October 2019

EU Court, Regulators and Internet Platforms Raise the Bar for Using Cookies

TOPICS: Data Protection, Cookies, Tracking Technologies, Google Chrome, ePrivacy Directive, GDPR, Germany, Spain, EU

The ECJ Ruled that only Active and Unambiguous Consent is Sufficient for the Use of Tracking Technologies

The European Court of Justice ("**ECJ**") has issued its long awaited decision in the case of Planet49, a lottery website that required users to consent to the storage of cookies in order to play a promotional game. In line with recent regulatory developments, the decision highlights that **pre-ticked check boxes authorizing the use of cookies and similar technologies do not constitute valid consent. The decision also analyzes the information and transparency requirements**.

In September 2013, Planet49 organized a promotional lottery on its website, where users wishing to participate, were required to provide their name and address. The registration page also included two checkboxes. The first box, which was unchecked, provided third party sponsors, with a general authorization to make commercial offers to users based on their contact details. **The second box, which was pre-selected, authorized Planet49 to set cookies to evaluate the user's surfing behaviors for advertising purposes**. Participation in the lottery was contingent on checking the first box.

The German Federal Court of Justice, which analyzed the appeal, decided to refer questions regarding the validity of consent to the ECJ. The ECJ based its decision mostly on the ePrivacy Directive and the Data Protection Directive (which had been replaced by the General Data Protection Regulation ("**GDPR**") that was not in force during the initial hearings). However, the ECJ's conclusion "matches" the GDPR definition of consent.

According to the ECJ, **operators should obtain active and unambiguous consent for the use of cookies**, **rather than relying on passive or implicit consent**. The ECJ inferred that **pre-checked boxes cannot be considered as active and unambiguous consent**. To support this finding, the ECJ referred to recital 32 of the GDPR, which excludes pre-checked boxes as valid means to obtain consent. The court emphasized that **consent shall be specific to the processing of data in question** and cannot be used to infer consent for other purposes.

The ruling confirmed that this **standard of consent applies to the placement of any tracking technologies, regardless of whether or not the information stored is considered personal data**. The decision aligns with one of the objectives of EU law, which is to protect the user from the risk that hidden identifiers and other similar devices enter the user's terminal equipment without his knowledge.

The ECJ also concluded that in order to provide valid consent, **users should be provided with clear and comprehensive information regarding the purposes for processing**, since such information will enable users to make informed decisions. The information provided to users **must include the duration of the operation of tracking technologies and whether or not third parties may have access to the data collected**.

The ECJ chose not to address the question whether setting the user's consent as a perquisite to use the service offered ("cookie walls") can be considered as constituting valid and freely given consent.

Earlier this year, we published our Practical Cookie Consent Handbook, in which we reviewed recent regulatory developments and provided practical tips on how to properly manage consent for the implementation of cookies.

Spanish DPA Fined an Airline Company for Failing to Comply with Cookie Regulations

The Spanish Data Protection Authority ("**AEPD**") fined the **Spanish airline** company Vueling, €30,**000 for failing to properly comply with the requirements regarding cookie consent**. In its decision, the AEPD stated that, although users are being informed on the use of cookies when accessing Vueling's website, they are not provided with access to any **cookie configuration tools**.

According to AEPD's decision, when accessing Vueling's website, a banner appears, in which users are informed that the company is using cookies and the purpose of their use. In addition, the banner refers users to Vueling's cookie policy for further information, and asks users to consent to all cookies, both for Vueling's own purposes and for third parties.

In this regard, **the AEPD found that the user is not properly given the option to refuse the use of tracking technologies**, given that users are not given an effective option for rejecting all or any specific cookies, or to withdraw their consent. Instead of providing users with an internal tool to manage cookies in a granular way, Vueling indicates that users must manage cookies by themselves, through accessing their browser's preferences.

The AEPD considered the consent collected by Vueling, **by means of "continue browsing"**, **to be invalid**, since the company did not offer tools to users in order to manage their consent. According to the decision, **Vueling should have enabled a mechanism to reject all cookies and also a mechanism to enable cookies, which would allow users to manage specific cookies in such a granular way**. It was stated that although browser configuration tools can serve as **complementary tools** to the ones offered by the website's operators, they cannot act as a stand-alone solution.

Following such findings, the AEPD concluded that Vueling had infringed Spanish Law on Information Society Services and Electronic Commerce ("**LLSI**"), according to which, service providers may use tracking technologies but only if they have provided clear and complete information on the use of tracking technologies and their purpose, and that the consent of the users had been obtained. **Althou**gh the AEPD imposed a €30,000 fine **on Vueling**, since Vueling acknowledged that it had infringed Spanish law and was willing to pay the fine promptly, the AEPD decided to reduce the fine to €18,000.

Google Warns Developers as it Tightens Cookie Security on Chrome 80

On a similar topic, we previously reported that browsers are taking measures regarding tracking technologies, including Google's plan to update Chrome in order to provide users with more transparency as to how sites are using cookies, and simpler controls for cross-site cookies.

This month, Google announced in a blog post, that it **plans to implement a new secure-by-default model for cookies** with the launch of Chrome 80 in February 2020. The new model, which was announced last May, has as its objective, to **improve privacy and security across the web**. Google warns developers who manage cookies to prepare in advance to the change in the "*SameSite*" cookie attribute.

The *SameSite* cookie attribute, which was introduced in July 2016, is used by developers when planting cookies. This attribute can obtain the values "*Strict*", "*Lax*" and "*None*", thereby enabling controlling access for third party websites: the *Strict* value blocks all third party cookies; *Lax* enables cookies only if the user clicked a link to the third-party site; and *None* enables all traffic to flow to third party websites.

The new model will mostly affect developers using cross-site (third party) cookies. Although currently, developers have the option to apply settings to prevent external access, only few developers do so, leaving many same-site cookies exposed to security threats. **Under the new secure-by-default model, cookies will be protected from external access by default**. Developers will have to use the new cookie setting

(*SameSite=None*) to designate cookies for cross-site access. When allowing cross-site access, developers will also have to use an additional "*Secure*" attribute such that cross-site cookies will only be accessed over HTTPS secured connections.

According to Google, **the change will assist in mitigating some of the risks associated with cross-site access and will provide protection against network attacks**. In addition, the requirement for an explicit declaration, when using cross-site cookies, will **create greater transparency and enhance the user's choice**, allowing browsers to manage samesite and cross-site cookies separately.

If the developers will not use the *none* value, **Google's new Chrome 80 will block external access for all cookies, automatically setting *SameSite* value as *Lax***. Only cookies with "*None*" value will be available for external access. In addition to Google, **Mozilla and Microsoft also announced that they are planning to implement the new model in the near future**.

Please do not hesitate to contact us if you have any questions on how to lawfully implement cookies and on implementing compliant cookie consent management tools.

*This update was published as part of our Technology & Regulation monthly client update. To read more about HFN's Technology & Regulation Department, **click here**.*