

# Complaint to the Commission Nationale de l'Informatique et des Libertés

---

## Doctissimo

---

Privacy International – 26 June 2020

### A. Introduction and Purpose of this Complaint

Through this complaint Privacy International asks the Commission Nationale de l'Informatique et des Libertés ("CNIL") to investigate the compliance of **Doctissimo** with the General Data Protection Regulation 2016/679 ("GDPR"), and the Loi n°78-17 of the 6 January 1978 dite *Loi Informatique et Libertés*. Doctissimo is a French based company and therefore the CNIL is the relevant data protection supervisory authority to act on this complaint.

As set out in this complaint, Privacy International has grave concerns about the data practices of Doctissimo, a French health information site, who process the personal data of millions of people in France and likely further afield.

This complaint is based on technical investigations by Privacy International combined with publicly available information that Doctissimo provide on their services. The infringements are serious and systemic.

In summary, Doctissimo:

- Has no lawful basis for the processing of personal data highlighted in this complaint, in breach of Articles 5 and 6 of the GDPR, as the requirements for valid consent are not met. Consent is Doctissimo's stated basis for processing and the only available legal basis given the

nature of the processing involved requires consent in line with Article 82 of the *Loi Informatique et Libertés*. Nor do Doctissimo have explicit consent in the case of special category personal data, in breach of Article 9 of the GDPR.

- Does not comply with the Data Protection Principles in Article 5 of the GDPR, namely the principles of transparency, fairness, lawfulness, purpose limitation, data minimisation and integrity and confidentiality.
- Does not comply with its obligations under Article 25 (Data Protection by Design and by Default) of the GDPR and Article 32 (Security of Processing) of the GDPR.
- Requires further investigation as to compliance with the rights, obligations and safeguards in GDPR, including the rights in Articles 13 and 14 (the Right to Information).
- Does not comply with Article 82 of the *Loi Informatique et Libertés* in its use of cookies and other tracking technologies on users' devices.

Privacy International therefore calls on the CNIL to take action to investigate the practices detailed in this complaint and take appropriate and timely enforcement action in order to protect individuals from wide-scale infringements of the law.

Before submitting the present formal complaint, Privacy International has attempted to engage with Doctissimo regarding the company's data practices multiple times. First in August 2019 in anticipation to the publication of our first report in which we investigated the company, then in January 2020 prior to the publication of a follow up article. Both times we offered the company the opportunity to exercise its *droit de réponse* yet the company never did nor as far as we can see did it amend its practices. We have sent Doctissimo a copy of this complaint.

## B. Privacy International

Privacy International ("PI") is a non-profit, non-governmental organisation (Charity Number 1147471) based in London. We fight for a world where technology will empower and enable us, not exploit our data for profit and power. Established in 1990, PI undertakes research and investigations into government and corporate surveillance with a focus on the technologies that

enable these practices. As such PI has statutory objectives which are in the public interest, is active in the field of the protection of data subjects' rights and freedoms and is eligible to act under Article 37 paragraph 4 point 1 of the *Loi Informatique et Libertés*. This submission relates to PI's ongoing work on data exploitation, corporate surveillance and the GDPR.

## C. The Data Controller – Doctissimo

### Information about the company

Doctissimo is a simplified stock company operating in France offering websites and a range of mobile apps dedicated to health and wellbeing. Doctissimo's head office is situated at 8 rue Saint Fiacre 75002 Paris, and the company is registered under the "Registre du Commerce et des Sociétés de Paris" n°562 013 524. Doctissimo was established in 2000 and now belongs to French media group TFI since 2018.<sup>1</sup>

Doctissimo describes itself as a "health information website" that became a "space for expression where each and everyone can be a driver of its own health and wellbeing". According to Doctissimo, the content published on the website is written either by journalists or health professionals. Doctissimo also offers thematic forums for each of its sections (12 in total).<sup>2</sup>

Doctissimo generates revenue through advertising on its services. Doctissimo's terms and conditions state that "users are informed that access to free content is supported by advertising revenue".<sup>3</sup> Doctissimo reportedly had 12 million unique visitors per month in 2018 and 40 million in total.<sup>4</sup> It has also been reported that Doctissimo's audience is primarily women.<sup>5</sup> Doctissimo's very large pool of users interested in health and wellbeing is associated with effective search engine optimisation ("SEO") making Doctissimo a highly desired platform for advertisers. Reports indicate that SEO has been a core to Doctissimo since its inception, which has contributed

---

<sup>1</sup> <https://www.doctissimo.fr/equipe/charte/charte-donnees-personnelles-cookies> (viewed on 01/06/2020)

<sup>2</sup> <https://www.doctissimo.fr/equipe/doctissimo/qui-sommes-nous> (viewed on 01/06/2020)

<sup>3</sup> <https://www.doctissimo.fr/equipe/charte/CGU-site> article 7.1 (viewed on 01/06/2020)

<sup>4</sup> Platiau, "TF1 rachète Doctissimo à Lagardère, qui cède aussi "MonDocteur", Challenges 12 July 2017, [https://www.challenges.fr/media/tf1-rachete-doctissimo-a-lagardere-qui-cede-aussi-mondocteur\\_600690](https://www.challenges.fr/media/tf1-rachete-doctissimo-a-lagardere-qui-cede-aussi-mondocteur_600690) (viewed on 01/06/2020)

<sup>5</sup> "La pub, moteur de Doctissimo", Le Parisien, 13 February 2012, <http://www.leparisien.fr/la-pub-moteur-de-doctissimo-13-02-2012-1857941.php> (viewed on 01/06/2020)

overtime to making it one of the best referenced (and thus popular) French websites.<sup>6</sup> Doctissimo's forums<sup>7</sup> have more than 1.2 Million registered users<sup>8</sup> and Doctissimo's apps allow users to access forums from mobile devices.

## Products/ Services of concern

PI is concerned with a number of Doctissimo products/ services – primarily the Doctissimo website (<https://www.doctissimo.fr>) and the two Doctissimo apps, Club Docti – Forums Doctissimo And Ma grossesse Doctissimo.

The practices on these services which concern PI include:

- **Tests offered to users** - on a variety of topics such as mental health, sex, health (including medical conditions ranging from a headache to cancer), wellbeing, personality, beauty and more. Research by PI demonstrated how answers to these tests on Doctissimo's website are shared with a third party along with a unique identifier.<sup>9</sup>
- **Inadequate consent mechanism** - via a popup that disappears after a mere scrolling. Doctissimo interprets said scrolling as consent to a variety of data sharing practices.<sup>10</sup>
- **Programmatic advertising and tracking** - across its main website leading to the systematic sharing of personal data with a high number of third parties. Tracking advertising techniques observed by PI include technologies such as Real Time Bidding ("RTB"), cookies and potentially fingerprinting.
- **Data sharing with an extremely high number of third parties** - Doctissimo shares data with 557 partners (at the time of PI's testing) following the inadequate consent process described above. These are included as an Annex to this complaint.

---

<sup>6</sup> Eustache, "La "patiente informée", une bonne affaire", Le Monde Diplomatique, Mai 2019, <https://www.monde-diplomatique.fr/2019/05/EUSTACHE/59878> (viewed on 01/06/2020)

<sup>7</sup> <https://forum.doctissimo.fr> (viewed on 01/06/2020)

<sup>8</sup> See at the bottom of the forum page <https://forum.doctissimo.fr/> : "Utilisateurs Enregistrés : 1 231 871" (viewed on 01/06/2020)

<sup>9</sup> The website sends test answers, together with a unique identifier, to third party – player.qualifio.com <https://privacyinternational.org/sites/default/files/2019-09/Your%20mental%20health%20for%20sale%20-%20Privacy%20International.pdf> (viewed on 01/06/2020)

<sup>10</sup> From Doctissimo consent popup: "Pour accepter, nous vous invitons à poursuivre votre navigation (notamment au travers d'une action de scrolling)" (= to accept, we invite you to continue your browsing (including through scrolling))

- **Covid-19 Chatbot** – Doctissimo now offers on its website a chatbot to answer covid-19 related question. From PI’s analysis set out in this submission, the bot consent mechanism is flawed and text typed by the user is shared with a third party.

## D. Background

### Concerns about the AdTech industry and publishers’ role in the ecosystem

While this submission focusses on Doctissimo, it directly refers to advertising technology (“AdTech”) as the source of many of the concerns we raise with regards to GDPR infringements. AdTech is a catch all term referring to companies that work in “behavioural advertising”. At a generalised level these are companies that track, identify and profile individuals around the web to dictate which adverts they are targeted with. This ecosystem involves the collection, processing, and sharing of the personal data of millions of individuals.

Personal data is harvested, generated, shared and processed in a multitude of ways using a range of tracking technologies such as cookies, web beacons, device fingerprinting, tags and SDKs to segment/classify customers based on pages visited, links clicked and products purchased, among others. These forms of processing of personal data and PI’s concerns with them, are detailed in PI’s submission to data protection authorities concerning AdTech companies Criteo, Quantcast and Tapad.<sup>11</sup> AdTech is entwined with the data broker ecosystem which is the subject of PI’s submissions concerning Oracle and Acxiom, Experian and Equifax.<sup>12</sup> These submissions are currently the subject of ongoing regulatory investigations.<sup>13</sup>

---

<sup>11</sup> <https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem> (available also in French [https://privacyinternational.org/sites/default/files/2019-08/Final%20Complaint%20AdTech%20Criteo%2C%20Quantcast%20and%20Tapad%20%28FR%20ENCH%29\\_0.pdf](https://privacyinternational.org/sites/default/files/2019-08/Final%20Complaint%20AdTech%20Criteo%2C%20Quantcast%20and%20Tapad%20%28FR%20ENCH%29_0.pdf)) (viewed on 01/06/2020)

<sup>12</sup> <https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem> (viewed on 01/06/2020)

<sup>13</sup> The UK Information Commissioner has been investigating AdTech, in particular RTB throughout 2019 (<https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/>) and has ongoing investigations into Acxiom, Experian and Equifax. In May 2019, the Irish Data Protection Commission announced its investigation into Quantcast, following PI’s submission (<https://www.dataprotection.ie/en/news-media/press-releases/data-protection->

As a publisher, Doctissimo integrates and relies on the technologies developed and offered by AdTech companies to commercialise its audience through advertising. Publishers like Doctissimo play a key role in the expansion of the AdTech ecosystem by participating in the deployment of tracking technologies across their services. Publishers embedding tracking and uniquely identifying technologies facilitate a myriad of third-party actors collecting vast amounts of personal data, including sensitive personal data – often under the guise of bundled ‘consent’ processes which leaves little room for user control. In this regard, some publishers are complicit and enable a privacy invasive ecosystem to thrive by not properly assessing and limiting the privacy impact of the advertising solutions they implement.

It is against this background and in this context that PI raises its concerns regarding Doctissimo’s infringements of GDPR and the Loi Informatique et Libertés .

## Privacy International investigation

### “Your mental health for sale” report – September 2019

PI’s investigation of Doctissimo was part of a larger research project “Your mental health for sale”<sup>14</sup> which looked into the data practices of multiple dedicated health websites in France, Germany and the United Kingdom. The research was two-fold:

1. A static analysis of the 136 most visited depression-related webpages in France, Germany and the United Kingdom before any action is taken by a user. This included number and qualification of third parties loaded, number of cookies set, number of scripts loaded, etc. The open source web scrapper Webxray<sup>15</sup> was used to conduct this analysis.
2. A dynamic network analysis of the data shared by the top 9 websites (within the 136 websites) offering depression tests. This analysis focused on data shared with third parties while taking the test as well as on the

---

[commission-opens-statutory-inquiry-quantcast](https://privacyinternational.org/news-analysis/3404/french-regulator-launches-investigation-criteo-following-pis-complaint)) and in February 2020, CNIL confirmed its investigation Criteo (<https://privacyinternational.org/news-analysis/3404/french-regulator-launches-investigation-criteo-following-pis-complaint>) (all viewed on 01/06/2020)

<sup>14</sup> <https://privacyinternational.org/campaigns/your-mental-health-sale> (viewed on 01/06/2020)

<sup>15</sup> <https://webxray.org> (viewed on 01/06/2020)

cookies set and the consent mechanisms deployed by the publishers. The open source network analyser HTTP Toolkit<sup>16</sup> was used to conduct this analysis.

This research revealed a number of concerning facts:

- 97.78% of all web pages PI analysed contained a third-party element, such as a third-party cookie, third-party JavaScript or an image hosted on a third-party server. Some third-party elements provide useful features, such as fonts or visual effects and are not primarily designed to collect data from the users visiting the page that load these resources. That said, integrating third-party services comes with an inherent privacy risk for users. Websites that contact third parties typically communicate the fact that a particular browser has opened a specific URL (often, in combination with more data related to the operating system, browsers, language settings etc.). Mental health websites often reveal lots of information, simply because it is contained in the URL (i.e. /symptoms/depression/help)
- While third parties can provide useful services, PI's research showed that the predominant motivation to include third-party elements on mental health websites seems to be tracking for advertising and marketing purposes. According to Webxray's classification, 76.04% of the analysed web pages contained third-party trackers for marketing purposes.
- Google, Facebook and Amazon trackers were present on many of the web pages PI scanned. Google's advertising services DoubleClick and AdSense, for instance, were used by the vast majority of web pages we analysed. 70.39% of all web pages we analysed use trackers by DoubleClick. Facebook is the second most common third-party tracker after Google. Amazon Marketing Services is also one of the most common third parties present on the web pages analysed.
- Depression-related web pages also used a large number of third-party tracking cookies, which were placed before users were able to express (or refuse) consent. On average, the mental health web pages PI analysed placed 44.49 cookies in France, 7.82 for Germany and 12.24 for the UK.
- Numerous mental health websites include trackers from data brokers, and AdTech companies, which are already facing scrutiny by regulators

---

<sup>16</sup> <https://http toolkit.tech> (viewed on 01/06/2020)

and raise specific privacy concerns when used on health-related websites.

In the context of the dynamic analysis run on a subset of websites offering depression tests (top 3 results in France, Germany and United Kingdom), PI found that:

- Some depression test websites ([doctissimo.fr](https://doctissimo.fr), [netdokter.de](https://netdokter.de) and [passeportsante.net](https://passeportsante.net)) use programmatic advertising with Real Time Bidding ("RTB"). Use of programmatic advertising with RTB risks sharing data relating to health with hundreds of companies in the RTB ecosystem. Typically, this includes information about the device used, or where a user is located. We found that in the case of some depression test websites we analysed this also included granular information about the exact web page people visited, and, as a result, what health conditions they had been looking at.
- A number of depression test websites store users' answers to the tests as variables (e.g. 1 = yes, and 0 = no) and share answers, as well as test results with third parties in the URL. Two websites (PasseportSanté and [depression.org.nz](https://depression.org.nz)) stored test results as variables in the URL, which is being shared with all third parties that the website contacts.
- As explored in more detail in this submission, [Doctissimo.fr](https://Doctissimo.fr) shares test related data with a third party directly. The website sends test answers, together with a unique identifier, to [player.qualifio.com](https://player.qualifio.com). Because Qualifio provides the test form, the company knows the test's questions and answers. As a result, the company knows how uniquely identifiable individuals have responded to each of the questions in the depression test. Because the request is sent in HTTP, instead of HTTPS, the request is also potentially susceptible to interception.

### **Doctissimo follow up investigation – January to May 2020**

PI's investigation of Doctissimo was extended after the initial research (set out above) to follow up on our findings and for the purpose of this complaint.



The follow-up investigation at the end of January/ early February 2020<sup>17</sup> included:

1. A second and third static analysis to study the evolution of metrics previously collected (number of third parties, cookies etc.).
2. A follow up dynamic network analysis extended to other tests offered by Doctissimo.
3. An in-depth analysis of the consent mechanism deployed on Doctissimo.
4. A dynamic analysis of the permissions required by the apps offered by Doctissimo.
5. An analysis of the company's privacy policies.

In addition, in May 2020, PI conducted a review of the Covid-19 chat bot available on Doctissimo's website since 19 March 2020<sup>18</sup>.

The details of this investigation as well as the findings for each step are detailed below:

## 1 - Static analysis (webxray)

We used the open-source software tool webxray to detect third-party HTTP requests and cookies. Webxray is designed to analyse third-party content on webpages and identify the companies that are collecting user data. It is an open-source tool that has been used in prior web privacy measurement studies.

Webxray uses a custom library of domain ownership to chart the flow of data from a given third-party domain to a corporate owner, and, if applicable, to parent companies. For example, webxray will tell you that the domain "[doubleclick.net](https://doubleclick.net)" is owned by the DoubleClick service, which is a subsidiary of Google, which is a subsidiary of Alphabet. The webxray library also categorises domain ownership to evaluate why a website may have chosen to

---

<sup>17</sup> Technical analysis carried out 31 January 2020 – followed up by analysis published on 6 February 2020 <https://privacyinternational.org/report/3351/mental-health-websites-dont-have-sell-your-data-most-still-do> (viewed on 01/06/2020)

<sup>18</sup> "Des questions sur le coronavirus ? Doctissimo, TF1 et LCI lancent un chatbot pour vous répondre en direct": <https://www.doctissimo.fr/sante/epidemie/coronavirus-chinois/chatbot-coronavirus> (viewed on 01/06/2020)

include content for the given service (e.g. audience measurement, marketing, social media, compliance or content hosting).

Once the sets of pages are established, webxray is given a list of URLs and loads each page in the Chrome web browser, closely reflecting the real behaviour of a user. During page loading the browser waits 45 seconds to allow page scripts to download and execute. For each page load, webxray creates a fresh Chrome user profile which is free of prior browsing history and cookie data. During page loading no interaction takes place, meaning that notifications to accept cookies are not acted on, and thus any cookies set are done so without any action by the user/ express user consent. Once a website has been scanned, webxray stores the data that is collected (third-party elements loaded, cookies stored, JavaScript, etc.) in a database. Webxray then produces an analysis of the data collected and generates analytical reports including information about the percentage of pages using third-party elements, the number of cookies stored, the third party most often detected or number of unsecure connections to third parties (non-SSL connections). A complete list of the default reports generated by webxray can be found on the official webxray website.<sup>19</sup>

Using webxray PI was able to establish that the following happens as soon as the page is loaded and without any action from the user (as the browser executing the requests has no user interface):

- [Doctissimo's page on depression](#) sends 71 requests to 41 third-party domains (first scan);
- As a point of comparison, in the dataset PI examined (42 webpages) Doctissimo ranks 11 in the number of third-parties it sends request to on loading, the maximum being 50 ([passportsante.fr](#)) and the minimum 1 ([info-depression.fr](#));
- Most of these third parties have marketing purposes, including major AdTech players such as: Criteo, AppNexus, AdSense, The Trade Desk, Rubicon Project, AdYouLike, Quantcast, Xiti and more (complete list available in annex);
- Some of the URLs clearly state the bidding purpose of the query such as [e.serverbid.com](#)

---

<sup>19</sup> <https://webxray.org> (viewed on 01/06/2020)

Using Chrome developer tools PI was able to further inspect what happens when a page is loaded without any user interaction. For example, on the page <https://www.doctissimo.fr/html/dossiers/depression/articles/9032-deprime-signes.htm> the following can be observed:

- Doctissimo places 23 cookies associated with 10 third parties
- 22 out of 23 of these cookies have a tracking/targeting purpose (according to cookiepedia<sup>20</sup>)

This is problematic for a number of reasons:

1. The requests made to third parties include potentially revealing data such as the referrer URL (URL being visited by the user which can include revealing keywords such as "depression", "coup de blues" as demonstrated in PI's research) as well as browser information which can be used to uniquely identify users via fingerprinting techniques;
2. Associated with the cookies these requests potentially allow third parties to uniquely identify the visitor (if they have visited another site implementing a similar technology) and therefore enrich the user profile. This is even more problematic if the page visited relates to sensitive personal data, which is this case with depression tests;
3. All of this happens before the user has a chance to consent or refuse.

## 2 - Dynamic analysis (HTTP Toolkit)

To complement the static analysis, PI used HTTP toolkit<sup>21</sup> in order to inspect the queries to the third parties detailed above as well as any other emerging query. This was done both on Doctissimo pages providing information (article type) and on tests.

The analysis consisted of the following steps:

1. Open HTTP toolkit and launch the embedded version of Firefox or Chrome. The interception starts automatically
2. Open the page to analyse

---

<sup>20</sup> <https://cookiepedia.co.uk> (viewed on 01/06/2020)

<sup>21</sup> HTTP Toolkit (<https://httptoolkit.tech/>) is an open source software that allows interception and analysis of HTTP traffic. By conducting a man-in-the-middle attack through the use of Certificate Authority it also allows decryption of SSL encrypted traffic, giving us the possibility to read data exchanged in HTTPS.

3. If the page is an online test: Answer test questions and press "suivant"
4. Look at the requests, which are collected by HTTP toolkit in the view section
5. Isolate POST requests and inspect the data sent
6. Use the HTTP toolkit search to search for relevant keywords in the GET requests (within the URL). Keywords include:
  - "RTB", "bid", "pre-bid" to find RTB-related queries
  - If the page is a test: Terms related to the test mechanics such as "question", "answers", "response", "A=", "R=", "score" etc.
  - Literal answers to test question
  - Other terms related to mental health (such as "depression")
7. Use <https://www.urldecoder.org/> to make the URLs more readable and inspect any data passed this way

### Key problematic elements observed as the results of this analysis:

1. Doctissimo uses **programmatic advertising with RTB**, therefore broadcasting potentially sensitive personal data to a vast array of advertisers.

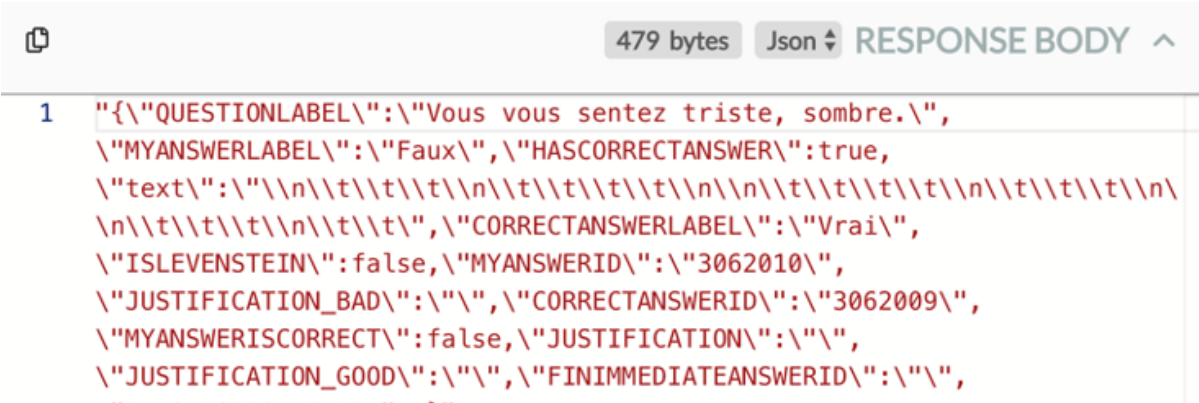
RTB requests include keywords related to the page being viewed as well as uniquely identifying information to be able to serve ads. The screenshot below shows the data that is included in a prebid request from [Doctissimo.fr](https://www.doctissimo.fr), which is sent to <https://europe-west1-realtime-logging-228816.cloudfunctions.net/realtime-logs> (a cloud function hosted by Google that will process the request). [Doctissimo.fr](https://www.doctissimo.fr) shares content keywords such as 'dépression', 'déprimé', or 'quizz', the page URL (psychologie/tests-psycho/tests-pstchologiques/coup-de-blues-ou-depression), as well as information about the page content ('psychologie', 'test psychologiques', 'coup de blues ou dépression?'). These keywords clearly communicate that a user is looking for information about depression and is possibly taking a depression test.

```
cm_client=doctissimo;
cm_rubrique=tests-psycho;
cm_section=Test;
level1=psychologie;
level_1=Psychologie;
level2=tests-psycho;
level_2=Tests Psycho;
level3=tests-psychologiques;
level_3=Tests Psychologiques;
level4=coup-de-blues-ou-depression;
level_4=Coup de blues ou dépression ?;
user_id=NaN;
new_visitor=1;
content_keywords=blues,coup,depression,deprime,doctissimo,gratuit,personnalite,psycho,psychologie,quiz,quizz,test;
url=/psychologie/tests-psycho/tests-psychologiques/coup-de-blues-ou-depression;
visitor=1563547374145361;
session=2;
```

Figure 1 - Extract from a POST request from Doctissimo to a Google Cloud Function including keywords

Prebid requests are typically used for header bidding to display video ads on a publisher's website. Header bidding is a form of programmatic advertising, in which a website shares its visitor's personal data with one or more advertising exchanges. These exchanges then broadcast the data to hundreds of partner companies. Header bidding typically involves the broadcasting of personal data, but the sharing of health-related data is especially concerning.

2. When taking a test on [Doctissimo.fr](https://www.doctissimo.fr), answers to the test's questions are sent in clear text to third party, [player.qualifio.com](https://player.qualifio.com) in a POST request. This third party is not mentioned anywhere on Doctissimo. Therefore, the purpose of this sharing is not clear.



The screenshot shows a JSON response body with the following content:

```
1 {"QUESTIONLABEL\":\"Vous vous sentez triste, sombre.\",
  \"MYANSWERLABEL\":\"Faux\", \"HASCORRECTANSWER\":true,
  \"text\":\"\\n\\t\\t\\t\\t\\n\\t\\t\\t\\t\\t\\t\\n\\n\\t\\t\\t\\t\\t\\t\\n\\t\\t\\t\\t\\n\\n\\t\\t\\t\\t\\n\\t\\t\\t\",
  \"CORRECTANSWERLABEL\":\"Vrai\",
  \"ISLEVENSTEIN\":false, \"MYANSWERID\":\"3062010\",
  \"JUSTIFICATION_BAD\":\"\", \"CORRECTANSWERID\":\"3062009\",
  \"MYANSWERISCORRECT\":false, \"JUSTIFICATION\":\"\",
  \"JUSTIFICATION_GOOD\":\"\", \"FINIMMEDIATEANSWERID\":\"\",
```

Figure 2 - Example of data shared with Qualifio including the question and answer provided by the user

Similar information can be observed in the URL of GET requests sent to Qualifio. Qualifio provides the test and therefore knows all questions and answers to them.

## URL

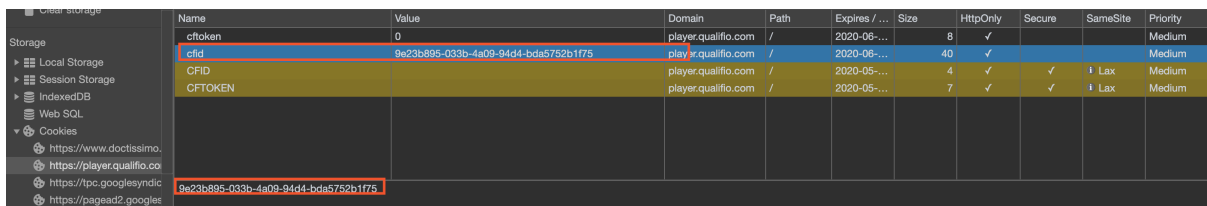
```
http://player.qualifio.com/20/ws/cfc/justification.cfc?method=answerJustification&id_client=292&id_reponse=3062010&id_question=1060062&displayCorrectAnswer=0&displayAnswerLabel=0&label_correct= Bonne+r%C3%A9ponse%26nbsp%3B!&label_bad=Mauvaise+r%C3%A9ponse&label_good_answer=La+bonne+r%C3%A9ponse+%C3%A9tait%26nbsp%3B%3A
```

Figure 3 - URL contacted by the user's browser when taking a test on doctissimo.fr. The URL includes parameters with the answer to the question, in this case id\_reponse=3062010. Testing demonstrated that the values are fixed (3062010 is always "Vrai")

Qualifio also places a cookie in the user's browser, which contains a unique identifier. As a result, the answers to the depression test questions that Doctissimo sends to Qualifio, can be linked to a uniquely identifiable individual.

While the initial research was focused on Doctissimo's depression test, a quick analysis shows that all the tests on doctissimo.fr rely on the same technology offered by Qualifio. This means that Qualifio, an unidentified third party, receives all the answers given by visitors to all Doctissimo tests (some of which are very sensitive information) without users' knowledge or consent.

It is also worth noting that this unique identifier used by Qualifio is not limited to the site it's being implemented on. Further testing demonstrated that the ID stored in the cookie by Qualifio is used globally, meaning that all actions taken by the user on multiple sites will be linked together, consolidating a unique user profile.



Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Priority
cfid	9e23b895-033b-4a09-94d4-bda5752b1f75	player.qualifio.com	/	2020-06-...	40	✓	✓	Lax	Medium
CFID		player.qualifio.com	/	2020-05-...	4	✓	✓	Lax	Medium
CFTOKEN		player.qualifio.com	/	2020-05-...	7	✓	✓	Lax	Medium

Figure 4 - Example of a Qualifio cookie on Doctissimo's site

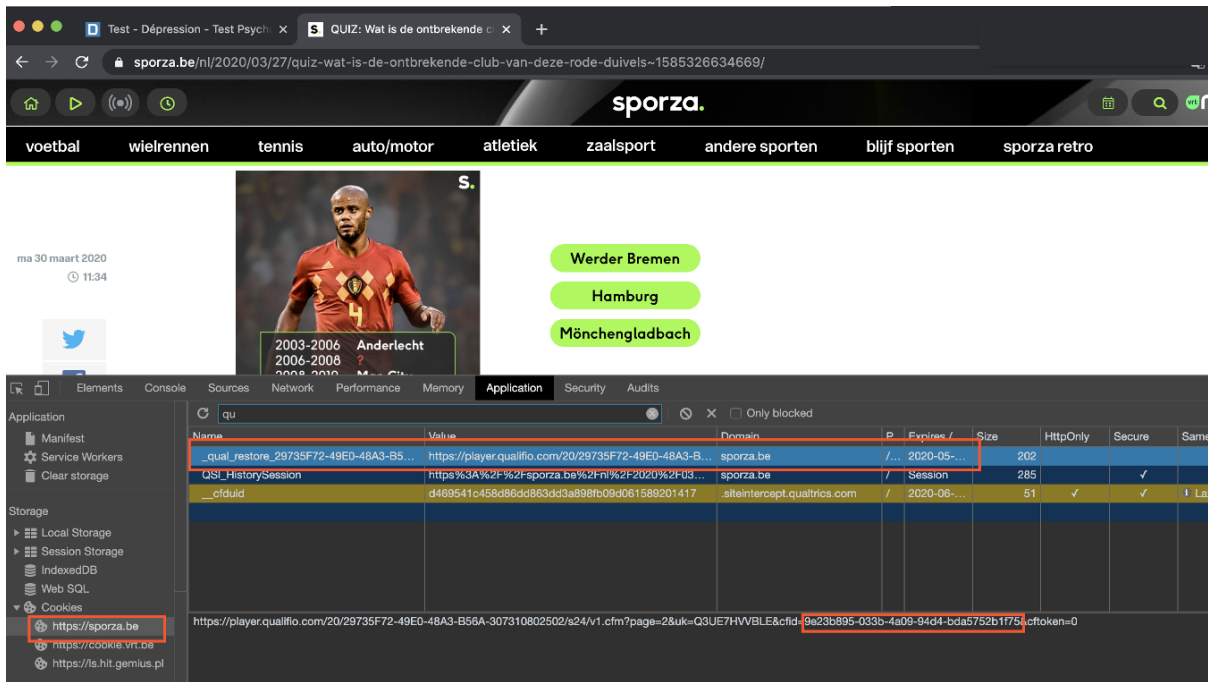


Figure 5 - Same cookie and unique ID used on sporza.be, a football site

3. The Covid-19 chatbot is sharing data with third parties without sufficient information and control for the users.

We also used HTTP Toolkit combined with Chrome’s developer’s tools to carry out a technical analysis of the Covid-19 chatbot.

We observed that when using the Covid-19 chatbot available on Doctissimo’s website since March 2020, all questions asked (either by typing it or clicking on one of the suggested questions) are sent to clustaar.io. Data collection for the purpose of best responding to a user’s questions, is clearly mentioned when starting a conversation, at which point users are asked if they accept the collection of their data in an anonymous manner and the bot is clearly labelled as “powered by clustaar”. However, clustaar.io is never mentioned as a data processor or recipient of data in the privacy policy which users are directed towards.

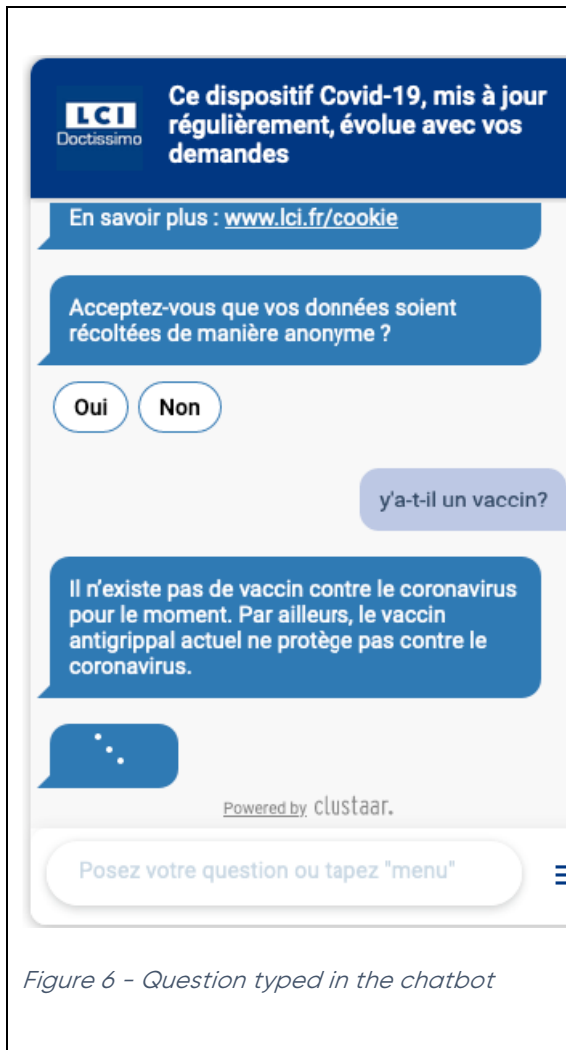


Figure 6 - Question typed in the chatbot

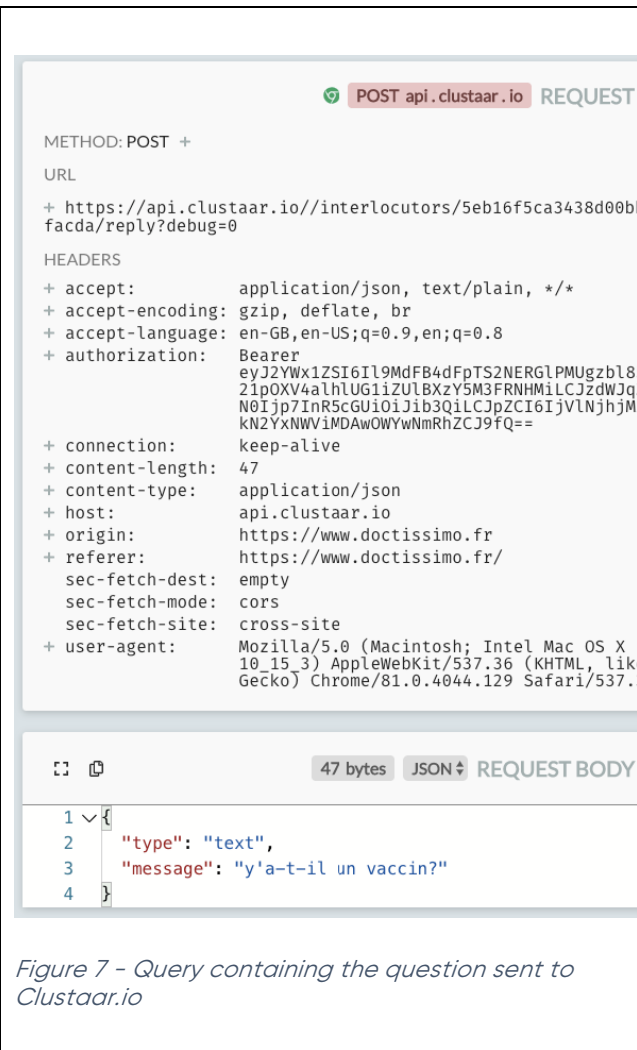


Figure 7 - Query containing the question sent to Clustaar.io

Users are assigned a unique ID which is consistent across questions asked allowing clustaar to create a unique profile that can be linked to everything that is typed by the user or clicked within the chat (links, suggested question or answers).

In some cases, the use of a unique identifier may be necessary for messaging technology in order to create and maintain a unique session between the user and the server operating the chatbot. However, users must still be clearly informed that all interactions with the chatbot will be processed by a third party and given details as to how this data will be used. As set out above, this not the case on Doctissimo's chatbot.



POST api.clustaar.io REQUEST

METHOD: POST +

URL  
+ https://api.clustaar.io/interlocutors/5eb16f5ca3438d00bb6fcda7/reply?debug=0

HEADERS

```
+ accept: application/json, text/plain, */*
+ accept-encoding: gzip, deflate, br
+ accept-language: en-GB,en-US;q=0.9,en;q=0.8
+ authorization: Bearer eyJ2YWx1ZSI6Ij9MdFB4dFpTS2NERGLPMUgzbl85V2p0XV4alhLUG1iZULBxzY5M3FRNHMiLCJzdWJqZWNOIj07InR5cGUiOiJib3QiLCJpZCI6IjVlNjhjMzNkN2YyWViMDAwOWYwNmRhZCJ9FQ==
+ connection: keep-alive
+ content-length: 47
+ content-type: application/json
+ host: api.clustaar.io
+ origin: https://www.doctissimo.fr
+ referer: https://www.doctissimo.fr/
  sec-fetch-dest: empty
  sec-fetch-mode: cors
  sec-fetch-site: cross-site
+ user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36
```

47 bytes JSON REQUEST BODY

```
1 {
2   "type": "text",
3   "message": "j'ai mal a la gorge"
4 }
```

Figure 8 – Request 1 with Unique ID

POST api.clustaar.io REQUEST

METHOD: POST +

URL  
+ https://api.clustaar.io/interlocutors/5eb16f5ca3438d00bb6fcda7/reply?debug=0

HEADERS

```
+ accept: application/json, text/plain, */*
+ accept-encoding: gzip, deflate, br
+ accept-language: en-GB,en-US;q=0.9,en;q=0.8
+ authorization: Bearer eyJ2YWx1ZSI6Ij9MdFB4dFpTS2NERGLPMUgzbl85V2p0XV4alhLUG1iZULBxzY5M3FRNHMiLCJzdWJqZWNOIj07InR5cGUiOiJib3QiLCJpZCI6IjVlNjhjMzNkN2YyWViMDAwOWYwNmRhZCJ9FQ==
+ connection: keep-alive
+ content-length: 126
+ content-type: application/json
+ host: api.clustaar.io
+ origin: https://www.doctissimo.fr
+ referer: https://www.doctissimo.fr/
  sec-fetch-dest: empty
  sec-fetch-mode: cors
  sec-fetch-site: cross-site
+ user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36
```

126 bytes JSON REQUEST BODY

```
1 {
2   "type": "go_to_action",
3   "target": {
4     "id": "5e75078940a749014c1fa906",
5     "type": "step",
6     "name": "Autres symptômes"
7   },
8   "sessionValues": {}
9 }
```

Figure 9 – Request 2 with the same unique ID

We also observed requests made to heatmap.it every time something is clicked on the page. Heatmap (<https://heatmap.com/>) is a company that provides heatmaps and real-time analytics of webpages to track clicks on a page. This may not be linked to the chatbot itself but the requests clearly reference Clustaar and Doctissimo meaning Heatmap knows that the user is interacting with the chatbot on Doctissimo.

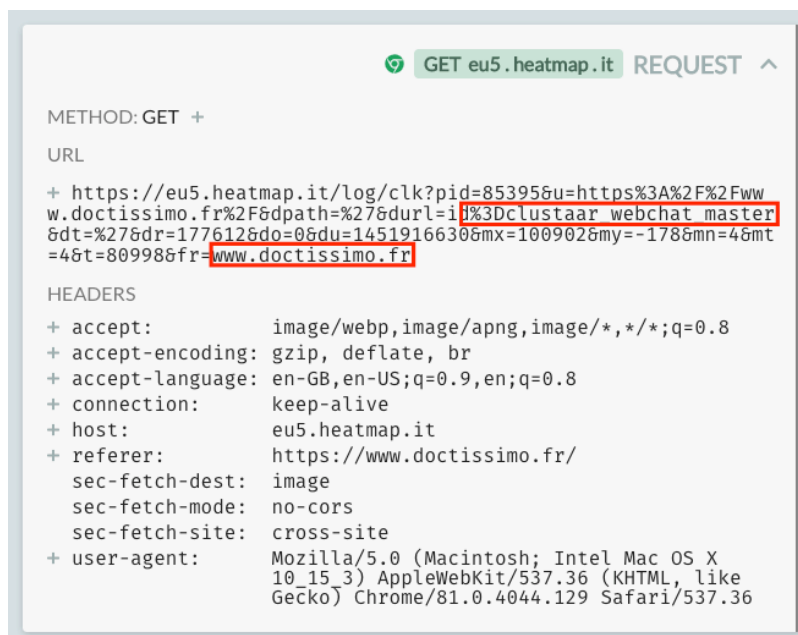


Figure 10 – Request from Doctissimo to heatmap.it including the name of the chatbot and the url of Doctissimo

### 3 – Consent mechanism

#### 1. Doctissimo website

When you first load the Doctissimo webpage, a notification appears at the bottom of the page.

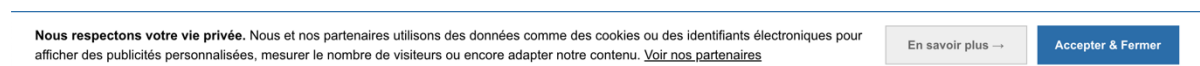


Figure 11 – Screenshot of Doctissimo 'Consent' Banner - 1 May 2020

The "Accept and Close" option is highlighted by default. With no immediate option of how to refuse. If you scroll down the page or clicking anywhere on the page the notification disappears, Doctissimo considers this an expression of consent. As set out in more detail below, this fails to constitute valid consent in line with the GDPR and Article 82 of the Loi Informatique et Libertés,

as supported by the CNIL recommendations and guidelines from the European Data Protection Board (“EDPB”).<sup>22</sup>

If you click on “Learn more” you are faced with a pop-up with a list of six purposes together with text informing you that you will also be consenting to Doctissimo partners processing your data, as well as to the processing of offline data, location data and device links. Again “Accept All” is highlighted by default.

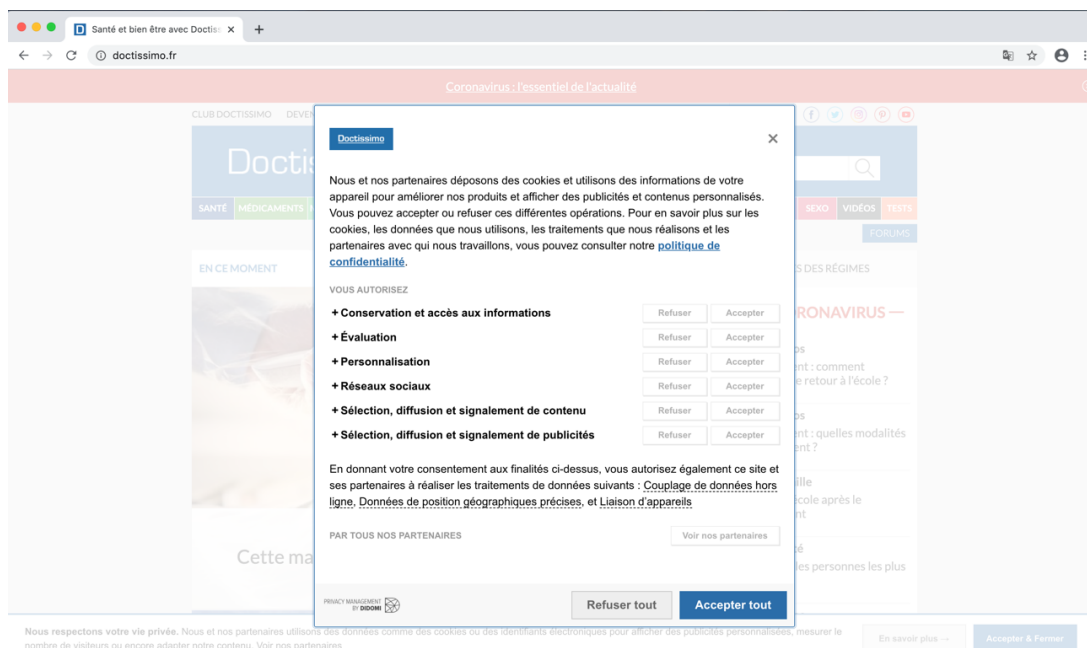


Figure 12 – Screenshot of ‘Learn More’/ ‘En savoir plus’ – 1 May 2020

There is an option in the first banner together with the larger pop up notice to see a list of Doctissimo’s partners, which leads you to a further screen with a list of 100s of partners.

<sup>22</sup> CNIL “Conformité RGPD : comment recueillir le consentement des personnes ?” (August 2018) <https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes> and EDPB Guidelines 05/2020 on consent under Regulation 2016/679 [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf) (links visited on 01/06/2020); Article 82 of the Loi Informatique et Libertés <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>

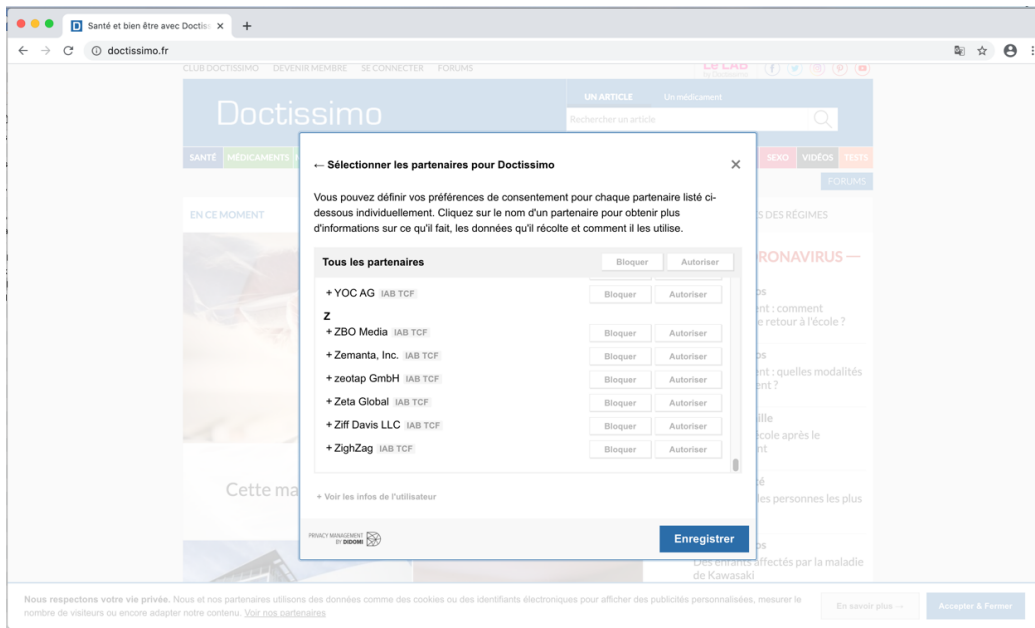


Figure 13 – Screenshot of long list of partners / 'Voir nos partenaires' - 1 May 2020

## 2. Covid-19 chatbot

The chatbot only opens after having 'consented' to sharing data with Doctissimo by clicking on the 'consent' banner or scrolling the site. The chatbot offers users the option to refuse data collection. If the user refuses to share data and confirms, the chatbot informs the user that they won't be able to use the feature anymore. Despite this message, taking any action (writing a question or clicking a suggested question) will still work and the observations made above remain (i.e. all actions and questions are transmitted to Clustaar under a unique identifier).

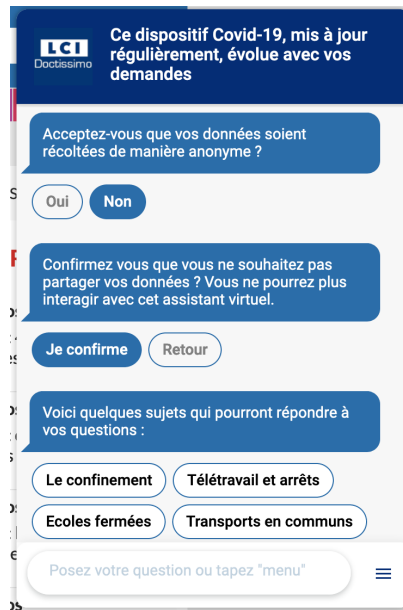


Figure 14 – Screenshot of the chatbot reaction after refusing data collection

A similar scenario occurs if the user does not answer the consent question posed by the chatbot. If the user starts interacting it will work straight away. Given how data is shared with Clustaar when using the bot, it appears that interaction with the bot is taken to be an expression of consent.

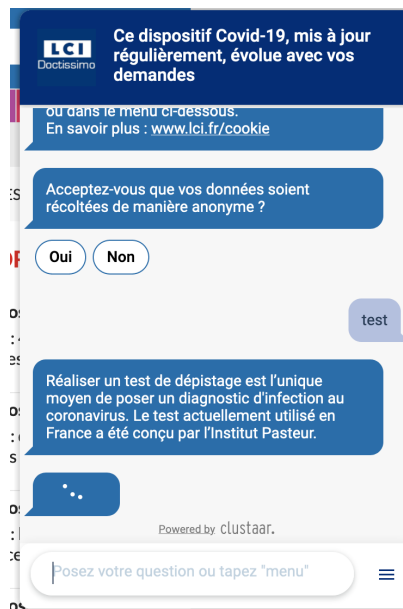


Figure 15 – Sending a message after refusing data collection returns a response showing the chatbot is functional

It is far from clear how the chatbot data will be used. The LCI cookie policy<sup>23</sup> (which the chatbot redirects to) does not mention the chatbot and only covers data collected through cookies. We could not locate any specific information on the LCI or Doctissimo website about how the chatbot data will be used.

#### 4 - Website access to location

When taking a test, the Doctissimo website asks to access the user location. Permission to access location is requested after the notice in the cookie banner has been accepted (which as noted above can be a simple click or scroll on the page). If permission is provided, location data is shared with [www.proxistore.com](http://www.proxistore.com), a geolocation based advertiser.

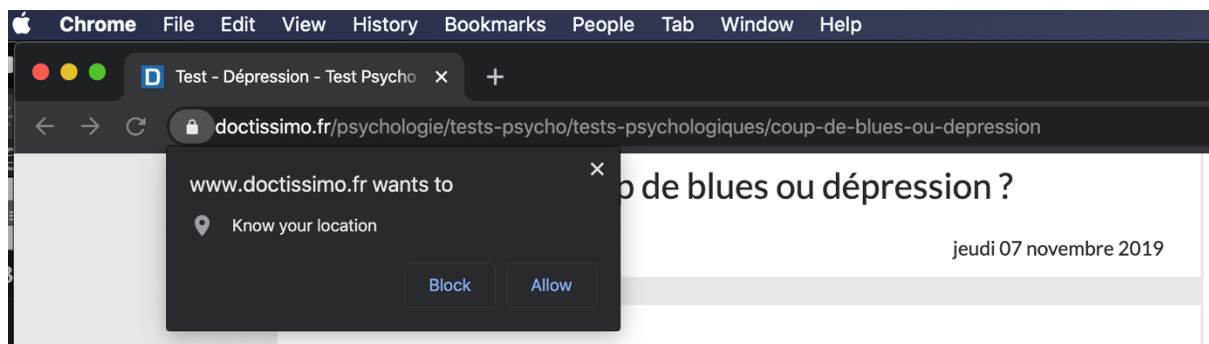


Figure 16 - Doctissimo's website asking for access to location

---

<sup>23</sup> <https://www.lci.fr/cookie> (viewed on 01/06/2020)

```
1  {
2    "geoCookieType": "HTML5",
3    "version": 4,
4    "geoHash": "gcpvjee",
5    "disqualified": false,
6    "countryIso2": "GB",
7    "countryIso3": "GBR",
8    "country": "United Kingdom",
9    "postalCode": "EC1R-0",
10   "locality": "London EC",
11   "areas": [
12     {
13       "level": "L6",
14       "label": "POSTAL CODE",
15       "code": "EC1R-0",
16       "name": "London EC"
17     }
18   ],
19   "html5Refusal": false
20 }
```

Figure 17 - POST request sent to proxistore.com and including semi-precise location data

Yet, by default and before the user has taken any action, location information is already shared with Proxistore as shown in the following request

```
METHOD: POST +
URL
+ https://abs.proxystore.com/fr/v3/rtb/prebid
HEADERS
+ accept: */*
+ accept-encoding: gzip, deflate, br
+ accept-language: en-GB,en-US;q=0.9,en;q=0.8
+ connection: keep-alive
+ content-length: 480
+ content-type: application/json
+ cookie: proxystore-uv=%7B%22id%22%3A%2297799700928461176%22%7D;
proxystore-geo-
ip=%7B%22geoCookieType%22%3A%22IP%22%2C%22version%22%3A%22%22geoHash%22%3A%22gcpvj37%22%2C%22disqualified%22%3A%22%22%2C%22countryIso%22%3A%22GB%22%2C%22countryIso3%22%3A%22GBR%22%2C%22country%22%3A%22United+Kingdom%22%2C%22postalCode%22%3A%22WC2R-3%22%2C%22locality%22%3A%22London+WC%22%2C%22areas%22%3A%5B%7B%22level%22%3A%22L6%22%2C%22label%22%3A%22POSTAL+CODE%22%2C%22code%22%3A%22WC2R-3%22%2C%22name%22%3A%22London+WC%22%7D%5D%2C%22html5Refusal%22%3A%22false%7D
+ host: abs.proxystore.com
+ origin: https://www.doctissimo.fr
  sec-fetch-dest: empty
  sec-fetch-mode: cors
  sec-fetch-site: cross-site
+ user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149
Safari/537.36
```

Figure 18 - POST request to proxystore.com including location data

## 5 – App permissions

PI also observed that the Doctissimo Apps (Club Docti- Forums Doctissimo and Ma Grossesse Doctissimo) also request permission to a lot of personal information which does not seem necessary for their main purpose:



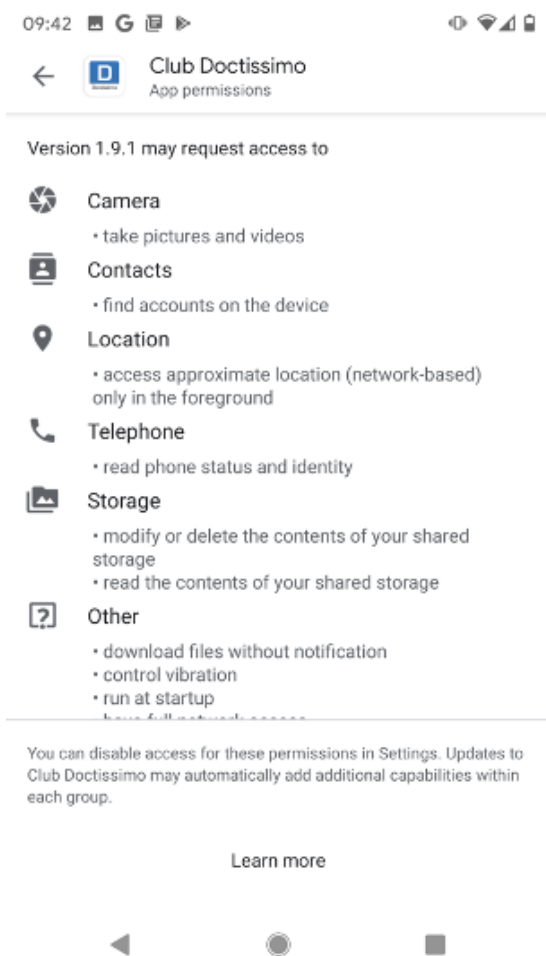


Figure 19 - Permissions for the app Club Doctissimo which gives access to Doctissimo's Forum

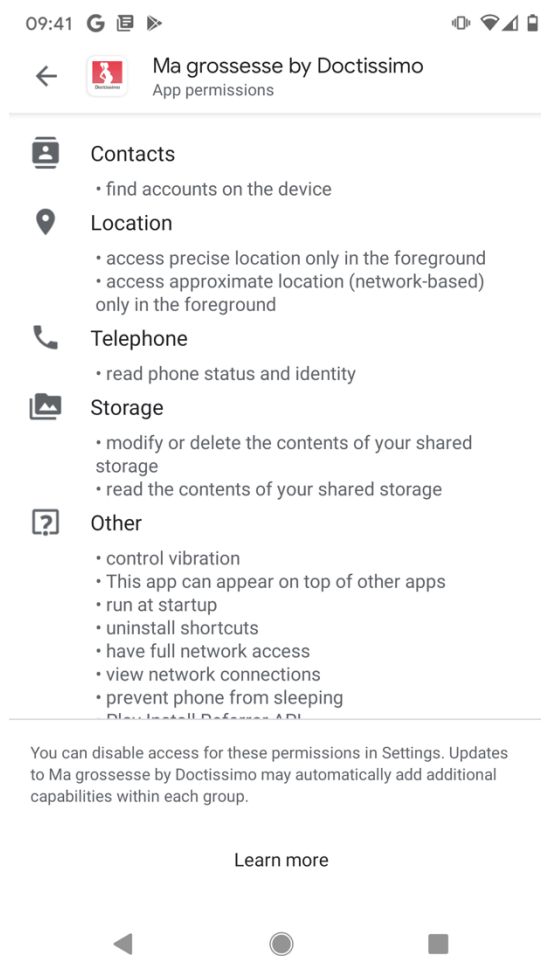


Figure 20 - Permissions for the app Ma Grossesse by Doctissimo, a pregnancy tracking app

## E. Legal Framework and Concerns

Our legal analysis and concerns are based on findings in PI's investigations set out in detail above as well as a review of Doctissimo's Privacy Policy.<sup>24</sup>

The data practices of Doctissimo give rise to substantial and on-going breaches of the GDPR and of the Loi n°78-17 of the 6 January 1978 dite *Loi*

<sup>24</sup> <https://www.doctissimo.fr/equipe/charte/charte-donnees-personnelles-cookies> (viewed on 01/06/2020)

*Informatique et Libertés*. The primary concerns that are set out in this submission are namely, that (i) the processing of personal data by Doctissimo is in breach of various data protection principles; (ii) the processing has no valid legal basis; (iii) the company did not implement some of the most basic security requirements; and (iv) the setting of cookies and other trackers on users' terminal equipment by Doctissimo and/or Doctissimo's commercial partners violates Article 82 of the *Loi Informatique et Libertés*.

The present complaint is structured to set out why the personal data processing of Doctissimo falls short of the requirements of the GDPR and Article 82 of the *Loi Informatique et Libertés*.

The submission starts with highlighting the company's failings in relation to some of the core data protection principles in Article 5 of the GDPR, including the requirement that processing be lawful and the failure to fulfil a valid legal basis under Articles 6 and 9 of the GDPR.

It then goes through Doctissimo's disregard of its obligation to implement appropriate technical and organisational measures as foreseen under Articles 25 and 32 of the GDPR.

Finally, the submission underlines the company's and third parties systematic installation of cookies and other trackers on users' devices regardless of their choices in violation of Article 82 of the *Loi Informatique et Libertés*.

### *The Data Protection Principles (Article 5 GDPR)*

#### ***1. Principle 1: Lawfulness, fairness and transparency***

As a data controller, Doctissimo must comply with the Data Protection Principles set out in Article 5 of the GDPR.

Article 5(1)(a) of the GDPR requires data to be "processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')."

#### ***(a) Transparency***

This sub-section of the submission deals with transparency. The issues of legality and fairness are addressed below.

A key issue with Doctissimo is its lack of transparency. While being one of the most consulted websites for health-related information in France, the company is far from clear when it comes to its participation in the AdTech ecosystem and how personal data, including special categories are being collected, used, shared or otherwise processed, including for profiling, in and outside of Doctissimo.fr.

This lack of transparency is most evident and concerning when it comes to the failure to provide information to data subjects that they are entitled to, particularly regarding recipients of personal data, as well as the very existence of many of these hidden processing operations.

#### Recipients of data are not transparent and easily accessible

Under the Transparency Principle and specifically Articles 12, 13 and 14 of the GDPR, a data subject is entitled to know the recipients or categories of recipients of their personal data. This information must be provided in a clear, intelligible and easily accessible form. The Article 29 Working Party Guidance on Transparency (endorsed by the EDPB) further specifies that:

*“The “easily accessible” element means that **the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question (for example in an online layered privacy statement/ notice, in FAQs, by way of contextual pop-ups which activate when a data subject fills in an online form, or in an interactive digital context through a chatbot interface, etc.**”<sup>25</sup> (emphasis added).*

The Article 29 Working Party Guidance on Transparency is also clear that detailed information on recipients is required:

“The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most

---

<sup>25</sup> WP29 Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) Page 7, [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=622227](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227) (viewed on 01/06/2020)

meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients."<sup>26</sup>

However, with the exception of seven commercial partners to whom personal data is to be transferred outside of the EEA (Appnexus, Zendesk, Dropbox, Cheetah Digital, Ligatus, Salesforce and Tag Commander), Doctissimo's Privacy Policy does not name any recipient of personal data. Rather, the Privacy Policy states that personal data *"may be transferred to third parties, such as commercial partners for purposes defined by such third parties that will be specified when consent will be collected"*. In practice data subjects only have two possibilities to find out which commercial entities their personal data may be shared with: (1) when visiting Doctissimo's webpage on a clean browser for the first time and clicking through two different greyed out links "En savoir plus" and "voir nos partenaires" contained in the 'consent' banner, bearing in mind that the latter automatically disappears from the moment users start scrolling the page; or (2) when clicking the link "Préférences cookies" contained at the bottom of the Doctissimo.fr page. They are then faced with a list of commercial partners containing hundreds of advertising companies.

At least two issues flow from this.

First, there is a significant gap between the language used in the privacy policy that makes the transfer of personal data to third parties sound purely hypothetical to the actual practise of the company that actively broadcasts vast amounts of personal data to hundreds of recipients by default from the very moment users start scrolling the page.

Second, users have to make significant efforts to find the information they are entitled to. Should they miss the information contained in the 'consent' banner, they have to access it via a tool that is presented to them as dedicated to cookie settings but in fact contains information related to all kinds of processing, including "offline data coupling, processing of location data and device linking". Overall, the information is disseminated in such a way that makes it extremely difficult to retrieve.

---

<sup>26</sup> Ibid, Page 37

## Hidden processing operations

Another important aspect of the Transparency Principle is that data subjects should be aware of the extent to which their personal data is processed. The Article 29 Working Party highlighted this in the Guidelines on Transparency:

*“A central consideration of the principle of transparency outlined in these provisions is that **the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used.**”<sup>27</sup> (emphasis added)*

In spite of Doctissimo’s transparency and accountability obligations, the company does not disclose an important number of sensitive processing operations to data subjects. This lack of transparency is most noticeable in the online tests offered on Doctissimo.fr, as well as in the company’s use of tracking and programmatic advertising.

Regarding online tests, neither Doctissimo’s Privacy Policy nor the aforementioned cookie tool makes any reference to Qualifio as a commercial partner. Yet, as demonstrated in PI’s investigations set out above, this company is behind over 300 tests accessible on Doctissimo.fr and, importantly, collects all the participants’ answers to the test questions. These answers include some data that could reveal special categories of personal data under Article 9 of the GDPR. Besides, they are compiled with those obtained from the multiple tests Qualifio offers online. As set out above, through the use of a “cfid” third party cookie, the company can indeed build detailed profiles of participants, no matter which site an individual takes part in a Qualifio test. This is especially concerning since this processing takes place without the data subjects’ knowledge.

As to Doctissimo’s use of tracking and programmatic advertising, the company’s mere participation in RTB involves much more data sharing and by extension profiling, than individuals are made aware of and/or would reasonably expect. It is only through static and dynamic analysis that PI could uncover the company’s broadcasting of sensitive data to hundreds of advertisers whose identities are hardly accessible as demonstrated above. PI’s

---

<sup>27</sup> Ibid, Page 7

research showed that header bidding on words such as “psychology”, “psychological test”, “coup de blues” or “depression” take place outside of any information provided to data subjects.

Doctissimo is required under the GDPR to provide data subjects with concise intelligible and easily accessible information about the processing of their personal data. The Article 29 Working Party (as endorsed and re-affirmed by the EDPB) has been clear that the more intrusive (or less expected) the processing is, the more important it is to provide such information in advance of the processing (in accordance with Articles 13 and 14).<sup>28</sup>

In this case, data subjects are not properly informed. As set out above and in PI’s investigation, again and again data is gathered and shared by Doctissimo, without clear information as to the fact that data is being collected, the purpose, the legal basis, who the recipients are, what will happen to the data including how long it will be stored and whether any profiling or automated decision-making takes place and if so, whether it complies with Article 22 of the GDPR.

#### Implications for data subject rights

These infringements entail a number of implications for the exercise of data subject rights. When data is collected on Doctissimo.fr, individuals often have no idea that over 550 companies could gather it, including companies that were previously investigated/ or under investigation by the CNIL, such as Criteo, Vectaury or Fidzup. It is only after thoroughly looking through the website that data subjects can locate Doctissimo’s long list of commercial partners, which contains no valid indication as to which of them has indeed processed their personal data. Such practises go against data subjects’ right to information as foreseen under Articles 13 and 14 of the GDPR. The lack of such information creates an immediate barrier to data subjects going onto exercise other rights, including the right of access in Article 15 of the GDPR, the right to erasure in Article 17 of the GDPR, the right to object in Article 21 of the GDPR (which is absolute in relation to direct marketing) and the right not to be subject to a decision based solely on automated decision making, including profiling which produces legal effects concerning them or significantly affects them as foreseen under Article 22 of the GDPR.

---

<sup>28</sup> Ibid, Page 8

Considering the extensive and intrusive nature of Doctissimo's data processing and the failure to provide the required information about it, the CNIL should examine the extent to which Doctissimo is fully complying with its transparency and information obligations under Article 5(1)(a) and Articles 12, 13 and 14 of the GDPR.

### *(b) Fairness*

The principle of fairness lies at the core of the GDPR and includes the requirement for controllers to consider the reasonable expectations of data subjects, the effect that the processing may have on them and their ability to exercise their rights in relation to that information. This includes the obligation to duly inform data subjects of any processing operation concerning them before such processing occurs. Depriving data subjects of this information could amount to a denial of the free exercise of their rights. In a judgment from the 14<sup>th</sup> of March 2006, the *Cour de Cassation* considered the collection of people's email addresses without their knowledge to constitute an unfair and unlawful processing operation in that such process hampers the exercise of the right of opposition.<sup>29</sup>

Similar considerations of fairness can and should be applied to Doctissimo data practices. Not only does Doctissimo not inform individuals in a meaningful way that their personal data is shared by default with hundreds of advertising companies, the company sometimes does not inform them at all of the existence of certain processing operations. Such is the case for instance when users take the tests provided by Qualifio accessible on Doctissimo's site as PI demonstrated. As such, the information Doctissimo provides is far from being either sufficient or meaningful, making the processing unfair.

In a 2019 IFOP survey ordered by the CNIL, no less than 90% of French people agreed on the necessity to know the identity of the companies likely to track their browsing activity through the use of cookies.<sup>30</sup> It follows that a vast majority of French users expect controllers to disclose the identity of commercial partners likely to track them online. Thus, the tracking of individuals through hidden processing operations cannot possibly take place within

---

<sup>29</sup> Crim. 14 mars 2006, n° 05-83.423 P. "est déloyal le fait de recueillir, à leur insu, des adresses électroniques personnelles de personnes physiques sur l'espace public d'internet, ce procédé faisant obstacle à leur droit d'opposition"

<sup>30</sup> See IFOP, « Les Français et la réglementation en matière de cookies » Sondage Ifop pour la CNIL, December 2019, page 19, <https://www.ifop.com/wp-content/uploads/2020/01/116921-Pr%C3%A9sentation.pdf> (viewed on 01/06/2020)

people's reasonable expectations. Furthermore, the widespread use and subsequent normalisation of such practices does not make them fair.

In this case, data subjects do not know or have the opportunity to agree to the multiple data processing operations concerning their data – this processing is not within their reasonable expectations. Consequently, Doctissimo's processing is unfair and in breach of Article 5(1)(a) of the GDPR.

### *(c) Lawfulness & Lawful Basis (Articles 6 and 9 GDPR)*

The first data protection principle in Article 5(1)(a) of the GDPR requires that personal data be processed lawfully and Article 6 of the GDPR sets out an exhaustive list of legal bases on which personal data can be processed.

Of these, the majority of the processing carried out by Doctissimo seems to be based on consent (Article 6(1)(a) of the GDPR). This is confirmed by Doctissimo's Privacy Policy.<sup>31</sup>

However, Doctissimo's processing of personal data is far from meeting the stringent requirements of consent as a valid lawful basis.

Consent is the only legal basis open to Doctissimo for this processing, as well as the basis stated by Doctissimo in their Privacy Policy, furthermore the processing involves data from users' terminal equipment for which consent is required in line with Article 82 of the Loi Informatique et Libertés. The requirements of Article 82 are set out towards the end of this submission. On this basis, we have not gone on to consider the other legal bases set out in Article 6 of GDPR as the lack of valid consent means this processing is unlawful. This breach of Article 6 of the GDPR should be investigated further by the CNIL.

### Consent

Consent as a legal basis should operate in a manner that gives individuals control and choice over the way their personal data is processed. Article 4(11) of the GDPR defines 'consent' for the purposes of the GDPR as:

---

<sup>31</sup> <https://www.doctissimo.fr/equipe/charte/charte-donnees-personnelles-cookies> (viewed on 01/06/2020)



*"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."*

Recitals (42) to (43) of the GDPR expand on the concerns underlying these requirements:

"(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, **safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given.** In accordance with Council Directive 93/13/EEC a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. **Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.**

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a **clear imbalance** between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. **Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."**  
(emphasis added)

Where processing is based on consent, Article 7 of the GDPR establishes additional conditions that a data controller must comply with in order that consent be valid. These include:

- The data controller must be able to demonstrate that the data subject has consented;

- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of the GDPR shall not be binding.
- The data subject has the right to withdraw their consent at any time. Such withdrawal must be as easy to exercise as the act to give consent in the first place.
- Consent should be freely given (it should not be procured as a result of an imbalance of power). In particular, utmost account has to be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

The EDPB Guidelines on Consent<sup>32</sup> under the GDPR provide a helpful overview of what these requirements mean in practice. In summary, consent must be:

- **Freely given** – this means there must be no imbalance of power between the data controller and the data subject; that the consent is not conditional; that consent is granular (i.e. does not conflate purposes for processing); and it must be possible for the data subject to refuse without detriment
- **Specific** – the data controller must apply purpose specification as a safeguard against function creep, consent requests must be granular and clearly separate information related to obtaining consent from information about other matters. The guidelines also state that “a controller that seeks consent for different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes”.
- **Informed** – the EDPB guidelines list a minimum of information that is required prior to obtaining valid consent. According to the guidelines “If

---

<sup>32</sup> European Data Protection Board, Guidelines on Consent under Regulation 2016/679, [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en) (viewed on 01/06/2020)

the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing”.

- **Unambiguous indication of the data subject’s wishes** – this is where an individual, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject must have taken a deliberate action to consent to the particular processing. The guidelines further specify that “The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement” and that “merely continuing the ordinary use of a website is not conduct from which one can infer an indication of wishes by the data subject to signify his or her agreement to a proposed processing operation”.

The EDPB also highlights that “consent must always be obtained **before** the controller starts processing personal data for which consent is needed” (emphasis added).

Doctissimo’s ‘consent’ banner and Privacy Policy<sup>33</sup> indicate that the company relies on consent as a lawful basis for a vast number of processing operations. Yet, the company is far from meeting the requirements set out above.

In this context, as set out in more detail above, PI’s static analysis of doctissimo.fr demonstrated how queries to third parties, including advertisers, are executed and cookies are dropped before consent can possibly be obtained. The static analysis was conducted in a headless browser with no user interaction.

Doctissimo’s failure to obtain valid consent is clearly demonstrated when taking the requirements of consent in turn.

### Freely given

Doctissimo allegedly collects data subjects’ consent through a banner deployed on Doctissimo.fr. Yet this banner does not provide data subjects with

---

<sup>33</sup> <https://www.doctissimo.fr/equipe/charte/charte-donnees-personnelles-cookies> (viewed on 01/06/2020)

a free choice. First, users are not provided with an immediate option to refuse consent. Second, the consent the company collects lacks granularity.

### No genuine choice

In order for consent to be freely given, the GDPR requires controllers to present data subjects with a genuine choice. In a report dedicated to dark patterns, the CNIL's digital innovation lab (LINC) highlighted two practises that strongly affect the ability of individuals to make such a choice by complicating it. When controllers make it fastidious to adjust confidential settings and when they obfuscate them.<sup>34</sup>

In the present case, Doctissimo did both.

First, the company is *"facilitating consent by a single action and making the process of data protection longer and complicated"*<sup>35</sup>. Users are indeed not only presented with a 'consent' banner that automatically disappears as soon as they start scrolling the page or interacting with the site (e.g.: by clicking a link), the banner in itself nudges them to accept all processing operations of their personal data through an "Accept & Close" button. It is only when users go through the greyed out "Find out more" button that they are presented with multiple settings and links. It follows that users are not presented with an immediate option to reject the processing operations of their personal data.

Second, the company created a *"deliberately long and tedious process to achieve the finest settings or [made] them so fine and complicated that they [...] encourage the user to give up before reaching their initial target"*.<sup>36</sup> Should users miss the 'consent' banner and start scrolling, they have to go through great lengths to locate the confidentiality settings contained in the "Préférences cookies" tool. Moreover, the options contained in the 'consent' banner are complicated and users could feel discouraged from adjusting the confidentiality settings when faced with the long list of Doctissimo's commercial partners.

---

<sup>34</sup> LINC CNIL, Shaping Choices in the Digital World, IP Reports Innovation and Foresight N°06, page 29, [https://www.cnil.fr/sites/default/files/atoms/files/cnil\\_ip\\_report\\_06\\_shaping\\_choices\\_in\\_the\\_digital\\_world.pdf](https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf) (viewed on 01/06/2020)

<sup>35</sup> Ibid

<sup>36</sup> Ibid

It follows that users are not presented with a clear and immediate option to say no to the processing of their personal data. Thus, the choice they are being offered cannot qualify as “genuine”.

### A lack of granularity

There is a significant lack of granularity in the consent Doctissimo seeks to obtain. The first level of the ‘consent’ banner presents users with a non-exhaustive list of overly broad purposes, such as “to better understand the use you make of the website” or “to offer you services, editorial content and advertisements that are adapted depending on your interests” and nudges users to click a blue “Accept & Close”. The only other option is a greyed out “Find out more” link.

In this configuration, consent is bundled since clicking “Accept & Close” or merely scrolling the page amounts to giving consent once for all purposes. Even the language of the banner seems to admit this bundling practice since it mentions that users have the possibility to exercise “*un choix plus granulaire*” by clicking on “*Find out more*”.

This second screen presents users with a list of 6 purposes (“Personnalisation”, “Sélection, diffusion et signalement de publicités”, “Evaluation”, “Sélection, diffusion et signalement de contenu”, “Réseaux sociaux”, “Conservation et accès aux informations”) with the apparent possibility to agree or reject the processing operations related to each one of them. Yet, once again consent is bundled since consenting to each of these purposes amounts to authorising over 550 Doctissimo partners to process users’ personal data.

In the Deliberation of the CNIL’s Restricted Committee of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, the Committee made the following observation:

*“(…) while certain user journeys may include a feature allowing the user to consent in a mutual way to the processing of their data for different purposes, this facility can only be considered as compliant if the different purposes of processing were presented to them in a distinct way beforehand, and they were able to give specific consent for each purpose, by a clear positive act, without boxes being pre-checked. In order for this type of user journey to be considered compliant, the option of giving specific consent for each purpose must be offered to people before the option “Accept all”, or “Refuse all”, and this must be*

*without them having to perform any particular action to access it, like clicking on "More options"*<sup>37</sup> (emphasis added).

Similarly, in this case, by conflating several purposes into the "Accept & Close" button and by forcing users to visit the "Find out more" tab to discover the different purposes, the consent Doctissimo seeks to obtain lacks granularity.

It follows that not only did Doctissimo fail to present users with a genuine choice and an immediate option to say no to its processing operations and those of its partners, it also bundled consent into a single "Accept & Close" button for multiple processing purposes. As such, the company implemented a consent mechanism that does not allow for users' free choice.

### Specific

Consent can only be specific when data subjects are specifically informed about the intended purposes of data use concerning them. According to the EDPB, this requirement aims to *"ensure a degree of user control and transparency for the data subject"*<sup>38</sup>. The Guidelines on consent further insist that *"specific consent can only be obtained when data subjects are specifically informed about the intended purposes of data use concerning them"*.<sup>39</sup> PI research illustrates several occasions where Doctissimo's consent requests severely lack specificity.

This is the case, for instance, when users take a test on Doctissimo.fr and they receive a browser notification asking them to consent to the sharing of their location data or when they install the Doctissimo apps such as Club Doctissimo or Ma Grossesse and are prompted to grant the company permission to access their contacts, location or phone status and identity.

Similarly, when data subjects interact with the Covid-19 Chatbot provided by Clustaar and are prompted to accept the collection of their data with little to no information on how this data will be used.

---

<sup>37</sup> Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC.

<sup>38</sup> European Data Protection Board, Guidelines on consent under Regulation 2016/679, [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en) (viewed on 01/06/2020)

<sup>39</sup> *Ibid* (viewed on 01/06/2020)

At no point in time during these consent notices, does Doctissimo provide users with the purposes for any of these processing operations. Users are left without any explanation as to why so much personal information should be necessary for the functioning of the service the company aims to offer.

This also goes against the language of the company's Privacy Policy, which indicates that the reasons for data processing will be provided, stating: *"La ou les raisons pour lesquelles les Données sont recueillies dans les formulaires de collecte sont précisées lors de cette collecte"*.

The fact that such practises are unfortunately widespread online does not make them less concerning or less unlawful. The consent that Doctissimo purports to obtain is not at all specific and the CNIL should investigate further.

### Informed

As set out above, the information Doctissimo provides its users with is far from being easily accessible and does not comply with the principle of transparency under Article 5(1)(a) of the GDPR. Beyond transparency obligations, the CNIL has highlighted<sup>40</sup> that in order to obtain informed consent, controllers should provide data subjects with a number of specific pieces of information, including the categories of personal data they intend to process. According to the CNIL, this information should be presented to users before consent is collected.

In this case, neither the consent notices on the website or chatbot nor Doctissimo's Privacy Policy make any reference to the processing of medical or health data. Yet, as Privacy International demonstrated, this type of information may be processed by Doctissimo, including for example, when users take a test on Doctissimo.fr or when they start interacting with the Covid-19 chatbot located on Doctissimo's homepage.

For instance, as set out above, as soon as users start taking a test on Doctissimo.fr, Qualifio, a company they will likely have never heard of and that is neither part of Doctissimo's long list of commercial partners nor referenced in Doctissimo's Privacy Policy, collects all the users' answers. Through the use of a third party "cfid" cookie, Qualifio may be able to build detailed profiles on individuals not only from the answers to this test and other Doctissimo test but

---

<sup>40</sup> <https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes> (viewed on 01/06/2020)

also from any other tests Qualifio provides across the internet that the user may take. As set out above, this processing, without informing data subjects, breaches the transparency principle and a data subject's right to information.

It follows that the consent Doctissimo collects could not possibly qualify as informed.

### Unambiguous

One of the most concerning and clear infringements of the consent requirements by Doctissimo is the need for consent to be unambiguous.

- Scrolling interpreted as 'consent'

First of all, the 'consent' banner deployed on Doctissimo.fr does not offer data subjects the possibility to perform a clear and affirmative action in order to consent. In the recent update to the WP29 guidelines on consent, the EDPB provided the following example:

*"Example 16: Based on recital 32, actions such as scrolling or swiping through a webpage or similar user activity will not under any circumstances satisfy the requirement of a clear and affirmative action: such actions may be difficult to distinguish from other activity or interaction by a user and therefore determining that an unambiguous consent has been obtained will also not be possible. Furthermore, in such a case, it will be difficult to provide a way for the user to withdraw consent in a manner that is as easy as granting it" (emphasis added)<sup>41</sup>.*

This example perfectly captures the conduct of Doctissimo in this case. Indeed, the language of the company's banner states that the mere scrolling on the site will be interpreted as consent to all processing: *"Pour accepter, nous vous invitons à poursuivre votre navigation (notamment au travers d'une action de scrolling) ou à cliquer sur Accepter & Fermer"*. The only way to refuse consent, as set out above, is to click through the banner settings, should the banner still be visible to data subjects or to visit the "preferences cookies" tool to access

---

<sup>41</sup> EDPB Guidelines on Consent under Regulation 2016/679, [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en) (viewed on 01/06/2020)



similar settings. As such, consent does not qualify as unambiguous. Furthermore, this consent is significantly harder to withdraw than it is to give, infringing Article 7(3) of the GDPR.

- Opt-out by default

Second, Doctissimo seems to be using opt-out mechanisms. When users visit the "Find out more" part of the 'consent' banner, they find greyed out control settings next to each of the purposes they are presented with, bearing the mention "Refuser" or "Accepter". The same observation can be made when users access the extremely long list of commercial partners accessible through the "voir nos partenaires" link on the same window with two greyed out options for each partner stating "Bloquer" or "Autoriser". By displaying such a design, Doctissimo is ambiguous as to whether or not the controls it provides users with are disabled by default, as the law requires. Should the data subjects refrain from engaging with the settings they are presented with, their consent will be stored by default.

As a result, the consent Doctissimo collects cannot possibly qualify as an unambiguous indication of the data subject's wishes for Doctissimo's processing, let alone the subsequent processing by hundreds of AdTech companies. PI<sup>42</sup> and others<sup>43</sup> have previously expressed concerns with the validity of consent replicated in this manner, including using the IAB Transparency and Consent Framework of which many of the companies Doctissimo shares data with are members, such as Criteo or Vectaury.

The consent Doctissimo supposedly collects therefore does not meet the threshold required under the GDPR since it is neither free, specific, informed, nor unambiguous. As consent is the stated legal basis of Doctissimo and given that no other legal basis in Article 6 of the GDPR would be valid in these circumstances, the processing has no legal basis and is unlawful, in violation of Article 5(1)(a) of the GDPR.

---

<sup>42</sup> PI AdTech complaint to the UK ICO, the Irish DPC and CNIL concerning AdTech companies, Criteo, Quantcast and Tapad: <https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem> (viewed on 01/06/2020)

<sup>43</sup> Complaint to the ICO by Jim Killock of Open Rights Group and Michael Veale, available at: <https://brave.com/ICO-Complaint-.pdf> ; and to the Irish DPC by Johnny Ryan available at: <https://brave.com/DPC-Complaint-Grounds-12-Sept-2018-RAN2018091217315865.pdf> (viewed on 01/06/2020)

## Sensitive/Special categories of personal data (Article 9 GDPR)

Article 9(1) of the GDPR prohibits the “processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning natural person’s sex life or sexual orientation”, unless one of the narrowly prescribed conditions in Article 9(2) of the GDPR or set out in national legislation is met. In this context, the only potentially applicable condition is that the data subject has given explicit consent (Article 9(2)(a) of the GDPR).

According to the CNIL, explicit consent requires controllers to obtain “*an express declaration by the data subject, which implies special attention and the setting up of ad hoc mechanisms*”.<sup>44</sup>

As PI’s research demonstrated, there are at least two occurrences where processing operations of data concerning health systematically take place on Doctissimo.fr.

First, in Doctissimo’s use of programmatic advertising with RTB, PI uncovered that Doctissimo.fr shares content keywords such as ‘dépression’, ‘déprimé’, ‘test psychologique’, which taken together communicate that a user is looking for information about depression and is possibly taking a depression test. Even though this information could clearly qualify as health-related data, Doctissimo still broadcasts it for header bidding purposes. Thus, this data is shared with hundreds of advertising companies without individuals’ knowledge or consent – let alone explicit consent.

Second, when taking an online test on Doctissimo.fr, questions and answers are systematically sent to Qualifio, a third-party unknown to users. Tests usually contain medical related information and include sensitive data, notably related to mental health, but also other special categories of personal data, such as personal data concerning sex life or sexual orientation. For instance, Doctissimo offers a full section with tests dedicated to sexuality named “Test Sexualité”.<sup>45</sup>

---

<sup>44</sup> <https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes> (viewed on 01/06/2020)

<sup>45</sup> <https://www.doctissimo.fr/tests> (viewed on 01/06/2020)

None of these situations is covered in Doctissimo's Privacy Policy, which strangely enough for an informational website dedicated to health - where users are invited to participate in a forum, take tests related to their health conditions or chat online about potential coronavirus symptoms they might experience - does not make a single reference to special categories of personal data. Nor, as set out above, do Doctissimo make any effort to request users' explicit consent.

Consequently, the processing of personal data revealing special categories, such as data concerning health or data concerning a person's sex life, by Doctissimo is not lawful and in breach of Article 5(1)(a) and Article 9(1) of the GDPR.

## *2. Principle 2: Purpose specification*

Article 5(1)(b) of the GDPR requires that personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ... ('purpose limitation')".

The Article 29 Working Party Opinion 03/2013 on purpose limitation<sup>46</sup> is clear that any purpose must be **specified** prior to, and in any event, no later than the time when the collection of personal data occurs - the purposes must be precisely and fully identified; **explicit**, sufficiently unambiguous and clearly expressed (i.e. no hidden purpose); and **legitimate**, in accordance with the law and within the reasonable expectations of the data subject.

The compliance assessment of the purpose of processing requires consideration of the context in which the data has been collected and the reasonable expectations of the data subject as to further use and also the nature of the data and the impact on the data subject.

There are several instances where Doctissimo does not sufficiently specify the purposes for its collection of users' personal data.

Such is the case, for instance, when users start use Doctissimo's apps, Club Doctissimo or Ma Grossesse, which may have access to an important range of data

---

<sup>46</sup> [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf) (viewed on 01/06/2020)

for poorly specified purposes or when they are prompted through a browser notification to accept sharing their location, as previously mentioned.

This is also the case when users try to understand how their data might be used by Doctissimo's 556 commercial partners. While the « Find out more » part of the 'consent' banner defines purposes such as « Conservation et accès aux informations », « Evaluation », « Personnalisation » or « Sélection, diffusion et signalement de publicités », it also casts much doubt as to the processing practises of these companies, and including those identified as participating in the IAB's Transparency and Consent Framework (TCF).

Indeed, each TCF participant is flagged with a number of broad purposes, such as « Conservation et accès aux informations » or « Personnalisation », but also with the following mention « *Vous pouvez en apprendre davantage sur ce partenaire et sur la façon dont il traite les données dans sa politique de confidentialité* », redirecting users to the partner's privacy policy. The purposes indicated are therefore misleading or at least ambiguous since data subjects are invited to find out more.

In fact, Doctissimo is expecting users to read over 550 privacy policies in order to find out the exact purposes for its partners' uses of personal data. As such, the partners' purposes are far from clearly stated or from meeting the reasonable expectations of data subjects, who besides facing an opt-out mechanism need to deploy disproportionate efforts in order to understand the uses of their personal data.

Thus, Doctissimo is in breach of the purpose-specification principle.

This is extremely concerning, especially since some of Doctissimo's partners include data brokers, such as Criteo and Oracle who were previously the subject of investigations and complaints by PI for their lack of compliance with European data protection law.

### *3. Principle 3: Data minimisation*

Article 5(1)(c) of the GDPR requires that personal data shall be "adequate, relevant and **limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation')".

Doctissimo engages in data maximisation. Any action users take on Doctissimo.fr

is closely tracked and monetised. The company is an active part of an AdTech ecosystem whose goal is to maximise the amount of information on individuals for profit – this means that the data of those using Doctissimo’s services may be used to analyse, profile, assess, categorise and may even inform decisions that are made about them. The complexity and opacity of the AdTech system to which Doctissimo’s feeds in its users’ data, means that ultimate consequences of this vast data gathering can be difficult to predict.

Whether it is the processing of users’ location data or that of their test answers or their browsing data, it is not clear how this processing is necessary and proportionate to the provision of the service Doctissimo offers, i.e. an informational website dedicated to health information. Doctissimo should consider how to offer its services in a way that least interferes with an individual’s rights to data protection and privacy, however, the amount of data processed by Doctissimo goes well beyond what is needed.

As such, Doctissimo is in breach of the data minimisation principle.

#### *Data Protection by design and by default (Article 25 GDPR)*

Under Article 25 of the GDPR, controllers have an obligation to implement Data Protection by Design and by Default. In its Guidelines on Article 25, the EDPB highlighted that this obligation relates essentially to the *“effective implementation of the data protection principles and data subjects’ rights and freedoms by design and by default”* through the implementation of *“appropriate technical and organisational measures and necessary safeguards, designed to implement data protection principles in an effective manner and to protect the rights and freedoms of data subjects”*.<sup>47</sup>

As set out above, Doctissimo does not comply with key data protection principles, including the principle of transparency, the principle of fairness, the principle of lawfulness, the principle of data minimisation and the principle of purpose specification. By doing so, the company disregards some essential data subjects’ rights, including the right to information under Articles 13 and 14 of the GDPR.

---

<sup>47</sup> See EDPB Guidelines on Article 25 GDPR, [https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_guidelines\\_201904\\_dataprotection\\_by\\_design\\_and\\_by\\_default.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf) (viewed on 01/06/2020)

PI's research uncovers a system where Doctissimo covertly processes vast amounts of personal data outside of any valid legal basis. As set out in the section on consent above, consent is the only possible legal basis available for the processing, and no valid consent is obtained. The design of Doctissimo's services and the default settings within them (as set out in detail above) are the antitheses of Data Protection by Design and by Default. As such, the company is in breach of its obligations under Article 25 of the GDPR.

### Security of processing (Article 32 GDPR)

Under Article 32 of the GDPR, controllers must protect personal data by taking *"appropriate technical and organisational measures to ensure a level of security appropriate to the risk"*.

PI and other organizations have consistently underlined the crucial security risks the AdTech ecosystem entails, especially in RTB where personal data is broadcasted to hundreds of advertisers.<sup>48</sup> This is confirmed by the UK ICO, in their report on AdTech, specifically RTB,<sup>49</sup>

"...once data is out of the hands of one party, essentially that party has no way to guarantee that the data will remain subject to appropriate protection and controls." Concluding that "Individuals have no guarantees about the security of their data within the ecosystem."<sup>50</sup>

As such, Doctissimo's mere participation in this ecosystem puts its users' personal data at risk.

Furthermore, in some instances it is clear that the company did not implement some basic security requirements. For example, the use of unencrypted POST

---

<sup>48</sup> PI AdTech complaint to the UK ICO, the Irish DPC and CNIL concerning AdTech companies, Criteo, Quantcast and Tapad: <https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem>; Complaints re behavioural advertising with a focus on security, filed 12/09/2018, to the ICO by Jim Killock of Open Rights Group and Michael Veale, available at: <https://brave.com/ICO-Complaint-.pdf>; and to the Irish DPC by Johnny Ryan available at: <https://brave.com/DPC-Complaint-Grounds-12-Sept-2018-RAN2018091217315865.pdf>; this is also highlighted by Polish NOG Panoptykon, in '10 Reasons Why Online Advertising is Broken' (January 2020) <https://en.panoptykon.org/online-advertising-is-broken> (all links visited on 01/06/2020)

<sup>49</sup> <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf> (viewed on 01/06/2020)

<sup>50</sup> <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf> (see pages 20 and 23) (viewed on 01/06/2020)

requests (HTTP), an unsafe transport method that should never be used when dealing with sensitive data as it allows anybody monitoring the traffic to see the data in clear.<sup>51</sup> As set out above, Doctissimo shares users answers to its online tests with Qualifio via HTTP . Considering the nature of these tests, their answers are likely to include Article 9 special categories of personal data. Thus, through the use of non-encrypted requests, Doctissimo is putting users' sensitive data at risk.

Therefore, it appears that Doctissimo's approach towards data security is quite concerning and the CNIL should investigate the company's compliance with its obligations under Article 32 of the GDPR.

### *Cookies and other trackers (Article 82 Loi Informatique et Libertés)*

Article 82 of the Loi Informatique et Libertés is the French implementation of Article 5(3) of the ePrivacy Directive and regulates the setting of cookies and other trackers on users' devices. In particular, this article provides that *"access or registration may only take place if the subscriber or user has expressed [...] his consent, which may result from the appropriate parameters of his connection device or any other device under his control"*.

Such consent must be interpreted in accordance with the criteria and conditions defined under Article 4 (11) and 7 of the GDPR set out above, as confirmed by the Court of Justice of the European Union (CJEU), the Conseil d'Etat and the CNIL.<sup>52</sup> These conditions and criteria must be respected regardless of whether the processing involves personal data.<sup>53</sup>

Therefore, controllers are required to obtain free, specific, informed and unambiguous consent prior to the installation of any cookie or tracker on users' devices.

This prior consent requirement does not apply only if access to information stored in the users' devices or the registration of information therein (1) has the exclusive purpose of allowing or facilitating communication by electronic

---

<sup>51</sup> [https://www.w3schools.com/tags/ref\\_httpmethods.asp](https://www.w3schools.com/tags/ref_httpmethods.asp) (viewed on 01/06/2020)

<sup>52</sup> See CJEU 1 October 2019, Planet49, C-673/17, ECLI:EU:C:2019:801; Conseil d'Etat, 10th - 9th Chambers, 16 October 2019, 433069; and CNIL, Deliberation n°2019-093 of 4 July 2019

<sup>53</sup> see Planet49, para 69

means; or (2) is strictly necessary for the provision of an online communication service at the user's express request.

These exceptions are strictly interpreted. For example, in a decision of 6 June 2018, the Conseil d'Etat considered that all cookies that are set for advertising purposes cannot be treated as cookies that are "*strictly necessary*" for the provision of an online communication service, even when such cookies are necessary for the economic viability of a website.<sup>54</sup>

As we previously mentioned, Doctissimo deploys a 'consent' banner on Doctissimo.fr, which aims to collect users' consent not only for a range of processing operations, but also for the setting of cookies. As set out in detail above, this consent does not fulfil the requirements of valid consent under the GDPR and thereby of Article 82 of the Loi Informatique et Libertés.

PI's research showed that cookies are set on users' devices before they have a chance to consent or refuse their installation. In fact, even when users go through the extensive steps of visiting the "preference cookies" tool Doctissimo provides and disable each cookie related feature contained therein, cookies are still set on their devices.

The vast majority of the trackers appear to be for advertising purposes and could not therefore qualify as being strictly necessary for the functioning of Doctissimo.fr.

Cookies may be used to associate unique identifiers with users and may contribute to profiling. For instance, as set out above, when taking an online test on Doctissimo.fr, PI observed that Qualifio sets a third party "cfid" cookie on users' devices. Through the ID stored in this cookie, Qualifio is able to retrieve any data that the user might have shared with them, such as questions and answers to the test, and may consolidate the profiles of test takers without their knowledge or consent. As a hypothetical example, a unique user who scored very high on Doctissimo's depression test and very high on a football test provided by Qualifio on another site, using the same browser, could possibly be profiled by Qualifio as a depressed football lover. Again, the lack of transparency by Doctissimo, in particular the sharing of data with Qualifio, makes it difficult for a user to ascertain whether their data may be used for profiling and if so, the extent of and details of such profiling.

---

<sup>54</sup> Conseil d'Etat, 10th - 9th chambers together, 06/06/2018, 412589



Given that opt-out mechanisms cannot amount to valid consent for the setting of advertising cookies and we do not consider there to be a valid exception in this case, it follows that Doctissimo and its partners set cookies in violation of Article 82 of the *Loi Informatique et Libertés*.

## F. Applications/ Remedy

### Request to Investigate

Privacy International hereby requests the CNIL to fully investigate this complaint, in accordance with the powers vested in it as the Data Protection Authority under Article 19, 20, 21, 22 and 23 of the *Loi Informatique et Libertés*, in order to determine in particular:

- (i) The processing operations carried out by the Data Controller in relation to the users of its services;
- (ii) The purposes of these processing operations;
- (iii) Their legal basis;
- (iv) The validity of the 'consent' banner deployed by the Data Controller
- (v) The compliance of the cookies and other trackers set by the Data Controller and its commercial partners

In addition, Privacy International requests that a copy of any record of processing activities (Article 30 the GDPR) be provided.

Finally, Privacy International would like to request that the results of this investigation are made available in the course of this procedure, in accordance with Article 77(2) of the GDPR.

### Request to prohibit the relevant processing operations

PI requests that the CNIL take the necessary measures in accordance with the powers conferred on it, including Article 58(1)(d) and (f) and Article 58(2)(c) of the GDPR in conjunction with Article 17 of the GDPR, to stop any hidden processing operations by the Data Controller, Doctissimo, in particular those outlined in this complaint. Similarly PI requests that the CNIL takes action to enforce Article 82 of the *Loi Informatique et Libertés* and prohibit any tracking, use of cookies and access to data, including those set out in this complaint, that fail to comply.

## Application for the imposition of effective, proportionate and dissuasive fines

Finally, we ask that the CNIL impose an effective, proportionate and dissuasive fine on the Data Controller pursuant to Article 20, III, 7° of the *Loi Informatique et Libertés*.

**Annex - List of Doctissimo partners on 19 May 2020  
(Total: 556)**

Tappx	Duplo Media AS	Perform Media Services Ltd
1plusX AG	Duration Media, LLC.	Performax.cz, s.r.o.
2KDirect, Inc. (dba iPromote)	DynAdmic	Permodo GmbH
33Across	Dynamic 1001 GmbH	Permutive
6Sense Insights, Inc.	EASYmedia GmbH	Permutive Technologies, Inc.
7Hops.com Inc. (ZergNet)	Effiliation	Pexi B.V.
A Million Ads Ltd	Effinity	pilotx.tv
A.Mob	Emerse Sverige AB	PIXIMEDIA SAS
Accelerize Inc.	emetriq GmbH	Platform161
Accorp Sp. z o.o.	EMX Digital LLC	Playbuzz Ltd.
Active Agent AG	Epsilon	PLAYGROUND XYZ EMEA LTD
Acuityads Inc.	Etarget SE	plista GmbH
ad6media	Eulerian Technologies	Pocketmath Pte Ltd
Adacado Technologies Inc. (DBA Adacado)	Exactag GmbH	Polar Mobile Group Inc.
adality GmbH	Exponential Interactive, Inc	PowerLinks Media Limited
ADARA MEDIA UNLIMITED	Eyeota Pte Ltd	Predicio
adbility media GmbH	Ezoic Inc.	PREX Programmatic Exchange GmbH&Co KG
AdClear GmbH	Facebook	Programatica de publicidad S.L.
AdColony, Inc.	Fandom, Inc.	Proxi.cloud Sp. z o.o.
AddApptr GmbH	Fidelity Media	PROXISTORE
AdDefend GmbH	Fidzup	Publicis Media GmbH
AdElement Media Solutions Pvt Ltd	Fifty Technology Limited	PubMatic, Inc.
Adello Group AG	Flashtalking, Inc.	PubNative GmbH
Adelphic LLC	FlexOffers.com, LLC	PulsePoint, Inc.
Adevinta Spain S.L.U.	Forensiq LLC	Qriously Ltd
Adform	Free Stream Media Corp. dba Samba TV	Qualifio
Adhese	Fusio by S4M	Quantcast International Limited
adhood.com	Fyber	Radio Net Media Limited

Adikteev / Emoteev	Gammed	Rakuten Marketing LLC
ADITION technologies AG	Gamoshi LTD	Readpeak Oy
Adkernel LLC	GDMServices, Inc. d/b/a FiksuDSP	Realeyes OU
Adledge	GeistM Technologies LTD	Reignn Platform Ltd
Adloox SA	Gemius SA	Relay42 Netherlands B.V.
Adludio Ltd	Genius Sports Media Limited	remerge GmbH
ADMAN - Phaistos Networks, S.A.	Getintent USA, inc.	Research and Analysis of Media in Sweden AB
ADman Interactive SLU	GlobalWebIndex	Revcontent, LLC
adMarketplace, Inc.	Go.pl sp. z o.o.	Reveal Mobile, Inc
AdMaxim Inc.	Goldbach Group AG	Rezonence Limited
Admedo Ltd	Golden Bees	RhythmOne LLC
admetrics GmbH	Good-Loop Ltd	Rich Audience
Admixer EU GmbH	Goodway Group, Inc.	RMSi Radio Marketing Service interactive GmbH
Adnami Aps	Google	Rockabox Media Ltd
Adobe Advertising Cloud	Google ad manager	Rockerbox, Inc
Adobe Audience Manager	Google analytics	Roku DX Holdings, Inc
Adprime Media Inc.	Google optimize	Roq.ad GmbH
adrule mobile GmbH	GP One GmbH	RTB House S.A.
Adserve.zone / Artworx AS	GRAPHINIUM	RTK.IO, Inc
Adsolutions BV	GroupM UK Limited	RUN, Inc.
AdSpirit GmbH	GumGum, Inc.	salesforce.com, inc.
adsquare GmbH	Haensel AMS GmbH	Samba TV UK Limited
Adssets AB	Happydemics	Scene Stealer Limited
AdsWizz Inc.	hbfsTech	Seeding Alliance GmbH
Adtelligent Inc.	Heatmap	Seedtag Advertising S.L
AdTheorent, Inc	HIRO Media Ltd	Seenthis AB
AdTiming Technology Company Limited	Hivestack Inc.	Semasio GmbH
ADUX	Hotjar	Seznam.cz, a.s.
advanced store GmbH	Hottraffic BV (DMA Institute)	ShareThis, Inc
ADventori SAS	Hybrid Adtech GmbH	Sharethrough, Inc
Adverline	ID5 Technology SAS	SheMedia, LLC
ADWAYS SAS	IgnitionAi Ltd	Shopalyst Inc

Adxperience SAS	IgnitionOne	Showheroes SE
ADYOULIKE SA	Illuma Technology Limited	Sift Media, Inc
Adzymic Pte Ltd	Impactify	Signal Digital Inc.
Aerserv LLC	Improve Digital BV	Signals
Affectv Ltd	Index Exchange, Inc.	Simplifi Holdings Inc.
Affle International	INFINIA MOBILE S.L.	SINGLESPOT SAS
Alive & Kicking Global Limited	InMobi Pte Ltd	Sirdata
Alliance Gravity Data Media	INNITY	Sizmek
Amazon	Innovid Inc.	Skaze
Amobee, Inc.	Inskin Media LTD	Skimbit Ltd
AntVoice	Inspired Mobile Limited	Smaato, Inc.
Anzu Virtual reality LTD	Instinctive, Inc.	Smadex SL
Apester Ltd	Instreamatic inc.	Smart Adserver
AppConsent Xchange	InsurAds Technologies SA.	Smart Traffik
Appier PTE Ltd	Integral Ad Science, Inc.	smartclip Europe GmbH
Arcspire Limited	Intent Media, Inc.	Smartclip Hispania SL
Arkeero	Intercept Interactive Inc. dba Undertone	Smartme Analytics
ARMIS SAS	Internet Billboard a.s.	Smartology Limited
Arrivalist Co.	INVIBES GROUP	SMARTSTREAM.TV GmbH
AT Internet	INVIDI technologies AB	SmartyAds Inc.
ATG Ad Tech Group GmbH	iotec global Ltd.	Smile Wanted Group
Audience Network	IPONWEB GmbH	Snapshort Inc., operating as Sortable
Audience Trading Platform Ltd.	Jaduda GmbH	Sojern, Inc.
AudienceProject Aps	Jampp LTD	Solocal
Audiencerate LTD	Jivox Corporation	Somo Audience Corp
Audiens S.r.l.	Johnson & Johnson	Sonobi, Inc
AuDigent	Join	Soundcast
audio content & control GmbH	Jointag S.r.l.	Sourcepoint Technologies, Inc.
AUDIOMOB LTD	Justpremium BV	Sovrn Holdings Inc
Automattic Inc.	Kairion GmbH	Spolecznosci Sp. z o.o. Sp. k.
Avazu Inc.	Kairos Fire	Sportradar AG
Avid Media Ltd	Kayzen	Spot.IM LTD
Avocet Systems Limited	Keymantics	Spotad

Axel Springer Teaser Ad GmbH	Knorex Pte Ltd	SpotX, Inc.
Axonix LTD	Kochava Inc.	SpringServe, LLC
Azerion Holding B.V.	KUPONA GmbH	StackAdapt
Bandsintown Amplified LLC	Kwanko	StartApp Inc.
Bannerflow AB	L'Oreal	Steel House, Inc.
Batch	LBC France	Ströer Mobile Performance GmbH
Beachfront Media LLC	LeftsnRight, Inc. dba LIQWID	Ströer SSP GmbH (DSP)
Beaconspark Ltd	Leiki Ltd.	Ströer SSP GmbH (SSP)
Beemray Oy	Lifesight Pte. Ltd.	Sub2 Technologies Ltd
BeeswaxIO Corporation	Liftoff Mobile, Inc.	Sublime
BEINTOO SPA	Ligatus GmbH	SunMedia
BeOp	Linicom	TabMo SAS
Better Banners A/S	LiquidM Technology GmbH	Taboola Europe Limited
Between Exchange	Little Big Data sp.z.o.o.	TACTIC™ Real-Time Marketing AS
BidBerry SRL	Liveintent Inc.	Tapad, Inc.
BidMachine Inc.	LiveRamp, Inc.	Tapjoy, Inc.
Bidmanagement GmbH	Localsensor B.V.	TAPTAP Networks SL
Bidstack Limited	Location Sciences AI Ltd	Targetspot Belgium SPRL
BIDSWITCH GmbH	LoopMe Limited	Teads
Bidtellect, Inc	Lotame Solutions, Inc.	Tealium Inc.
BidTheatre AB	M32 Connect Inc	Teemo SA
Bigabid Media Ltd	Madington	Telaria SAS
BILENDI SA	Madison Logic, Inc.	Telaria, Inc
Bit Q Holdings Limited	MADVERTISE MEDIA	Telecoming S.A.
BLIINK SAS	mainADV Srl	Telefonica Investigación y Desarrollo S.A.U
Blingby LLC	MAIRDUMONT NETLETIX GmbH&Co. KG	Temelio
Blis Media Limited	Marfeel Solutions S.L	Teroa S.A.
Blue	Market Resource Partners LLC	The ADEX GmbH
Blue Billywig BV	Maximus Live LLC	The Kantar Group Limited
Bmind a Sales Maker Company, S.L.	McCann Discipline LTD	The MediaGrid Inc.
Bombora Inc.	Media.net Advertising FZ-LLC	The Ozone Project Limited

Bounce Exchange, Inc	Mediaforce LTD	The Reach Group GmbH
Brand Advance Limited	MediaMath, Inc.	The Rubicon Project, Inc.
Brand Metrics Sweden AB	mediarithmics SAS	The Trade Desk
Browsi Mobile Ltd	Mediasmart Mobile S.L.	Think Clever Media
Bucksense Inc	Mediasquare	Timehop, Inc.
BusinessClick	Meetrics GmbH	TimeOne
Capitaldata	MGID Inc.	Totaljobs Group Ltd
Captify Technologies Limited	Mindlytix SAS	travel audience GmbH
Carbon (AI) Limited	MiQ	TreSensa, Inc.
Cavai AS & UK	Mirando GmbH & Co KG	Triapodi Ltd.
Cedato Technologies LTD.	MISSENA	Triboo Data Analytics
Celtra, Inc.	mobalo GmbH	TripleLift, Inc.
Centro, Inc.	Mobfox US LLC	Triton Digital Canada Inc.
ChannelSight	Mobile Professionals BV	TrueData Solutions, Inc.
Chargeads	Mobilewalla, Inc.	TTNET AS
CHEQ AI TECHNOLOGIES LTD.	Mobsuccess	Tunnl BV
Cint AB	Mobusi Mobile Advertising S.L.	twiago GmbH
Clipcentric, Inc.	Monet Engine Inc	Twitter
Cloud Technologies S.A.	MOVLads Sp. z o.o. Sp. k.	UberMedia, Inc.
Clustaar	My6sense Inc.	ucfunnel Co., Ltd.
Codewise VL Sp. z o.o. Sp. k	Myntelligence Limited	Underdog Media LLC
Collective Europe Ltd.	MyTraffic	Unruly Group Ltd
Colpirio.com	N Technologies Inc.	Uprival LLC
Comcast International France SAS	Nano Interactive GmbH	usemax advertisement (Emego GmbH)
Commanders Act	Nativo, Inc.	Ve Global
communicationAds GmbH & Co. KG	NC Audience Exchange, LLC (NewsIQ)	VECTAURY
comScore, Inc.	Near Pte Ltd	Venatus Media Limited
Confiant Inc.	Neodata Group srl	Verizon Media EMEA Limited
Connatix Native Exchange Inc.	NEORY GmbH	Vibrant Media Limited
ConnectAd Realtime GmbH	Netsprint SA	Vidazoo Ltd

Consumable, Inc.	NetSuccess, s.r.o.	video intelligence AG
Contact Impact GmbH	netzeffekt GmbH	Video Reach
Converge-Digital	NEURAL.ONE	Vidoomy Media SL
Crimtan Holdings Limited	Neustar on behalf of The Procter & Gamble Company	ViewPay
Criteo SA	NeuStar, Inc.	Viralize SRL
Cxense ASA	News and Media Holding, a.s.	Visarity Technologies GmbH
Cybba, Inc.	NEXD	VRTCAL Markets, Inc.
Cydersoft	NextRoll, Inc.	WebAds B.V
Czech Publisher Exchange z.s.p.o.	Nielsen Marketing Cloud	WebMediaRM
D-Edge	Norstat Danmark A/S	WEBORAMA
Dailymotion SA	Noster Finance S.L.	Welect GmbH
Dataseat Ltd	Notify	WhatRocks Inc.
DeepIntent, Inc.	numberly	White Ops, Inc.
DEFINE MEDIA GMBH	Ogury Ltd.	Widespace AB
Delta Projects AB	On Device Research Limited	Wizaly
Demandbase, Inc.	OnAudience Ltd	X-Mode Social, Inc.
Densou Trading Desk ApS	OneTag Limited	xAd, Inc. dba GroundTruth
Dentsu Aegis Network Italia SpA	Onfocus (Adagio)	Xandr, Inc.
Digilant Spain, SLU	Online Advertising Network Sp. z o.o.	YellowHammer Media Group
Digital Control GmbH & Co. KG	Online Solution Int Limited	Yieldlab AG
Digital East GmbH	Onnetwork Sp. z o.o.	Yieldlove GmbH
digitalAudience	OpenX	Yieldmo, Inc.
DIGITEKA Technologies	Optomaton UG	Yieldr UK
Digitize New Media Ltd	Oracle AddThis	YOC AG
DigiTrust / IAB Tech Lab	Oracle Data Cloud	ZBO Media
district m inc.	Orion Semantics	Zemanta, Inc.
DistroScale, Inc.	ORTEC B.V.	zeotap GmbH
DoubleVerify Inc.	Otto (GmbH & Co KG)	Zeta Global
Dr. Banner	Outbrain UK Ltd	Ziff Davis LLC
Drawbridge, Inc.	PaperG, Inc. dba Thunder Industries	ZighZag
Dugout Limited	Passendo ApS	
dunnhumby Germany GmbH	Pebble Media	



