Come to the Dark Side, We Have Cookies

Insights
7.30.18

Have you noticed recently that when you click on most websites a notice appears stating that the host uses cookies? Many are aware that on May 25, 2018, the GDPR ("Global Data Protection Regulation") took effect. The law applies to any person or organization that is physically located in the European Union ("EU") and has a website, as well as any website that targets consumers in the EU. The law requires a cookie consent notice, depending on the type of cookie used by the site. Hence, the recent increase in cookie notices.

There are two kinds of cookies: session cookies and persistent cookies. Session cookies are temporary and merely necessary for website functionality. Once the browser is closed, there is no more activity or data tracked. Persistent cookies actually track the user's activities even after the user has left the site or closed the browser. Those sites that use persistent cookies require a cookie consent notice under the GDPR.

While most of us have assumed for years that websites were dropping cookies on our computers, this law has brought the issue to the forefront, and applies to smartphones, tablets and other devices used to access websites. Those covered by the law are supposed to let each individual user know they use cookies, provide a link where the user can learn about how the data gathered is used, and provide a way for users to provide consent to the use of cookies. This can be particularly challenging with multiple user devices.

Many website hosts are simply displaying a banner or a box somewhere at the top or bottom of the website when it's first accessed. The notice will have a link to a detailed privacy policy and a consent feature for the use of the cookies, which, once clicked, hides the banner.

Consent can be explicit or implied. Explicit consent requires the user to take some action, such as checking a consent box, clicking an acknowledgment button, etc. Implied consent can be something as simple as a statement that continuing to use the site means that the user agrees to the use of cookies. Are your employees reading these notices and clicking on the links to review how the data is used before consenting? Likely not. Many of these notices simply have an X out feature in the corner of the banner box where the user can simply close the notice and move on. Hence, implied consent.

With the concerns about data breaches and hacking at an all-time high, it is important for employers to address how employees consent to the use of cookies on company computers, tablets, and

phones. Particularly, third party cookies, which are cookies that are placed on a device by a website other than the one the user is visiting.

Employers can reduce risk by limiting employee access to sites that are necessary to accomplish a business purpose, and have been verified to be legitimate. Employers may require that employees who are prompted with a cookie consent do not simply accept and move forward. The company may request the employee review the privacy link to determine what is being tracked, stored and used and compare that against information the company will not allow an employee to consent to without company authorization.

For those sites that provide a mechanism to manage cookies, employees should be directed on how to use those features. Alternatively, the company can use a spam filter or cookie blocking software to block cookies. The downside can be that this could interfere with cookies that are necessary for the efficient use of the site.

The bottom line is that employers should not ignore this recent uptick in cookie notices and should review and revise security policies and protocols accordingly. Failure to do so runs the risk that the dark side may end up with your cookies.

Related People

Michelle I. Anderson
Partner
504.529.3839
Email