WEBSITE COOKIES AND PRIVACY ADVISORY

Cookies in the privacy world are sometimes an expensive Achilles' heel for some organizations! Cookies are small pieces of data stored on devices when accessing a website that uses them. Cookies may be stored for short periods or more prolonged.

Holding a user's session active and tracking user activity and preferences are the most common reasons website owners love to use them.

The world has agreed to categorize cookies as either First-Party or Third-Party. Website owners set First-Party cookies, whereas Third-Party cookies are set by third-party content such as widgets. Such cookies are relied on to track a user's activity across many websites visited.

Whereas they are mostly intended for good, malicious actors may exploit the use of such cookies to gain unauthorized access to user accounts or to profile users. Exploits could include hijacking session cookies, searching for cookies to identify user credentials and other related data. Therefore, companies that use cookies must protect the data they collect and, most importantly, communicate to users why and how they are used, their rights, and if it's mandatory or discretionary. The myriad of approaches that organizations are using cookies has led to some facing stern regulatory action. The common causes for regulatory action are:

- Cookie consent violations.
- Using cookies without obtaining prior consent.
- Not being transparent enough to users.

Facebook itself is in the news by creating a privacy cookie consent bypass by catering for the use of cookies under its Terms and Conditions. NOYB (a nonprofit digital rights organization) filed a complaint with the Irish Data Protection Commission concerning this privacy consent bypass. This is NOYB's primary concern — '*Facebook simply tries to bypass the clear rules of the GDPR by relabeling the agreement on data use as a 'contract'. If this would be accepted, any company could just write the processing of data into a contract and thereby legitimize any use of customer data without consent. This is absolutely against the intentions of the GDPR that explicitly prohibits to hide consent agreements in terms and conditions*.' The outcome of this complaint will be a game changer on how best to achieve compliance with privacy laws when using cookies.

At the center of it all, cookies are used to collect data to define user preferences and track their browsing history, all of which may contain identity data of a user. As such, there is a lot of debate on how best an organization may use cookies on its website. This has seen the increased use of cookie banners and notices in some regions, such as the European Union. However, the effectiveness of such cookie banners is still unclear, given that the mix of implementation. One of the sticky issues is how best to obtain consent through cookie banners transparently — using opt-in options and using clear and simple-to-understand language.

For now, an organization should take on a more proactive and fair approach on how they use cookies by considering the following:

- Transparency by providing users with enough information to make an informed decision.
- Implementing means to obtain explicit consent and also allow withdrawal of consent in an effortless manner.
- Make use of privacy by default if identity data will be obtained from the use of cookies.

- Ensure that third parties that provide analytic platforms using data collected from cookies have adequate technical and organizational measures to protect data.