Updates
July 01, 2021

noyb Takes Aim at “Cookie Banner Terror” While CNIL Enforces Cookie Guidelines

Last month, the European Center for Digital Rights (more commonly known as *None of Your Business* or "*noyb* ") launched a new campaign against the use of allegedly unlawful cookie banners by sending nearly 600 draft complaints to companies across the European Union and European Economic Area (EU/EEA). *Noyb* is the privacy watchdog organization co-founded by Max Schrems, and it has been very vocal about its new effort to end "cookie banner terror." According to *noyb*, EU privacy law requires that users be given a clear "yes" or "no" option to accept cookies, but many companies fail to provide a "no" or equivalent option on the first page of the website or use "dark-patterns," such as deceptive colors, button contrast, or a labyrinth of sub-menus to frustrate or confuse users into clicking "yes" to accept cookies.

Noyb has given companies one month to cure the alleged violations of EU privacy laws before *noyb* files formal complaints with the applicable regulators.

Noyb's war on cookies is also significant because the alleged violations in the draft complaints were identified using new software *noyb* developed. *Noyb* plans to use this software to scan up to 10,000 of Europe's most visited websites in 2021 (regardless of organization type or industry) to identify, in *noyb*'s view, websites that use unlawful cookie banners. The websites identified by the tool are then reviewed by *noyb*'s legal team, which subsequently sends alleged offenders a draft complaint, along with step-by-step guidance on how to make their cookie banners legally compliant.

Noyb has identified more than 15 types of alleged violations of EU privacy laws, which it lists in its compliance guide. We provide a summary and initial analysis of the key violation types below.

It is also worth noting that similar cookie notice and consent issues have been the focus of France's data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL). Last month, the CNIL issued formal notices to at least 20 companies (and some public organizations) for not allowing internet users to reject cookies as easily as they can accept them. The CNIL gave these companies and public organizations 30 days to address the alleged violations. On June 29, 2021, the CNIL reported that every organization targeted had modified its practices to comply with EU privacy laws. We summarize the CNIL's recent actions in more detail below.

Noyb's Violation Types and the GDPR and ePrivacy Directive

Type A—No "reject" option on the first layer. *Noyb* says the most common issue it found is that no "reject" option for cookies is featured on the initial page of a website. This is an issue because, according to *noyb*, EU privacy law requires that internet users be given a "simple yes or no option" regarding cookies. *Noyb*'s position is based on its interpretation of the General Data Protection Regulation (GDPR) principle that refusing consent should be as simple as providing consent. According to *noyb*, therefore, cookie banners without an initial "reject" or "reject all" option violate the GDPR consent requirement.

Noyb's interpretation, however, is not rooted in the text of the GDPR, which does not clearly require that a "reject" option be provided at the same time consent is obtained.

Type B—Pre-ticked boxes on second layer. *Noyb* asserts that using pre-ticked boxes to obtain cookie consent violates the GDPR, specifically referring to pre-ticked boxes typically found in the settings section of cookie consent platforms like OneTrust.

Noyb's position aligns with legal requirements in the EU/EEA. The GDPR expressly states in its recitals that pre-ticked boxes should not constitute consent. Additionally, this position is in line with recent decisions from the Court of Justice of the European Union (CJEU), the EU's highest court, regarding cookie consent (see, e.g., the CJEU's decisions in October 2019 and November 2020, concluding that consent was not validly given where a checkbox was pre-checked). Thus, companies should make sure that their current practices for obtaining cookie consent require internet users to take a clear affirmative action, such as ticking an unticked box, to indicate consent.

Type C—Deceptive link design. According to *noyb*, the use of deceptive link designs, including use of "dark patterns" and confusing hyperlinks to reject cookies, "nudges" 90% of internet users into clicking an "agree" button, and therefore is in violation of the GDPR's consent requirements. *Noyb* cites industry statistics indicating that only 3% of internet users actually want to accept cookies to support its argument that offering hyperlinks (rather than buttons) to reject cookies essentially forces users to accept all cookies.

While "nudging" and use of "dark patterns" can implicate whether consent is freely given, specific, informed, and unambiguous, as the GDPR standard requires, the GDPR itself does not prescribe how companies must format and design their approach to obtaining consent, nor does it dictate that an option to refuse consent be offered in the same manner or at the same point as an option to consent. Accordingly, companies have more leeway in designing their approaches to cookie consent than *noyb* would suggest. To comply with the GDPR, companies should take a holistic view of not only link and button designs, but also the placement of such links and buttons on the site, their prominence, and any accompanying text.

Types D and E—Deceptive button colors and contrast. Similar to its position on deceptive link designs (violation Type C), *noyb* alleges that use of deceptive colors and contrasts for cookie "accept" and "reject" buttons violates GDPR consent requirements. In complaints issued so far, *noyb* found that the "accept" button is presented in a prominent color (like green) whereas the "reject" button is in a more subdued color (like gray), which allegedly nudges users into accepting cookies that they may actually want to refuse.

As noted above, the GDPR itself does not provide specific requirements for designing consent mechanisms, and it is unclear whether EU regulators would deem that certain color and color contrast designs violate the GDPR. However, companies should still consider button design in their overall approaches to cookie consent.

Type H—Legitimate interest claimed. *Noyb* alleges that any indication that a company relies on legitimate interests, rather than on consent, for its use of cookies violates EU privacy law. This position aligns with the EU ePrivacy Directive, which requires companies to obtain valid consent from an internet user for the use of non-essential cookies.

Accordingly, companies should ensure their cookie banner language does not reference "legitimate interests," and should ensure that they obtain consent where required. The intersection of ePrivacy Directive and GDPR requirements, however, is nuanced, and it is important to note that consent may not always be the most appropriate legal basis for subsequent processing of data obtained via cookies.

Type I—Inaccurate classification of cookies. *Noyb* suggests that some companies misclassify non-essential cookies as "essential" (also called "strictly necessary") cookies to circumvent the ePrivacy Directive's consent requirements. *Noyb*'s step-by-step compliance guidance focuses on mischaracterized statistics and advertising cookies, but notes that it only checked a limited set of cookies for each allegedly offending company, meaning a full cookie review may be required.

As noted above, the ePrivacy Directive requires companies to obtain an internet user's consent before placing non-essential cookies on a user's devices. *Noyb* asserts that statistics and marketing cookies should not be considered "essential," and companies should obtain consent in that context. However, for other cookie types, particularly analytics cookies, proper classification of "essential" versus "non-essential" is a hot topic of debate. EU regulators take widely varying interpretations, which companies should consider when determining how to classify cookies and when to seek users' consent.

Type K—Not as easy to withdraw as to give consent. Another key violation type *noyb* identifies is cookie banners that do not include an easy and readily accessible option to withdraw consent. To provide such an option, *noyb* compliance guidance suggests that cookie banners should persistently hover so that internet users may access and update their cookie preferences at any time.

As noted above, the GDPR allows companies flexibility in implementing consent and withdrawal/rejection options. Companies must enable users to withdraw consent as easily as they can give it, but neither the GDPR nor the ePrivacy Directive dictate that the right to withdrawal be provided at the same time or in the same manner as the consent method.

CNIL Amended Guidance and Formal Notices

Less than two weeks before *noyb* launched its war on cookie banners, the CNIL also took aim at companies for allegedly failing to comply with cookie consent requirements. The CNIL issued formal notices (or "orders to comply") to at least 20 organizations for not allowing internet users to refuse cookies as easily as they can accept them, which the CNIL asserts violates French rules implementing EU privacy law. According to the CNIL, this first set of targeted companies is considered "important within the digital economy." The notices provided the companies one month (which has now elapsed) to comply or otherwise incur financial penalties of up to 2% of the company's global turnover for the past year. On June 29, 2021, the CNIL reported that every organization identified in its first round of formal notices had complied and modified its practices to allow internet users to refuse cookies as easily as they can accept them. The CNIL's statement did not describe what specific measures companies implemented to become compliant.

These orders to comply mark the CNIL's first cookie enforcement effort since the grace period companies had been given to come into compliance with France's new cookie guidelines expired at the end of March. The CNIL was the first EU regulator to issue such cookie guidelines, which were originally published in July 2019 to address the strengthened consent requirements of the GDPR and later amended in October 2020 to comply with a decision from the French Council of State. Key requirements include:

- Individuals must be able to refuse consent as easily as they can give it;
- Individuals must be able to withdraw consent as easily as it was given;
- Users must consent specifically to each purpose of processing;
- The identity of the controller(s) who place cookies on the individual's device must be kept updated and made available when consent is obtained;
- Companies must be able to demonstrate to the CNIL that valid consent has been obtained.

The CNIL stated that compliance with France's cookie requirements is one of its key priorities for 2021, and that it will continue its enforcement efforts over the coming months. Orders to comply (which may be public) are sent to companies identified after investigation as having "serious infringements." Infringing organizations that do not address violations within the designated time period may face significant monetary and nonmonetary penalties.

Looking Ahead

Notice and consent requirements for the use of cookies have long been in the spotlight, especially as cookie banners proliferate across the web. Although some EU regulators have sought to address questions related to the use of cookies under EU privacy laws, compliance is still subject to a range of interpretations, which may ultimately be addressed by implementation of the ePrivacy Regulation. Until then, *noyb*'s campaign and the CNIL's recent enforcement actions provide a useful reminder for companies to review their cookie notice and consent practices and make updates where needed.

Explore more in

Technology Transactions & Privacy Law Privacy & Security

Related insights

Update

Ninth Circuit Rejects Mass-Arbitration Rules, Backs California Class Actions

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights