BDO USA

ARTICLE

April 09, 2024

BY:

Mark Melnychenko
Practice Leader, Privacy & Data Protection

"Me Want Cookie" — Balancing the User Website Experience and Data Privacy

In today's digital age, website cookies have become an integral part of online user experience. This technology can enable website owners and marketers to gain valuable insights into user behavior and preferences, implement personalization features, and tailor advertising. However, the use of cookies and other tracking technologies has also raised concerns about data privacy and compliance with relevant laws and regulations. This article will explore the delicate balance between providing a seamless user experience and safeguarding user data privacy, with a particular focus on considerations for nonprofit organizations.

Understanding Website Cookies

Gaining a clear understanding of website cookies is crucial in effectively addressing the challenge of balancing user experience and data privacy. Cookies are small text files stored on a user's device, which collect and store data. While they can be used for various purposes, they are often referred to by the following types:

- **First Party:** This type of cookie is set by the website itself or by another domain, which the website owner controls. They are primarily used to enhance the user experience by enabling features such as remembering login information, language preferences, and shopping cart contents.
- **Third Party:** This type of cookie is set by external domains, which are not controlled by the website owner, but incorporated into the website for various reasons. One reason is to track user behavior across multiple websites, allowing advertisers to deliver personalized ads based on the user's interests.
- **Fourth Party:** It is possible for third-party website code to set fourth-party cookies, which are controlled by the third party’s third parties. There can even be fifth-party cookies and beyond, but generally these are included by this definition for fourth-party cookies.

Depending on how they are used, all cookies have the potential to raise concerns about user privacy and data sharing. However, third- (and fourth-) party cookies tend to receive the most scrutiny. As a result, there is a growing emphasis on transparency and user consent regarding the use of these cookies.

Privacy Laws Include Cookie Compliance Requirements

Data privacy has become a pressing concern for users, regulators, and activists alike. With the increased frequency of data breaches and misuse of personal information, people are demanding greater transparency and control over their data. Over the last six years, regulators have been enacting laws to protect data privacy, such as the General Data Protection Regulation in Europe and the California Consumer Privacy Act in the United States, among many others. Most of these laws include requirements related to the use of cookies and other tracking technologies, obtaining user consent, providing clear and concise privacy policies, and implementing robust security measures to safeguard collected data.

Noncompliance with cookie-related requirements can carry substantial consequences, as there is a growing trend of actions and penalties imposed on entities found to be in violation. Regulatory bodies are taking a stricter stance on enforcing these laws, aiming to protect individual privacy and ensure transparency in data practices. Organizations must be aware of the potential risks and financial implications associated with noncompliance, including significant fines and reputational damage, and put solutions in place to avoid these. Once a privacy program and these solutions are in place, organizations should regularly review and update their privacy practices as new laws and requirements continue to emerge.

Solutions for Cookie Compliance

To comply with cookie-related requirements, websites require the use of a Consent Management Platform (CMP). This presents the user with a banner and/or preference center as a transparent and user-friendly mechanism to inform visitors about the use of cookies and to obtain the user's consent for using them. The solution should provide clear and concise information about the types of cookies used, their purpose and the option for users to manage which optional cookies are used. Some laws also explicitly require the user interface design to meet certain parameters aimed at making it equally easy to grant or withdraw consent.

Even when a CMP is initially implemented correctly, the implementation must be maintained properly. Websites are not static and frequently change over time, including the addition or removal of tracking technologies. As such, the CMP implementation should be tested on a regular basis to ensure that banners appear consistently and that cookies behave correctly when a user opts into or out of different cookie categories. In many cases, the default settings for optional categories also need to differ depending on where the user is in the world. To accommodate this, testing must be simulated from different locations to ensure appropriate behavior. BDO does this type of testing for clients using a proprietary application and finds that about 95% of the websites it tests are not fully compliant with the requirements of one or more privacy laws.

Unique Considerations for Nonprofits

Not all privacy laws apply to all nonprofits. For example, many U.S. state laws include exemptions for nonprofits, but the exemptions vary and may not exempt all nonprofit organizations. Though many of the requirements imposed by privacy laws are considered good practice for everyone, it is important for each nonprofit to determine which laws apply to them.

Nonprofits that must comply with individuals' requests to opt out of targeted advertising or the sale of their personal information may encounter constraints in leveraging data on advertising platforms to engage potential donors and volunteers. Nonprofits have to balance respecting consumer privacy choices with expanding their outreach and support base. Moreover, nonprofits that fail to honor rights granted under relevant privacy laws risk facing enforcement actions from state attorneys general, which can include penalties and mandates to alter practices.

Maintaining trust with donors and supporters is of utmost importance for nonprofits, as their success heavily relies on the continued support and engagement of these stakeholders. Compliance with privacy best practices plays a crucial role in building and preserving this trust. By demonstrating a commitment to protecting individual privacy and adhering to related laws, nonprofits can reinforce their reputation as responsible custodians of data and foster stronger relationships with their supporters.

Conclusion

As organizations use cookies and other tracking technologies on their websites for various reasons, they must also prioritize compliance with relevant privacy laws. For cookie-related requirements, the first step is to implement a Consent Management Platform that complies with all relevant laws. Once this solution is implemented, it should be tested regularly to ensure proper functioning as websites change over time. Ultimately, by striking the right balance, nonprofit organizations can build trust with their users and ensure compliance with global and U.S. regulations, while dealing with some of the considerations unique to the space.

Have Questions? Contact Us.

Return to Nonprofit Standard Newsletter