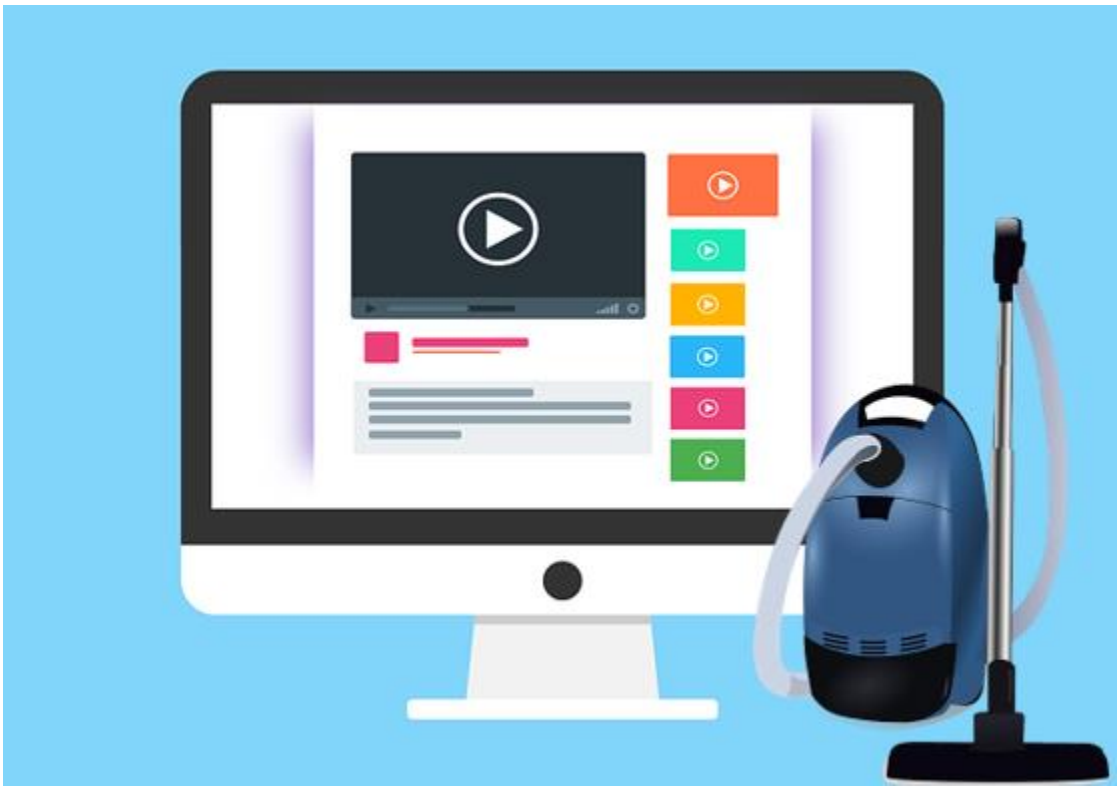
It’s Springtime – Time to Clean up Your Websites!



Lessons from a Belgian website

I’ve wanted to write about this Belgian case for a while at the request of some of you. I think it is of particular interest to US companies doing business in Europe. All feedback from your side is of course welcome!

In December 2019, the Litigation Chamber of the Belgian Data Protection Authority (“DPA”) imposed a EUR 15,000 fine on a website for noncompliance with the General Data Protection Regulation (GDPR) with respect to the website’s privacy policy, information notices, and cookie management. The website focuses on legal news and reportedly has an audience of 35,000 readers.

The DPA’s Executive Committee brought the case to the DPA’s Inspection Service based on the information published on the website. The Inspection Service performed an inquiry, and the website had to be fixed four times to comply with the GDPR. The findings of the inquiry are the following:

1) Noncompliance with the transparency requirement

- In the first audited version of the website, the privacy policy was only in English, even though the website was directed toward a French- and Dutch-speaking audience

- The website's users could not easily access the information
- The privacy policy actually referred to *US privacy law* and the *California Online Privacy Protection Act*
- A provision of the privacy policy stated "your IP address is not personal data". The DPA concluded that this provision went against Article 12 of the GDPR because it did not conform to the definition of personal data (Article 4(1) and Recital 30 of the GDPR)

2) Noncompliance with the information requirement (Article 13 of the GDPR)

- In the first audit of the website privacy policy, the policy did not state the identity and the contact details of the controller. During the second audit, the identity of the website owner was stated, but it did not explicitly state who the controller was. The website owner did not explicitly add this information until the third audit of the website.
- In the first audit of the website privacy policy, several pieces of required information were missing: the data subjects' rights, the legal bases and purposes of processing, the right to lodge a complaint with the DPA, and the data retention period for the personal data collected by cookies.

3) Findings related to the required consent

- In the first two audited versions of the website, the privacy policy did not state that the user's consent was the required legal basis for setting cookies even though the website was using first-party and third-party cookies (including Google cookies).
- In the third audited version of the website, the user was requested to state his/her cookie preferences, but the boxes were pre-checked. This was not considered valid consent in accordance with Recital 32 of the GDPR.

To bring its website into compliance with the GDPR, the website owner had to clean up the privacy policy by taking the following steps:

- explicitly stating the name and contact details of the controller
- explicitly and precisely stating the purposes and legal bases of processing
- explicitly stating the data retention periods for processing activities
- explicitly stating data subjects' rights
- stating the right to lodge a complaint with the Belgian Data Protection Authority (and providing a hyperlink to the DPA's website) and removing any reference to the Dutch Data Protection Authority since it does not have jurisdiction in Belgium

It's also interesting to note that the Inspection Service stated in its inspection report that since the website's purpose was to disseminate legal news, the website should serve as a role model and comply with the GDPR.

During the audit process, cookie management was highly scrutinized. At the beginning of the audit, the website was using cookies: (1) to enable the website to work properly; (2) to play video clips, share articles on LinkedIn, etc., and (3) to analyze the website usage and generate statistics. Although the

number of cookies changed throughout the audit, the case mentioned that, at one point in time, 50 cookies were used (9 first-party cookies and 41 third-party cookies). Here is a summary of the findings and changes required:

- No non-necessary cookie can be set on the user's device before the user has given his/her consent (the DPA emphasizes that "necessary" must be understood within the meaning of the GDPR, i.e., necessary for the data subjects' interests and not just the website's interests).
- The "legitimate interest" legal basis is not valid for non-necessary cookies.
- The user must be able to refuse the cookies (there must be a "Refuse" button next to an "OK" button).
- The consent for setting cookies must be specific: one consent per cookie type or category, not just one consent for all cookies (reference is made to Recitals 61 and 62 of the CJEU ruling in the Planet40 case and the EDPB guidelines on consent).
- A pre-checked box for accepting cookies does not constitute valid consent.
- The information provided to the user on the website must match the actual cookie practices (all cookies used must be stated in the cookie policy).
- The cookie policy must be easily accessible (e.g., footer on every page of the website; a single notice during the user's first visit to the website is not sufficient).
- The cookie policy must be written in the targeted audience's language(s) (in this case, Dutch and French).
- Information to easily withdraw consent must be provided.
- The cookie retention period must be stated.
- For third-party cookies, the cookie policy must state the identity of the third party setting the cookie and, if different, the identity of the third party using the cookie.
- The word "anonymized" can only be used if the personal data are properly anonymized. In this instance, the DPA considered the generation of a random identification number for Google cookies to be a pseudonymization process (Article 4.5.1 of the GDPR).

The website owner had to pay an administrative fine of EUR 15,000—calculated based on the owner's last three annual turnover figures, the duration of the violation, the number of data subjects concerned, the consideration of whether the violation was committed deliberately or negligently, and the corrective steps taken by the data controller. This was a costly cleanup exercise. Here is a list of tools that I continually refer to when I translate privacy policies into French. I hope you find them useful too in case you need to clean up your websites or help your clients clean up theirs:

- GDPR – Even if your front end needs to stay away from legalese, it's important to use the right words: A controller should not be called anything else—not the "entity responsible for the data," the "holder of the data," or the "master of the data," as I've seen translated into French. Let's call a spade a spade in EVERY language version of a privacy policy, a just-in-time transparency information notice, or a cookie policy.
- The Article 29 Working Party Guidelines on Transparency under Regulation 2016/679 (with a special focus on p. 35 of the Annex)
- The EDPB's Guidelines 05/2020 on Consent under Regulation 2016/679, which contain updated sections on cookies and websites

- The Planet49 ruling
- The information issued by the different data protection authorities in Belgium, France, and Luxembourg on their websites. Only part of this information is available in English. This is where your privacy translator can team up with you to help you dust off your documents and publish a shiny image of your organization on the web—the picture clients and supervisory authorities will see!

Happy spring cleaning, everyone!