

109. For example, the confirmation of a purchase or the acceptance of the general conditions is not sufficient to

assume that consent to placing or reading cookies has been validly given.

Nor can consent be given for the sole "use" of cookies, without further

precision as to the data collected via these cookies or as to the purposes for which these

data is collected. The GDPR requires, in fact, a more detailed choice than a simple "all or

nothing", but it does not require consent for each cookie individually. If the

operator of a website or mobile application requests consent for various

types of cookies, the user should have the choice to give (or refuse) consent for

each type of cookie, or even, in a second layer of information with choices, for

each cookie separately.

110. By the use of pre-ticked boxes, as set out by the Inspection Service in its reports,

the defendant violates articles 4, point 11 j° 6, paragraph 1, point a) and 7, paragraph 1 GDPR, as

explained in recital 32 of the GDPR

II.5.3. Disclaimer for third-party cookies (potential violation of

articles 5, paragraph 2 and 7, paragraph 1 of the GDPR) - finding 4 Inspection Service.

Inspection Service finding:

111. According to the Inspection Service, the defendant is trying to absolve itself of the liability of the

third-party cookies placed when visiting the Knack and Le Vif sites.

112. For example, the cookie policy states that the defending party is not

responsible for cookies placed and managed by third parties, for example, to allow sharing

information through social networks. The defendant also asserts that it has no

control over certain cookies used on its website.

113. With regard to this aspect, the Inspection Service refers to the Wirtschaftsakademie judgment of the

Court of Justice in which it was held that the owner of a website is responsible for the

processing of cookies installed or read from its website.66 At the very least, it participates in the

definition of the purposes and means of processing visitors' personal data

65This is also linked to the specificity requirement of consent, cf. EDPS, Guidelines 05/2020 on consent under the

Regulation 2016/679, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_nl.pdf, § 50.

66 Judgment of the Court of Justice of 5 June 2018, C-210/16, ECLI:EU:C:2018:388, Wirtschaftsakademie, in particular para. 39



of its website by authorizing third-party applications on its website or the distribution of content

third parties in the advertising spaces of its website.

114. Next, the Inspection Service refers to the principle of responsibility of Article 5, paragraph 2 of the GDPR,

according to which the controller is responsible for ensuring compliance with the principles relating to the

processing of personal data and must be able to demonstrate compliance with

these principles.

115. This practice used by the defendant must also, as mentioned above, be

considered a violation of Article 7, paragraph 1 of the GDPR, because a data controller

must demonstrate that the data subject has given consent for the placement of cookies

that are not strictly necessary from its website.

Defendant's position:

116. The defending party declares that it is not responsible for the processing of cookies placed by

third parties under the IAB TCF.

According to the respondent, this interpretation was also confirmed by the DPA in the

framework of the ongoing IAB Europe investigation: "Belgium's Data Protection Authority found IAB Europe's

Transparency and Consent Framework does not meet several standards under the EU General Data

Protection Regulation, TechCrunch reports. The DPA determined the framework fails to comply
with the GDPR's principles of transparency, fairness and accountability. IAB Europe said in
response it respectfully disagree[s] with the [Belgian DPA]'s apparent interpretation of the law,
pursuant to which IAB Europe is a data controller in the context of publishers' implementation of
the TCF".

117. Next, the Respondent indicates that, in the event that the Litigation Chamber arrives
to a different conclusion, its practices nevertheless comply with Article 5, paragraph 2 of the GDPR.
The obligation of justification means "(I) the need for a data controller to take
appropriate and effective measures to implement the principles of data protection
data."67 No guidelines have been issued by the APD to clarify what is meant by a
minimum of appropriate and effective measures. Furthermore, Roularta has chosen to use the IAB Framework
which is described as "the most sophisticated and scrutinized model of GDPR-compliance for digital
advertising in the world". Roularta clarifies that the disclaimer was not intended
to disclaim responsibility, but rather to indicate that it is not able to block cookies
placed by third parties.

118. The liability shift in the cookie policy was not so much intended
to shift liability, asserts the defendant, but to indicate that the party

67 WP29, Opinion 3/2010 on
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_nl.pdf.
the "responsibility principle", 13
July 2010, WP173, 10, available at
the site
:



defendant is not technically able to block cookies placed by certain third parties (in
occurrence: advertisers).

Advertisers and agencies may, when broadcasting an advertising campaign on one of the
Roularta sites, run cookies or scripts through this campaign that are not
known in advance by Roularta.

119. The respondent states in its pleadings that the sentence in question was deleted from
cookie policy because, since the introduction of the IAB TCF Framework, it can be assumed that
IAB vendors will no longer place cookies or scripts in accordance with this framework unless the
consent has been obtained for the cookies and that the vendor in question has been approved in the
list of partner companies.

Position of the Litigation Chamber:

120. The Litigation Division does not agree with the Defendant's assertion that
which it is not responsible for the processing of cookies by a third party.68

121. IAB Europe's liability does not exclude the liability of other controllers
within the framework of the TCF-framework.69 The Litigation Chamber recalls that the defendant
must be considered as a (co-)controller within the meaning of the TCF, because it is supposed to
decide whether or not to cooperate with a registered CMP, and is also able to determine
which advertisers may offer advertising on its website or in its application and which
means (cookies) can be used for this purpose.

122. The defendant states in its submission that, given the dominant position of IAB
Europe, it was obliged to implement the IAB TCF. The Litigation Chamber judges that this
defendant's argument cannot be followed. In general, one can also
point out that there are alternative suppliers on the market, not to mention that it is not true that it
there is an obligation for the defending party to use the IAB offer in order to facilitate publicity
on its websites. Roularta was free in its choice to implement the IAB TCF and therefore bears the
responsibility for the consequences of this implementation.

123. The Litigation Chamber considers that the defendant must be identified as the
controller, which is also not disputed in the present proceedings. As

as data controller, it is responsible for the processing of personal data

and must be able to demonstrate compliance with the principles governing the processing of personal data.

personal character. Therefore, the defendant cannot separate liability

of the placement of cookies by third parties on its websites of its responsibility for processing. Furthermore,

Decision

68

https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-21-2022.pdf.

69

litigation

Bedroom

21/2022

february

ODA

from

2

2022,

available

via

:

Decision on the merits 85/2022 - 41/58

the cookie policy also states that it has no control over certain cookies placed

on its website. However, it is up to the defendant, as site manager

web and, in casu, as data controller under the law on the protection of

data, to take appropriate technical and organizational measures to ensure that

its processing activities comply with the relevant legislation. The refusal to impute the

responsibility for the placement of cookies by third parties to data subjects for whom the

defendant party can be designated as controller constitutes an infringement

of Article 5, paragraph 2 GDPR juncto Article 24 GDPR (duty of justification).70

124. In summary, the Litigation Chamber finds that the Respondent failed in its obligation

of justification (article 5, paragraph 2, j° article 24) by denying responsibility in relation to persons

concerned.

II.5.4. Incorrect and insufficient information (potential violation of Articles 4,

point 11), 12, paragraph 1, 13 and 14 of the GDPR) - Finding 5 Service Inspection.

125. The Inspection Service notes a violation of the principles of transparency of the GDPR in the

defective cookie policy of Roularta Media Group. For example, Article 12, paragraph 1, of the

GDPR provides that the controller must take appropriate measures to ensure that the

information required, inter alia, by Article 13 of the GDPR is provided to persons

concerned in a concise, transparent, intelligible and easily accessible form and in a

clear and understandable language.

Articles 13 and 14 of the GDPR then determine what information must be provided by the

controller to the data subject. Paragraphs 1 and 2 of these two articles

list the information that must be provided to the data subject by the controller

of the treatment.

126. To clarify the legislation in this area, the Court of Justice specified in the Planet49 judgment

how, prior to the placement of cookies, the controller had to provide

information on the duration of the operation of cookies as well as on the possibility or not for

third parties to have access to these cookies, in order to guarantee correct and transparent information (article

5.3 of the ePrivacy Directive regarding the placement of cookies juncto information obligations

of article 13.1 (e) and art. 13.2 (a) GDPR).

Inspection Service findings:

127. The Inspection Service found that the cookie policy had shortcomings:

70 The obligation of article 5.2 and 24.1 GDPR implies in particular that the RT must demonstrate that he fulfills the obligations c

RT does not demonstrate it, there is a violation of these articles. See also: Article 39 Data Protection Working Party, Opinion 3/2

principle

https://ec.europa.eu/justice/article-29/documentation/opinion-

recommendation/files/2010/wp173_en.pdf.

accountability,

2010,

July

12,

13

of

Decision on the merits 85/2022 - 42/58

▪ The respondent's cookie policy contains provisions that

are not GDPR compliant. For example, the cookie policy talks about a

implied consent for cookies through access to the defendant's websites,

which is in contradiction with the need for an expression of the will by a

clear statement or affirmative action under Article 4(11) GDPR. She indicates

also that no specific consent is required for data sharing

collected through cookies, which is contrary to the specific nature of the

consent for data processing pursuant to Art. 4 No. 11 GDPR;

▪ The cookie policy would also lack clarity as to the necessity

to use third-party cookies due to technical problems that have lasted for more than a

year;

▪ The Inspection Service also observes that the names of the types of cookies in the

cookie policy do not match the cookie category names

in the cookie settings tool, which does not improve comprehensibility;71

Cookie Policy

Cookie settings tool□

Necessary cookies□

Necessary functional cookies□

Analytical cookies□

Analytical cookies□

Social media cookies□

Selection of content and provision and□

reporting□

Advertising cookies□

Advertising selection and supply and□

Contents□

reporting□

Personalization□

Advertising and marketing cookies□

▪ Furthermore, the cookie policy does not contain information on the periods□

storage of cookies. The Privacy Policy only states:□

71 Service Inspection, Technical investigation report on the use of cookies on the Knack website (Exhibit 6 administrative file),□

39.□

Decision on the merits 85/2022 - 43/58□

“Roularta Media Group will not retain your data for longer than required by law.□

authorizes it and only what is necessary for the purposes set out in this document”. In□

In addition, the cookie policy states: "the retention period varies from one□

cookie to another, in general, the cookie is kept until the user deletes his□

Cookies. »□

▪ The cookie policy mentions the use by the partners of the “IAB□

Europe Transparency & Consent Framework” as a consent management tool,□

which guarantees third-party compliance with the GDPR, while of the 449 partners

listed on the Knack and Le Vif sites, 312 are not or no longer validated by the IAB;

▪ The user must consult the policies of the 449 sellers to know what these

companies do with their data and to make an informed decision to give their

consent. It is illusory and unenforceable and will further result in the placement

even more cookies when visiting links to these partners;

▪ Finally, it should be noted that cookies are not individually documented, which does not

does not allow the user to control what is done with their data.

The privacy policy contains brief information about cookies:

Position of the Litigation Chamber:

128. The Litigation Chamber notes that the Respondent indicates in its submissions that it has

amended its cookie policy on certain aspects72:

- The statement that the defendant's recording system used

temporarily third-party cookies to connect to the party's websites

defendant due to a technical problem has been deleted (the problem would have been

resolved by switching to new logging software that only uses a cookie

purely functional so that users do not have to log in again to

every time) ;

- In the cookie policy update of July 31, 2020, all cookies

are properly inventoried and documented.

72 See exhibit 20 of the defendant's exhibit file: new cookie policy.



Correcting a few inaccuracies cannot undo the past violation. Bedroom

litigation therefore finds that the defendant acted negligently with regard to

several aspects of its transparency obligation under Articles 12 and 13 of the GDPR.

129. In the first place, the offenses relate to incorrect information in the information policy.

of cookies. In accordance with Articles 13 and 14 (resp. paragraphs 1 and 2) of the GDPR, the information

the following, in summary, must be provided to the data subject: the name and contact details of the

responsible for the processing, the reason for which the data is processed, the duration of

retention of personal data, with which companies/organizations the data is

shared, as well as the data protection rights of the data subject. In what

concerning this last element, the Inspection Service noted that erroneous information

were given in the defendant's privacy policy, as

the existence of implicit consent contrary to the relevant provisions of the GDPR.

130. The Litigation Chamber states that the fact of providing false information on the requirement of

consent in the GDPR violates Articles 12(1), 13 and 14 GDPR.

131. Secondly, with regard to the mention of the temporary technical problem following which

third-party cookies were temporarily used to log users in. This issue

would date back to November 19, 2018, however, so it is impossible to speak of a problem

"temporary" (the observation of the mention in the cookie policy dates back to January 8

2020). The Litigation Chamber also ruled that a technical difficulty cannot justify a

breach of GDPR rules, as it is a long-lasting breach that may

to affect a large number of data subjects, and that the responsibility of the person responsible for the

treatment for these activities cannot be ruled out.

132. Thirdly, regarding the inconsistencies between the cookie policy and the

cookie management. The defendant justifies this by asserting that it was obliged by IAB

Europe to use these terms in the consent tool or you will be excluded from the IAB TCF. She

wanted to use more understandable terms in its own cookie policy.

The Litigation Chamber understands the defendant's position with regard to

the mandatory application of the terms proposed by IAB Europe in its consent tool.

However, this does not change the fact that the use of different terms in its

privacy increases ambiguity and, in this sense, is not consistent with the provision

information in "a concise, transparent, understandable and easily accessible form, and

in clear and simple language" (article 12, paragraph 1 GDPR on the interpretation of articles 13 and

14 GDPR).

133. Fourthly, regarding the lack of information on cookie storage periods.

The Inspection Service found that there was only one cookie policy in the cookie policy.

mention that the retention period "depends on each cookie". The part

Decision on the merits 85/2022 - 45/58

defendant argues that the views of the Inspection Service that "there is no

concrete information on storage periods" and that "the cookie policy

refers to a storage period which is in principle unlimited" are incorrect. She asserts

that in principle, two types of information on the retention period of cookies were included in

the cookie policy: (i) the fact that the retention period varies from cookie to cookie; (ii)

the fact that the user can deactivate cookies, which leads to a retention period

non-existent. Therefore, the defendant argues that the Inspection Service went too

away by claiming that this information equates to an unlimited retention period.

134. The Litigation Chamber agrees with the Respondent regarding the latter

element. The information contained in the cookie policy does not mention

a storage period that is in principle unlimited. However, this does not change the fact that the

information in the cookie policy was not sufficiently clear

and transparent, because there was no indication of the concrete retention periods, and these

information was therefore also not available to the persons concerned. Section 13,

2(a) GDPR and Article 14(2)(a) GDPR make it clear that

information must be provided on "the retention period of personal data

or, if that is not possible, the criteria for determining this duration". The Committee of

the Protection of Privacy, legal predecessor of the DPA according to art. 3 LCA, has already issued a

recommendation to Facebook in 2017 regarding its cookie policy. In this

document, the Commission stated that the data subject should be informed in a manner

complete and precise, in a clear and understandable way, of the data retention period

that it collects via cookies.73 According to the Commission, providing this information would be

also necessary to ensure informed consent and fair and lawful processing.74

The defendant has since corrected this deficiency in its revised policy on

cookies.75

135. By not providing clear and transparent information on the concrete durations of

retention of cookies placed on its website, as established by the Inspection Service, the

defendant violates Articles 13 and 14 j° 12, paragraph 1) GDPR.

136. Fifthly, with regard to the mention in the management tool of the consent concerning

the use of the “IAB Europe Transparency & Consent Framework”. The defendant asserts

that with this mention, it only wanted to improve transparency and inform the user of

how it intends to control the use of cookies, namely by adhering to a standard

internationally recognized in the world of digital advertising. The Inspection Service has

73 CPVP, Recommendation n°03/2017 of April 12, 2017 supplementing recommendation n°04/2015 ex officio with regard to 1)

Facebook, 2) Internet and/or Facebook users as well as 3) Facebook users and service providers, in

in particular social plug-ins (CO-AR-2017-004).

74 Ibid.

75 Exhibit 20 of the defendant's book of exhibits.



considered that this reference in the privacy policy was insufficient to

grant consent by default to the 449 partners of Knack and Le Vif (the report of

the Inspection also shows that 312 of the 449 partners - an overwhelming number - are no longer

validated by the IAB).

137. From these elements, the Litigation Chamber concludes that the information provided by the party

defendant to users thus seek to create an appearance of compliance with the rules of

Data protection. It is impossible to assume that this reference increases the

transparency, especially when it turns out that the information was also incorrect. For this

reason, it must be concluded that the information provided by the defendant in this regard

also lack clarity and transparency within the meaning of Articles 13 and 14, j° 12, paragraph 1 of the

GDPR.

138. Sixthly, with regard to the fact that, in principle, the user of the website should consult

the policies of the 449 partners in order to know what happens to their data and to give their

informed consent on this basis. This reference cannot be accepted as the only supporting element

of the information of the people concerned, because it cancels de facto the responsibility of the person in charge

processing with regard to the obligation to inform - which is not in accordance with the provisions of the

GDPR in this context. The fact that data subjects do not receive more information

specific and clearer on the use and further use of their personal data

therefore constitutes a violation of the information obligation provided for in Articles 13 and 14 j° 12, paragraph 1

of the GDPR.

139. Seventh, the Litigation Division examines the findings of the Inspection Service

regarding the lack of individual documentation of cookies in the cookie policy of the

defendant.

In this regard, the Litigation Chamber recalls that, in accordance with Articles 13 and 14, j°article

12(1) GDPR, transparent information must be provided regarding cookies

who collect or otherwise process personal data. This requirement applies

regardless of whether or not consent is required for installing and playing

these cookies, and therefore also in the event that the cookie is strictly necessary.

140. In the cookie policy, there are only a limited number of informative elements

on cookies:



Given the very limited information provided in relation to the list of cookies present76, the

Litigation Chamber unequivocally establishes a problem of the obligation to inform.

141. For a cookie to be sufficiently documented, it would certainly be necessary to indicate separately for each category of cookies the following information: the personal data processed, the purposes of the processing of these cookies and the retention period of these cookies (see the obligations information of articles 13, paragraph 1 and 14, paragraph 1 GDPR). As this information is lacking for each category of cookies used in the cookie policy, it is not possible to consider that the cookies have been sufficiently documented.

142. The Litigation Chamber concludes from the offenses listed above that the defendant did not comply with its information obligations pursuant to Articles 13 and 14, j° 12, paragraph 1 GDPR at time of these findings. In this regard, the Litigation Chamber emphasizes that it is incumbent on the controller to ensure that the information provided on the website corresponds to reality, in accordance with the aforementioned provisions in the GDPR. The Litigation Chamber expressly refers to the liability obligation provided for in Articles 5, paragraph 2 and 24 of the GDPR.

II.5.5. Unjustified storage periods of cookies (Article 5, paragraph 1, point e) GDPR)

- Observation 6 Service Inspection

143. Article 5, paragraph 1, point e) of the GDPR provides that personal data may not be kept longer than necessary to achieve the intended purpose (principle of "retention limitation"). The retention period cannot therefore be unlimited. The information collected and stored in a cookie and information collected as a result of reading a cookie must be deleted when they are no longer necessary for the intended purpose.

144. On the DPA website, in the thematic file "cookies", it is indicated the following concerning the storage period or the lifetime of the cookies:

"A cookie exempt from the obligation of consent must have a lifespan directly related to the purpose for which it is used and must be configured to expire as soon as that it is no longer necessary, taking into account the reasonable expectations of the user medium. Cookies that are not subject to consent will therefore likely need to

expire at the end of the browser session, or even before. But it's not always the case. By□

For example, in the shopping cart scenario, a merchant can set the cookie to□

whether it is maintained after the end of the browser session or for a few hours to□

take into account that the user may accidentally close the browser and□

reasonably expect to find the contents of the shopping cart when he returns to□

the merchant's website a few minutes later. In other cases, the user can□

76 For an overview with the names of the cookies installed and the conclusions regarding their defective nature, see: Investigati

technical on the use of cookies on the Knack website, exhibit 6 administrative file, p. 29 and following.□



explicitly ask the service to remember certain information from a session□

to another, which requires the use of permanent cookies. »77□

145. The technical analysis reports of the Inspection Service, concerning the Knack and Le Vif websites,□

demonstrate that the effective storage periods of certain cookies are unreasonably□

long and that cookies have a lifespan of several years. Below you will find a□

overview of cookies with an unreasonably long shelf life (expressed in days)□

:□

- UID: 720 days (Le Vif and Knack)□

-□

_gfp_64b: 1000 days (Knack and Le Vif)□

- OB-USER-TOKEN: 90000 days (Knack and Le Vif)□

- U: 730 days (Le Vif)□

- Gdyn: 1698 days (Le Vif and Knack)□

- Gtest: 1698 days (Knack)□

146. The defendant argues that the Data Protection Authority did not issue a□

specific guidelines in the past regarding the exact periods for storing cookies. She□

argues that, because of this uncertainty, she did not understand what to hear□

precisely by "a lifespan which cannot exceed the time necessary to achieve the objective

for follow-up ".

147. However, the Litigation Chamber recalls that the absence of directives from an authority

of control cannot be used by a data controller as a reason not to

comply with the provisions of the GDPR.78 In accordance with the duty of responsibility provided for in

articles 5, paragraph 2 and 24 of the GDPR, the latter is required to ensure that the processing of personal data

personal data he performs complies with the provisions of the GDPR and must be able to

prove.

148. Following on from the foregoing, it should be noted that, if the defendant considered

that the lifetime of certain cookies and the retention period of personal data

personal collected through these cookies were proportional, it could have demonstrated it,

if it so wished, or argue during the procedure the reasons for which it considers

that the retention periods used comply with the requirements of Article 5, paragraph 1,

point e) GDPR. However, the defendant failed to do so.

77 https://www.gegevensbeschermingsautoriteit.be/professioneel/thema-s/cookies. It is the Litigation Chamber which underlines

78 See also supra, section II.3 of this decision.



149. In addition, the reports of the Inspection Service show that the lifespan of certain cookies in

casu is manifestly disproportionate and can in no way be considered as

proportionate to the purpose pursued. In this context, particular mention should be made of the

“OB-USER-TOKEN” cookie, whose lifespan is 90,000 days, i.e. approximately 246 years.

150. The defendant states in its reply submission that the retention period

provided for in its privacy policy implies that the cookies placed are

retained until deleted by the user.79 The Respondent argues that the

finding of the Inspection Department that retention periods are "indefinite" is therefore

incorrect.

151. While it is true that the defendant did not claim that the storage period was unlimited, it is

also true that the failure to have clearly and proactively set (criteria for) the

concrete storage periods constitutes a manifest breach of the principle of

storage limitation.

152. On the basis of the foregoing, the Litigation Chamber finds that the defendant has violated

Article 5, paragraph 1, point e) of the GDPR.

II.5.6. Non-compliance with the withdrawal of consent (Article 7, paragraph 3 GDPR) - Finding 7

Inspection Service

153. According to Article 7, paragraph 3 of the GDPR, the data subject has “the right to withdraw his

consent at any time. Withdrawal of consent does not affect the lawfulness of the

processing based on consent made prior to such withdrawal. The person concerned is

informed before giving consent. It is as easy to withdraw as to give

consent. »

Findings of the Inspection Service: 80

154. The technical analysis report on Le Vif's website demonstrates that:81

- When the inspector surfed the site, 60 cookies were detected before the

consent is given;

- When the inspector has given consent for all cookies in the tool

consent to cookies, 147 cookies were detected;

79 Cf. conclusion of the defendant's response, p. 32, n°86 and following.

80 Inspection Service Report, Exhibit 10, p. 30, with reference to the findings in the technical investigation reports on this subjec

81 Page 36 of the Vif technical analysis report.



- When the inspector wanted to return to the choice screen (consent tool) to withdraw

his consent, he was faced with a black screen, after which the website crashed:

Therefore, the Inspection Service considered it impossible to withdraw the consent.

155. For the Knack website, the Inspection Service found that 82:

- By following steps 1 to 15 (in step 15, all cookies were accepted), 86 cookies were

been detected;

-

at step 24 (delete cookies and reload the web page): number of cookies 73→

step 25 (re-authorize all cookies and reload the page): number of cookies 85 →

step 26 (return to minimum cookies and reload): number of cookies 88;

Between step 24 "all cookies" and step 26 "minimum cookies", the number of cookies

not decrease, on the contrary, it increases.

156. Furthermore,

the technical analysis report from the Inspection Service shows that removing

the

consent is more difficult than giving it:

- For Le Vif, it is even impossible to withdraw consent (see above).

- For Knack, it seems that modifying consent is only possible by clicking

on "cookie settings" in the "footer":

Defendant's position:

157. In its submission in response, the defendant asserts, with regard to the findings of the

Service Inspection described above regarding the withdrawal of consent, that some of these

problems are due to an unfortunate configuration of the OneTrust cookie tool, which was used

by the defendant at the time of the findings. In that regard, it argues in particular that,

82 For an overview of all the steps taken by the Inspection Service, see pages 31 to 33 of the technical analysis report.



firstly, during the implementation of the aforementioned tool, no correct technical link was established

between the consent given or not and the first party cookies placed by the site itself. She

argued that with respect to cookies placed by advertisers, consent was

correctly imposed by applying the IAB TCF. The defendant adds that the problem

aforementioned was resolved on March 31, 2020 by the implementation of the CMP Didomi.

158. Secondly, with regard to the finding of the Inspection Service that a black screen is

obtained for the website www.levif.be when an attempt to withdraw consent is made,

the defendant argues that this is also due to a problem with the configuration of

the OneTrust cookie tool. However, the defendant argues that by inserting the "more

info and configuration", its intention was to allow users to modify for free

their consent. It states that it regrets that during its investigation, the Inspection Service was

faced with a black screen instead of the corresponding setting screen.83

Position of the Litigation Chamber

159. Based on the findings of the Inspection Service, the evidence presented above and the

statements of the defendant, the Litigation Chamber considers that more measures

are necessary to withdraw consent than to grant it. This is not in accordance with

Article 7, paragraph 3, of the GDPR, which stipulates that the withdrawal of consent must be as simple as

its grant.

160. The fact that technical problems arise during the withdrawal process of the

consent indicates that correct technical measures have not been taken to ensure

that a data subject can withdraw their consent at any time. Furthermore, it seems that,

even when the person concerned is given the impression that he has withdrawn his consent, the

technical situation does not pass to a basic situation, but on the contrary, one can detect

more cookies processing personal data on the Knack website.

161. Consequently, the Litigation Chamber finds a violation of Article 7, paragraph 3 of the GDPR

both with regard to the Knack and Le Vif websites.

III. Offenses and Penalties

162. In summary, in casu, the Litigation Chamber finds violations of the following provisions of

the part of the defendant:

-

Article 6, paragraph 1, of the GDPR, read in conjunction with Article 129, paragraph 2, of the law on

electronic communications (now article 10/2 of the law of July 30, 2018 on the

83 Respondent's conclusion, p. 33.

Decision on the merits 85/2022 - 52/58

protection of natural persons with regard to the processing of personal data

staff84), due to the placement on its websites www.knack.be and www.levif.be of

cookies that were not strictly necessary, without consent having been

obtained. In accordance with the provisions mentioned, the processing of data to

personal character through the placement and/or reading of cookies requires consent

prior consent of the data subject, unless the cookies are strictly necessary for

1) carry out the transmission of a communication via a communications network

or 2) provide a service explicitly requested by the user. The findings

of the Inspection Service and the documents in the file show that cookies which cannot

be considered strictly necessary have been placed on both websites

aforementioned, without the consent of the user having been obtained. He has

also found that statistical cookies were placed without consent

of the user. The defendant does not deny or refute the above finding in its

response conclusion and at the hearing.

-

Articles 4, point 11 j° 6, paragraph 1, point a) and 7, paragraph 1 GDPR, as set out in

recital 32 of the GDPR, for non-compliance with the conditions relating to consent

contained in the aforementioned provisions. It was noted in particular that on the sites

web www.knack.be and www.levif.be, at the time of the survey, "pre-ticked boxes"

were used, the cookies of the partner companies being marked as "active"

by default. However, this cannot in any way be a valid consent within the meaning of

Article 4, point 11) GDPR for the placement of cookies (i.e. "any manifestation

of free, specific, enlightened and unequivocal will by which the person

concerned accepts, by a declaration or by a clear positive act, that

personal data concerning him or her are processed").

This practice is also contrary to the case law of the Court of Justice of the European Union

European Union (Planet4985 judgment).

-

Articles 5, paragraph 2, and 24 of the GDPR, due to the publication of a disclaimer

liability on the relevant websites where the defendant claims that it is not

not responsible for the placement of third-party cookies on these sites, in particular in the context of

using the IAB Transparency and Consent Framework. However, this position of the party

defendant is contrary to the case law of the Court of Justice of the European Union

in the Wirtschaftsakademie judgment,86 where the Court held that the owner of a website

is responsible for the treatment by means of cookies that its website installs or reads. the

84 MB September 5, 2018.

85 CJEU, C-673/17, 1 October 2019, ECLI:EU:C:2019:801.

86 CJEU, C-210/16, 5 June 2018, ECLI:EU:C:2018:388.



behavior of the defendant is therefore contrary to article 5, paragraph 2 j° article

24 of the GDPR, according to which the controller is obliged to ensure compliance with the

provisions of the GDPR and to provide proof of this compliance.

-

articles 12, paragraph 1, j° 13 and 14 GDPR, given that the way in which the information has

provided to data subjects does not meet the requirement of a "form

transparent, understandable and easily accessible". First, it was found that

the privacy policy contained erroneous information, in particular in

regarding the consent to the use of cookies, as well as the need to accept

third-party cookies. The Privacy Policy also did not contain, at

time of the survey, a complete list of the different types or categories of cookies

placed. This policy also did not contain sufficient information on (the criteria

determining) the lifespan of the cookies placed and the retention period of the

data thus collected, as required by Articles 13, paragraph 2, point a) and 14, paragraph 2,

point a) of the GDPR. The privacy policy also did not contain

information about treatments by partners, so that people

concerned had to consult the policies of a large number of partners and

vendors for this information.

-

Article 5, paragraph 1, point e) of the GDPR, for non-compliance with the principle of restriction of

storage. A cookie must have a lifetime directly linked to the purpose for which it is used.

is used and should be configured to expire as soon as it is no longer needed, taking into account

account the reasonable expectations of the user.

-

Article 7, paragraph 3 of the GDPR, for not having ensured that the withdrawal of consent to the

placement of cookies is as simple as granting them. Specifically, it was established for the

website www.levif.be that the withdrawal of consent is technically impossible via the tool

cookie management, because this management tool crashes and a black screen appears. He

emerges from the technical analysis of the site www.knack.be that the withdrawal of consent is not

not efficient, since the number of cookies does not decrease after returning to choices

minimal. The defendant does not deny or refute this finding and indicates in its

answer conclusion that this problem was caused by improper configuration of the tool for

OneTrust cookies used at the time.

163. Because of these offences, the Litigation Chamber decides to impose an administrative fine

of 50,000 euros to the defendant for the aforementioned infringements. Bedroom

litigation also decides to order the defendant to put the processing of

personal data in accordance with the applicable provisions of the legislation on

Decision on the merits 85/2022 - 54/58

data protection within three months of receipt of this

decision.

164. It should be noted in this context that the administrative fine is not intended to terminate

an offense committed, but rather to vigorously enforce the rules of the GDPR. In effect,

as can be seen from recital 148 of the GDPR, the latter provides that for each serious infringement -

i.e. even if an infringement is detected for the first time - sanctions, including

administrative fines, must be imposed in addition or as an alternative to the measures

appropriate.87In what follows, the Litigation Division demonstrates that the offenses committed by

the defendant in relation to the aforementioned provisions of the GDPR are in no way

minor offences, nor that the fine would cause a disproportionate burden on a person

physical as referred to in recital 148 of the GDPR, according to which it is possible to waive

the fine in both cases. The fact that this is the first observation of a violation of the GDPR

committed by the respondent therefore in no way affects the ability of the Chamber

court to impose an administrative fine. The Litigation Chamber imposes the fine

administrative in accordance with Article 58, paragraph 2, point i) of the GDPR. The instrument of the fine

administrative is not intended to put an end to the infringements. To this end, the GDPR and the LCA provide for a

a number of corrective measures, including the orders referred to in Article 100, §1, 8° and

9° ACL.

165. Taking into account Article 83 GDPR88, the Litigation Chamber gives concrete reasons for the imposition

an administrative penalty:

a) the nature, gravity and duration of the infringement (art. 83.2 a) GDPR): the infringements observed

relate in particular to a violation of the provisions of the GDPR relating to the principles of

data protection (Art. 5 GDPR) and lawfulness of processing (Art. 6 para. 1 GDPR) as well as the

transparency (Art. 12 et seq. GDPR). A breach of the above provisions is,

in accordance with Article 83(5) of the GDPR, liable to the highest financial penalties.

Reference should also be made to the extent of the processing in terms of the number of

persons concerned. According to figures from the Media Information Center (CIM), the sites

87 Recital 148 states: “In order to reinforce the application of the rules of this Regulation, sanctions including fines

administrative measures should be imposed for any violation of this Regulation, in addition to or instead of the measures

appropriate imposed by the supervisory authority under this Regulation. In the event of a minor violation or if the fine liable

to be imposed constitutes a disproportionate burden for a natural person, a call to order may be sent rather than a

fine. However, due consideration should be given to the nature, gravity and duration of the breach, the intentional nature

the breach and the measures taken to mitigate the damage suffered, the degree of responsibility or any relevant breach

previously committed, how the supervisory authority became aware of the breach, compliance with the measures

ordered against the controller or processor, the application of a code of conduct, and any other

aggravating or mitigating circumstance. The application of sanctions, including administrative fines, should be subject to

appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to

effective judicial protection and due process. [proper underlining]

88 See also the case law of the Cour des Marchés, cf. in particular Brussels Court of Appeal (Cour des Marchés section), X.

N/A DPA, Judgment 2020/1471 of February 19, 2020.



web in question are among the twenty most visited media sites in Belgium, which

means that the number of people involved is by definition large.

b) relevant breaches previously committed by controllers (Art. 83.2

e) of the GDPR): the defendant has never been the subject of enforcement proceedings by the Authority

of Data Protection.

h) the manner in which the DPA became aware of the infringement (Art. 83.2 h) GDPR): infringements have no

not reported by the defendant but were found during an investigation

carried out by the Inspection Service on the initiative of the APD Management Committee.

166. On April 20, 2022, a Sanction Form (“Reaction Form Against Proposed Sanction”)

was given to the defendant. This sanction form lists the offenses which are

the subject of this decision, as well as the amount of 50,000 euros which is envisaged as

Amount of the fine. On May 11, 2022, the defendant submitted its reaction to this form of

sanction in the Litigation Chamber.

167. In summary, the Respondent claims in this response that:

1) According to the defendant, the infringements were committed only during a period

limited, as the defendant only used the OneTrust cookie tool for 7 months.

2) According to the defendant, the Litigation Division wrongly refers to a "large number of

persons concerned", while, according to the defendant, the Litigation Chamber does not

does not demonstrate to what concrete order of magnitude this refers. According to the defendant, the

CIM classification "gives no indication of the number of visitors", nor of the people

concerned, since only visits are measured. Indeed, several visits can be

attributed to the same persons, in particular because the persons concerned visit the

defendant's websites via different devices.

3) The Respondent also raises objections to the methodology used

to determine the amount of the fine and makes a comparison with the fines

imposed abroad for similar offences. It also claims that the fine

proposed "is disproportionate" in relation to the modest turnover generated by its

websites (surveyed) through digital advertisements.

4) Finally, the defendant asserts that the turnover to which the application form refers

sanction is that of the entire group and should not be taken into account in its entirety

for the calculation of the fine, because all the subsidiaries are not part of "the same unit

economic ".

168. With regard to the Respondent's first argument in its response to Form□

fine, the Litigation Division refers to the findings made by the Inspection Department at several□

specific times during the survey period. The fact that a change in the management of the websites of□

the defendant intervened after these findings does not in itself affect the infringements□

observed at those times. It is true that the Litigation Chamber can take into account a□

improvement in the situation demonstrated by the defendant during the proceedings before□

the Data Protection Authority, but this requires the defendant to indicate in concreto□

why and how a certain modified situation can be used as a mitigating circumstance.□

In this regard, the defending party does not demonstrate that ceasing to use the cookie tool□

OneTrust means that the situation of the persons concerned by the processing of the data at□

personal character improved thereafter.□

169. With regard to the second argument, the Litigation Chamber underlines that, if the figures of the□

CIM to which, among others, the Inspection Service referred in its reports do not give□

concrete indication of the number of people involved, these figures provide an indication□

general popularity of news sites. The fact that the various organs of the Authority of□

Data Protection do not demonstrate in concrete terms how many data subjects are□

affected by the activities of a particular controller that is the subject of a procedure□

of execution does not mean that indications as to the order of magnitude of the number of people□

concerned cannot be relevant in determining the seriousness of one or more breaches□

of personal data protection law, in particular the impact on a certain□

order of magnitude of people involved. A comparison can be made with a situation where□

the number of people affected cannot be precisely determined, but where there are□

information on the concrete number of persons concerned.89 Mutatis mutandis, the fact that the party□

defendant contests the order of magnitude (generally expressed) of the number of people□

data subjects visiting its websites, without itself providing proof to the contrary, is not sufficient□

to demonstrate why the CIM figures cannot provide an indication of the order of□

magnitude of the number of people involved.

170. With regard to the third argument relating to the amount of the fine, the Litigation Division

recalls that the placement of cookies in this case is a commercial matter for the party

defendant, in which it has considerable financial interests in acquiring the income

related advertisements. The Litigation Chamber refers for information purposes to the directives

on monetary administrative penalties, which had not yet been adopted at the time of the

findings of the Inspection Service and transmission of the fine form.90

89 DPA Litigation Chamber, Decision 4/2021 of 27 January 2021, 46; an appeal against this decision was declared unfounded;

Court of Appeal of Brussels (Cour des Marchés), July 7, 2021, 2021/AR/320.

90 Guidelines 04/2022 on the calculation of administrative fines under the GDPR, 16 May 2022, available at:

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en.



171. As a fourth argument, the Respondent invokes the fact that the Litigation Chamber

has not proven that the companies belonging to its global group are part of the same unit

economic. The Litigation Chamber recalls in this regard that during the proceedings, it

acted against the defendant as a class, and also named the party

defendant in this capacity during the proceedings. Moreover, in its response to the form

sanction, the defendant designates itself in its legal form as a

group, without distinguishing between the different alleged economic activities, or presenting themselves as

part of a (separate) economic activity. The Litigation Chamber therefore emphasizes

that it can impose fines on the basis of the turnover of an entire company,

which is undeniably the group as a legal entity.91 As a reminder, the Chamber

litigation recalls that the supervisory authorities have the power - subject to a

adequate justification - to impose fines of up to

up to 10,000,000 or

20,000,000 euros, respectively, regardless of the size of the company, but in

depending on the type of offence.92

172. All of the elements set out above justify an effective, proportionate and

dissuasive within the meaning of Article 83 GDPR, taking into account the evaluation criteria defined therein. The

Litigation Chamber recalls that the other criteria of art. 83.2. GDPR are not in this case

likely to result in an administrative fine other than that determined by the Chamber

litigation in the context of this decision.

IV. Publication of the decision

Given the importance of transparency with regard to the decision-making of the Chamber

litigation, this decision will be published on the website of the Data Protection Authority,

in accordance with article 95, §1, 8° LCA, with the indication of the identification data of the party

defendant and this because of the specificity of this decision - which means that even in the event

omission of identification data, re-identification is inevitable or at least highly

probable - as well as the general interest of this decision.

91 Article 83, paragraphs 4, 5 and 6 GDPR.

92 Ibid.



FOR THESE REASONS,

the Litigation Chamber of the Data Protection Authority decides, after deliberation:

- to impose an administrative fine of EUR 50,000 on the basis of Article 58, paragraph 2, point

i) j° Article 83 GDPR and Article 100, § 1, 13° LCA for the violation of Article 6, paragraph 1 GDPR j°

article 129 LCE; Articles 4, point 11) j° 6, paragraph 1, point a) and 7, paragraph 1 GDPR; of clause 5,

paragraph 2 and 24 GDPR; Articles 12, paragraph 1, j° 13 and 14 GDPR; of Article 5, paragraph 1, point e)

GDPR; and Article 7(3) GDPR.

- to condemn the defendant, on the basis of article 58, paragraph 2, point d) GDPR and

article 100, § 1, 9° LCA, to bring into compliance with the provisions of the GDPR, within a period of

three months from receipt of the decision on the merits, the processing of the data to

personal character in the context of which various offenses have been noted in the

this Decision and for which a fine has been imposed under the first indent of this

device, and to provide proof thereof.

In accordance with Article 108, § 1 of the LCA, this decision may be appealed in a court of law.

period of thirty days from its notification, to the Court of Markets, with the Authority of

Data Protection as defendant.

(Sr.) Hielke Hijmans

President of the Litigation Chamber