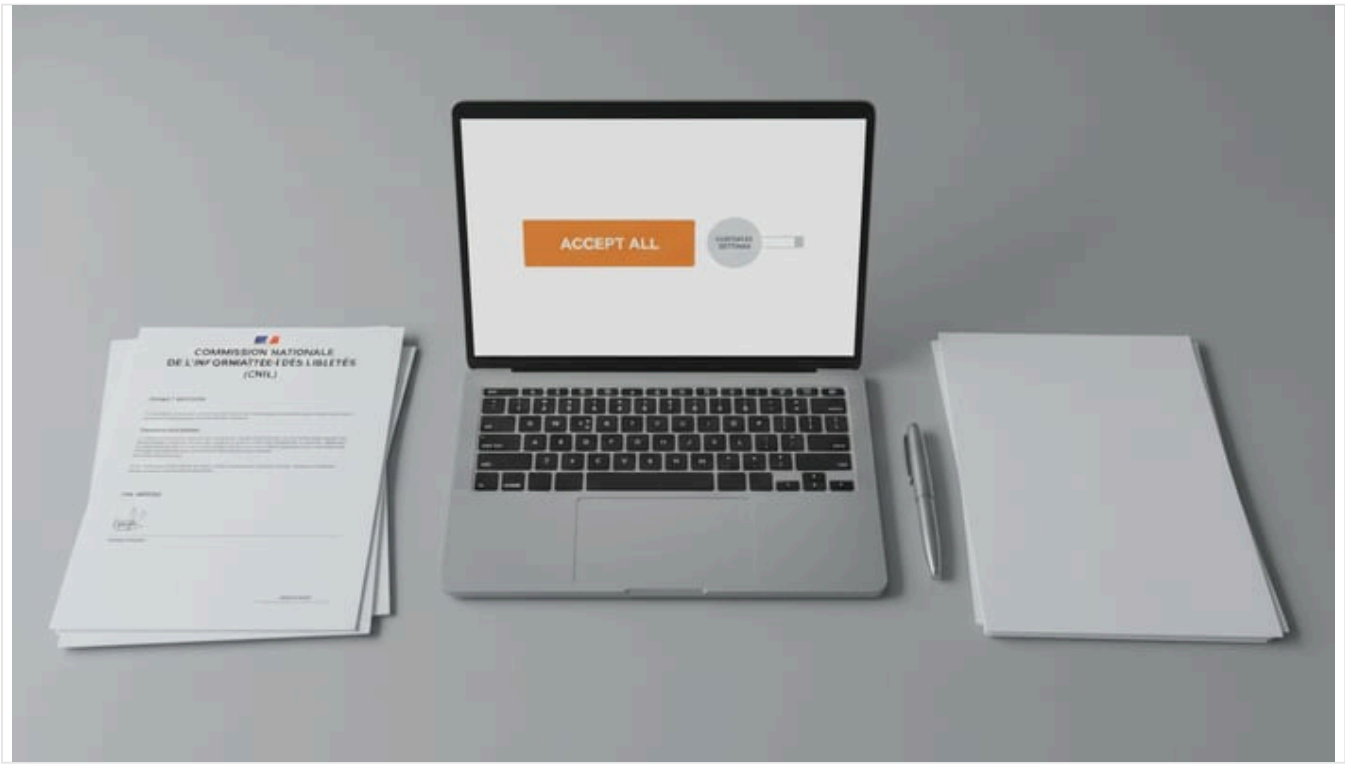
Cookie Consent Penalties: GDPR Fines & Legal Risks Explained

By rankstudio.net Published October 24, 2025 40 min read



Executive Summary

Cookie consent banners have become ubiquitous on websites in recent years, driven by privacy laws that require user permission before tracking technologies (like cookies) can be deployed. Failing to display a proper cookie consent banner – and thus failing to obtain valid user consent – is a direct violation of those laws. Across jurisdictions the penalties for such violations can include **substantial fines and enforcement orders**. For example, in 2025 the French Data Protection Authority (CNIL) levied *record fines* for cookie-related breaches: Google and Shein were hit with €325 million and €150 million penalties, respectively, for placing tracking cookies without freely given consent (Source: www.lemonde.fr) (Source: www.cnil.fr). Courts have also punished "cookie walls" – banners that coercively force users to accept cookies as a condition of service – and required companies to add clear "reject" options under threat of daily fines (Source: www.lemonde.fr) (Source: noyb.eu). In Belgium, for instance, the DPA ordered four major news websites to add a visible "reject all" button or face penalties of €50,000 per day (Source: noyb.eu). In short, **omitting a compliant cookie consent banner (or employing a defective one)** can trigger the maximum penalties under data protection law – often capped at 2–4% of a company's global turnover or tens of millions of euros – and may include daily fines or injunctive orders until compliance is achieved.

This report provides an in-depth analysis of the legal rules and enforcement trends governing cookie consent banners, the types of penalties imposed for non-compliance, and the practical implications for organizations. It covers the historical development of cookie consent laws, the current regulatory frameworks in different regions (especially the EU and UK, where the laws are strict), and the penalties that have been imposed in real cases. We examine academic research on cookie-banner compliance, expert commentary, and case studies (including major fines by CNIL and others). We also explore counter-perspectives (e.g. industry concerns about "consent fatigue" and potential future reforms of cookie rules). Throughout, claims are supported by extensive citations to legal sources, regulatory announcements, news reports, and scholarly studies.

Introduction

The dramatic rise of online tracking technologies in the past two decades prompted regulators to require websites to obtain user **consent** before deploying cookies or analogous tools. This requirement dates back to the early 2000s with the EU "cookie law" (the Privacy and Electronic Communications Directive) and has since been reinforced by broader data-protection laws (notably the EU's General Data Protection Regulation, or GDPR). In practice, the most visible manifestation of these rules is the **cookie consent banner** or popup that greets visitors on many websites today. These banners typically inform users about cookie usage and ask them to accept or decline non-essential cookies.

However, many websites have struggled to implement these banners in fully lawful ways. Common failures include not displaying any banner at all, hiding the reject/opt-out option, pre-checking consent boxes, or otherwise steering users towards consent. As a result, privacy regulators have increasingly cracked down, investigating sites and imposing penalties. Indeed, non-compliant cookie banners have become a major enforcement focus. Privacy advocates (such as the EU group NOYB) have filed hundreds of complaints about misleading banners, prompting data protection authorities ("DPAs") to act.

This report addresses the question: **What is the penalty for not showing a cookie consent banner?** In other words, what enforcement actions and sanctions can a website operator expect if it fails to obtain valid cookie consent. We proceed by first outlining the legal framework (why consent is required), then summarizing the various penalties (fines, injunctions, etc.) imposed for failures. We analyze data and case studies, and survey multiple perspectives (regulators, companies, privacy experts). We also discuss the broader context and the likely future of cookie consent law. The answer is comprehensive: it delves into the intricacies of ePrivacy and data protection law, reviews enforcement trends across jurisdictions, and provides detailed examples of penalties, supported by expert and academic sources.

Legal and Regulatory Background

Evolution of Cookie Consent Rules

The requirement to display cookie banners stems primarily from **data privacy laws** adopted in the EU and related jurisdictions. The key roots are:

- **EU ePrivacy Directive (2002/58/EC)**: Often called the "cookie law," this EU directive (amended in 2009 by Directive 2009/136/EC) explicitly requires that websites may not store or access information on a user's device (e.g. via cookies) *unless* the user has **given clear consent** after being informed about the purposes. In most member states this was transposed into national law (e.g. the UK's Privacy and Electronic Communications Regulations, "PECR"). The core rule can be summarized as: **Websites must inform users about cookies and obtain their unambiguous consent before placing non-essential cookies**.

- **EU GDPR (2016/679)**: Although GDPR does not specifically mention "cookies," it asserts that identifiable cookies (especially those tracking behavior) constitute personal data. Thus, processing that data requires a lawful basis, most commonly *consent*. Under GDPR, consent must be freely given, specific, informed, and unambiguous (Article 4.). If a cookie banner fails to meet these standards – for example by defaulting to accept all cookies or by hiding the opt-out option – consent is not valid under GDPR. Many of the EU fines for cookie violations have in fact been framed as GDPR breaches (e.g. failing to obtain consent as required by Article 6 and 7 of GDPR).

- **National Implementations**: Member states of the EU (and countries adopting similar laws) have enacted or adapted their privacy laws to impose cookie-consent obligations. For example, France's Data Protection Act (Loi Informatique et Libertés) contains provisions (e.g. Article 82) specifically targeting "advertising cookies," echoing the EU rule (Source: www.cnil.fr). In the UK, PECR and the Data Protection Act (and now UK GDPR) govern cookies. Other countries (e.g. Switzerland, Japan, South Korea) have their own privacy laws, and in some cases special rules for tracking technologies, though often not as detailed or strictly enforced as in the EU (Source: ico.org.uk) (Source: cookie-compliance.co).

In plain terms, under current EU/UK law a website **must** (1) notify visitors how cookies are used, and (2) allow them to *affirmatively opt in* to non-essential cookies. Essential cookies (e.g. for shopping cart functionality or basic security) are exempt, but virtually all advertising, analytics, and social-media cookies require consent. The website's cookie banner is the mechanism to achieve (1) and (2). As the UK ICO guidance states: "you must tell people the cookies are there; explain what the cookies are doing and why; and

get the person's consent to store a cookie on their device" (Source: ico.org.uk). If a website fails to get valid consent (for instance, by not having a banner, or by presenting it improperly), it is in breach of the ePrivacy/GDPR rules and thus exposes itself to penalties.

Consent Requirements in Detail

Under GDPR Article 7 and Recital 32, consent must be a **clear affirmative act**. This means no pre-ticked boxes or assumed consent through silence. The CJEU (EU Court of Justice) has clarified that privacy settings or mere use of the website cannot serve as consent. Users must take an explicit action (click "accept", for example).Moreover, consent must be as easy to withdraw as to give; a "reject" option must be available without penalty (Source: www.cnil.fr) (Source: www.mishcon.com).

Cookie banners often fail these tests by design: researchers have found many sites pre-check "accept all" by default or use dark patterns to nudge acceptance. One large-scale study found **54%** of tested websites violated the law — e.g. by giving users no real choice. Specifically, they discovered dozens of sites that recorded "positive consent" even when the user did nothing, and many that did not offer a direct opt-out (Source: arxiv.org). Another survey of 7,500 websites in Greece and the UK found that under half of them even displayed any cookie notice at all, despite most placing tracking cookies (Source: arxiv.org).

Regulators sometimes emphasize the form requirements. For instance, the Irish data authority's Digital Clearing House noted that banners are unlawful if they omit a clear "no" button or otherwise bias consent (Source: www.mishcon.com). In 2023 the UK's ICO Commissioner warned companies: failing to offer a straightforward "reject all" option on your banner is a breach of the law, and the ICO would pursue it (though with intervening steps before issuing fines) (Source: www.mishcon.com). Similarly, the EU Article 29 Working Party and the later European Data Protection Board have issued guidelines stressing that cookie banners should not hide or obfuscate the opt-out. The principle is clear: **accepting cookies must be a positive choice, not an opt-out default**.

Global Context: US and Others

By contrast, outside Europe the legal landscape is quite different. In the United States, **there is no federal law requiring cookie consent banners**. Privacy regulation is sectoral and at the state level. The California Consumer Privacy Act (CCPA/CPRA) grants users rights like "do not sell my data," but it does *not* explicitly mandate cookie banners or obtaining consent for common tracking cookies (Source: cookie-compliance.co). Federal laws like ECPA or COPPA restrict certain uses of communications data (notably COPPA requires parental consent for tracking children via cookies) but do not impose a general website opt-in requirement. As one legal FAQ notes, "under US privacy laws there is no clear requirement for cookie consent," although businesses are often advised to use banners voluntarily to avoid FTC actions or class-action suits (Source: cookie-compliance.co).

Some non-EU countries have adopted laws with consent elements. For example, Singapore's PDPA and Canada's PIPEDA require "meaningful" consent for personal data collection, which could encompass cookies, but they lack detailed cookie-specific rules. India's proposed Personal Data Protection Bill (not yet in force) would require consent for personal data processing, but implementation specifics are pending. In general, however, it is the **EU-centric ePrivacy/GDPR regime** that has driven the global adoption of banner consent as a common practice – and the hefty penalties for noncompliance that we see today stem mostly from European regulators enforcing those laws.

Enforcement Mechanisms and Penalties

If a website operator fails to present a valid cookie consent banner (and thus does not obtain lawful consent), the penalties usually arise in two main forms: **administrative fines** under data protection law, and **injunctive orders** or other enforcement remedies. In Europe, the primary enforcers are the national Data Protection Authorities (DPAs) or communications regulators. In other regions, enforcement might involve data agencies or consumer protection bodies.

Fines under Data Protection Laws

Under the GDPR (and mirror provisions in national laws), DPAs can impose substantial fines for violations. For cookie-related breaches, the relevant provisions generally fall under the GDPR's Article 83. The maximum fines are tiered: breaches of basic consent and transparency obligations (such as failing to respect cookie opt-outs) can lead to fines of up to **€20 million or 4% of**

global turnover (whichever is higher) (Source: www.reuters.com). Lesser infringements can incur up to €10 million or 2% (for example, non-compliance with some specific requirements). In practice, many cookie banner violations have been treated as serious enough to justify multi-million or even triple-digit-million euro fines.

The EU's strongest enforcement to date has come from France's CNIL. In late 2023 and 2025 the CNIL imposed record penalties on major companies for cookie violations. For example, in December 2023 France fined Yahoo €10 million for its cookie practices (Source: www.cnil.fr). And in September 2025 CNIL slapped **€325 million** on Google and **€150 million** on Shein for not obtaining valid consent (Source: www.lemonde.fr) (Source: www.reuters.com). These fines were remarkable not only in size but in their rationale: they explicitly cited cookie consent failures. CNIL stated that Google had "coerced" users into accepting cookies (a "cookie wall") when setting up accounts, and had inserted tracking cookies into Gmail without freely given consent (Source: www.lemonde.fr). Shein was penalized for placing tracking cookies even after users opted out, and for inadequate withdrawal mechanisms (Source: www.lemonde.fr) (Source: www.reuters.com). In CNIL's view, both companies "failed to obtain users' free and informed consent" before cookie placement (Source: www.lemonde.fr). These cases illustrate the extreme end of the penalty spectrum – fines equivalent to around 2-4% of the companies' revenues (Source: www.reuters.com).

Other European DPAs have issued lower-scale fines or orders. For instance, in Belgium the Data Protection Authority fined the Roularta press group **€50,000** (about 2% of the requested penalty for supportive consumer compliance) for cookie consent violations (Source: iapp.org). The ADP found that Roularta did not meet the conditions for obtaining user consent (it simply stored tracking cookies without clear opt-in). Though smaller in absolute terms, this fine (imposed in May 2022) reflects Belgium's application of GDPR rules: it was not a criminal sanction but an administrative fine under data protection law.

Potential fines vary across EU Member States depending on how national law channels GDPR. In France, for example, Article 82 of the Data Protection Act specifically addresses "advertising cookies" and lets the CNIL impose penalties for misuse (as seen above) (Source: www.cnil.fr). In the UK, similar violations fall under the Privacy and Electronic Communications Regulations (PECR) and UK GDPR. Historically, PECR breaches could be prosecuted or fined up to £500,000, but nowadays the ICO's fine regime follows the GDPR levels (up to £17.5M/4% for the most serious breaches). No high-profile cookie fines have yet been publicly announced by the ICO, but in late 2023 the ICO warned major UK companies with non-compliant banners to fix them or risk enforcement (Source: syrenis.com) (Source: www.mishcon.com) (more on this below).

Daily Penalties and Compliance Orders

In addition to one-time fines, regulators often use **periodic penalty payments** to enforce future compliance. Notably, in the CNIL Google case, the fine scheme included an order that Google must correct its practices within six months or face a **€100,000 per day fine** (Source: www.cnil.fr). The official CNIL decision (Sept 2025) explicitly stated that if Google did not implement the required measures (stop injecting ads and ensure valid cookie consent) within the deadline, it would incur that daily penalty (Source: www.cnil.fr). This "astreinte" (judicial fine) mechanism is a strong sanction to ensure companies actually fix their banners promptly.

Belgian authorities similarly attached daily penalties. In 2024, the Belgian DPA ordered four major news sites (operated by Mediahuis) to add a clear "reject" button to their banners and correct misleading design choices. The order came with a penalty of **€50,000 per day, per website**, for daily non-compliance (Source: noyb.eu). In other words, if any of those sites failed to implement the required changes in time, the publisher would owe €50,000 for every day of delay for each site (Source: noyb.eu). This is among the highest "daily fine" threats seen in cookie enforcement, and it underscores how seriously regulators view refusal of consent.

Other EU regulators have used similar tools. For example, under the Belgian settlement we saw above, a small "fine" of €10,000 was essentially an upfront payment to avoid forcing compliance, illustrating that even token sums can be used deterrently (though this resolution was widely criticized by activists as too lenient (Source: noyb.eu). Regulators may also suspend processing or order temporary bans on certain cookies until consent mechanisms are fixed, though such details are not always publicized explicitly.

Enforcement Case Studies

We now survey representative cases and regulatory announcements that illustrate how these penalties manifest.

- **France/CNIL (Blue and Red Giants)** – The most dramatic examples come from CNIL. In January 2024, CNIL fined Yahoo! **€10 million** for failing to honor user cookie preferences (Source: www.cnil.fr). CNIL had received dozens of complaints that Yahoo left tracking cookies active even when users had opted out, and made it very difficult to withdraw consent afterward. More recently, in September 2025, CNIL announced **€325M** and **€150M** fines against Alphabet/Google and Shein, respectively (Source: www.lemonde.fr) (Source: www.cnil.fr). Both sanctions were explicitly for cookie breaches. For Google, CNIL cited "inserting advertisements into Gmail" and "coercing users" to accept cookies via a cookie wall (Source: www.cnil.fr) (Source: www.techradar.com). For Shein, it noted cookies being dropped without consent and users' choices being ignored (Source: www.cnil.fr) (Source: www.reuters.com). These fines illustrate that major global companies can face the **ceiling of GDPR fines** for something as seemingly mundane as cookie banners, when consent is blatantly neglected. (Google's fine represented a small fraction of its revenue but was justified by the high user impact and repeated defections from compliance; Shein's was roughly 2% of its EU turnover (Source: www.reuters.com).) CNIL also ordered both companies to cease the identified practices within six months or face additional daily penalties (Source: www.cnil.fr).

- **Belgium/APD (Mediahuis and Roularta)** – In mid-2022, the Belgian DPA fined Roularta **€50,000** (Source: iapp.org) for placing tracking cookies without valid consent on two of its websites. The DPA noted that Roularta "did not meet the conditions for collecting user consent for the placement of cookies" under GDPR provisions (Source: iapp.org). This fine, while modest, shows that even a national press publisher cannot ignore consent rules. More recently (Sept 2024), after complaints by privacy NGO NOYB, the Belgian authority ordered four major news outlets (part of the Mediahuis group) to implement a prominent reject button on cookie banners (Source: noyb.eu). These sites were criticized for "deceptive" banner designs. The order explicitly warned of **€50,000 per day** sanctions if non-compliance continued (Source: noyb.eu). (Notably, an earlier handling allowed these sites to pay €10,000 settlements without changing their banners – a result NOYB blasted as letting them "buy themselves free from GDPR" (Source: noyb.eu).)

- **Netherlands/Autoriteit Persoonsgegevens (AP)** – In April 2025 the Dutch DPA signaled a broad enforcement sweep. It sent **warning letters** to 50+ organizations (retailers, media, insurers) across the Netherlands that their cookie banners were misleading or that they placed tracking cookies without consent (Source: www.hoganlovells.com). These letters gave firms three months to correct practices or risk formal investigations and fines (Source: www.hoganlovells.com). While no specific fines have yet been announced, the Dutch DPA's communication highlighted that it treats violations seriously and can impose administrative fines for breaches of the Dutch Telecommunications Act (which implements the EU ePrivacy rules) and parallel GDPR rules (Source: www.hoganlovells.com). Legal analysts noted that this is part of a funded campaign to enforce cookie rules more vigorously in the Netherlands. (The AP stressed that cookies used for marketing are only legal with prior consent, and companies failing to comply face the full panoply of sanctions under GDPR and ePrivacy.)

- **United Kingdom/ICO** – The UK's Information Commissioner has so far been relatively cautious on direct cookie fines. However, in mid-2023 the ICO publicly warned firms that substandard banners would not be tolerated (Source: www.mishcon.com). Deputy Commissioner Stephen Bonner explicitly stated that lacking a clear "reject all" option is a breach of UK law (PECR), and there is "no excuse" for non-compliance (Source: www.mishcon.com). The ICO also indicated that it may engage in a stepped approach ("stages of intervention") before jumping to fines. Notably, in November 2023 reports emerged that the ICO had sent official notices to several of the UK's largest websites (including media and tech firms) demanding improvements to their banners within 30 days or face enforcement (Source: syrenis.com). While those cases have yet to produce public fines, legal commentators observe that ICO enforcement (once seen as lax) is escalating; indeed, a legal blog urges companies to anticipate that the ICO will begin issuing fines rather than mere advice (Source: www.dataprotectionlawhub.com). (Recent UK legislation proposals even raise the stakes: the upcoming Data Protection and Digital Information Bill would authorize much larger fines under PECR, aligning with the GDPR's top tiers (Source: www.mishcon.com).)

- **Other EU DPAs** – Several other European authorities have issued cookie-related sanctions in recent years. For example, in Italy the Garante has discussed cookie design in guidance and launched inquiries, though large fines specifically for banners have been less publicized. In Germany, consumer associations have taken major publishers to court over banner design (e.g. the "Focus Online" case found its banner invalid, meaning consent was not legally obtained (Source: blog.eprivacy.eu) (Source: blog.eprivacy.eu). Spain's DPA has fined dozens of websites in the past for lack of consent or hidden banners (reportedly in five-figure totals). Austria's DSB has also scrutinized cookie consent, issuing orders to fix deceptive banners. The key takeaway is that across the EU, nearly every DPA now treats cookie consent as core privacy compliance: violations are subject to administrative fines and compliance orders.

- **United States (Class Actions and FTC Scrutiny)** – Again, it is important to note there is no federal *cookie law* in the US. However, companies targeting EU users or using GDPR-style standards may still face risk if they apply purpose-broad privacy and thus declare compliance with GDPR/CCPA everywhere. Separately, attorneys general in some states or the Federal Trade Commission (FTC) could conceivably challenge companies for deceptive privacy practices if a cookie banner is misleading (as an unfair or deceptive practice), but such cases are not prominent. The main US "penalties" related to cookies have arisen in the form of **class-action lawsuits** under various tort and consumer-protection theories (privacy invasion, unfair trade, etc.). Recently, US law firms have launched numerous cookie-related class actions, typically alleging that websites' banners or policies mislead consumers. These suits can result in monetary settlements (often in the low millions) but their ultimate viability remains untested by courts (Source: ipwatchdog.com). In contrast to the GDPR fines, these class actions are usually much smaller in aggregate – and the US government itself has not imposed big fines purely for cookie banners as of 2025 | .

In summary, the **penalties for failing to show or properly configure a cookie consent banner** can be severe, especially in Europe. At minimum, a non-compliant website might receive an order to fix its banner or stop using cookies, and if it fails to do so it can incur daily fines. In the worst case, DPAs have demonstrated they will use their full fining powers (up to 2–4% of turnover) when the violation is blatant and widespread (Source: www.reuters.com) (Source: www.cnil.fr). We present a table of notable cases below:

COUNTRY / REGULATOR	YEAR	ENTITY (COMPANY/ORG)	PENALTY/ACTION	VIOLATION
France (CNIL)	2025	Google (Alphabet)	€325 million fine; 6-month compliance order; €100k/day penalty if not cured (Source: www.cnil.fr) (Source: www.cnil.fr)	Inserting ads and placing tracking cookies without valid consent (coercive “cookie wall”) (Source: www.lemonde.fr) (Source: www.techradar.com).
France (CNIL)	2025	Shein (Infinite Styles Services)	€150 million fine (Source: www.cnil.fr)	Placing advertising cookies without consent, ignoring opt-outs (Source: www.reuters.com) (Source: www.cnil.fr).
France (CNIL)	2023	Yahoo! (Yahoo EMEA)	€10 million fine (Source: www.cnil.fr)	Ignoring users’ refusal of cookies on yahoo.com and Yahoo Mail (consent not respected) (Source: www.cnil.fr).
Belgium (APD)	2024	Mediahuis (publisher of 4 titles)	Order to fix banners (add “reject”); €50,000/day penalty if not complied (Source: noyb.eu)	Using deceptive cookie banners lacking clear opt-out (Source: noyb.eu).
Belgium (APD)	2022	Roularta Press Group	€50,000 fine (Source: iapp.org)	Failing to meet consent requirements when placing cookies on websites (Source: iapp.org).
Netherlands (AP)	2025	50 companies (retailers, media, etc.)	Warning letters; 3-month deadline to fix or face fines (Source: www.hoganlovells.com)	Misleading cookie banners or placing tracking cookies without valid consent (Source: www.hoganlovells.com).
UK (ICO)	2023	Various top sites (news, tech)	Formal notices given; 30 days to fix or face enforcement (Source: syrenis.com)	Cookie banners lacking clear options (‘reject all’) in breach of PECR/GDPR (Source: syrenis.com) (Source: www.mishcon.com).
EU-wide jurisdictions (Varies)	2023–24	Various websites	Compliance orders by DPAs; small fines or commitments	Use of dark patterns; blocking content unless accept (“cookie walls”); insufficient information.
(For comparison) US†	—	—	No federal fine for cookies; CCPA opt-out regs; FTC warnings possible	No explicit consent mandate; privacy lawsuits in tort (class actions) observed.
† In the US, enforcement is driven by state privacy laws and the FTC rather than				

COUNTRY / REGULATOR	YEAR	ENTITY (COMPANY/ORG)	PENALTY/ACTION	VIOLATION
an EU-style penalty regime (Source: cookie-compliance.co).				

Evidence and Data Analysis

Compliance Rates and Studies

Multiple studies have documented widespread non-compliance with cookie consent rules:

- **Academic Surveys**: Kampanos & Shahandashti (2021) systematically surveyed 17,000 websites in Greece and the UK and found that although around 60% of sites were issuing third-party tracking cookies, *fewer than 50%* displayed any cookie notice at all (Source: arxiv.org). Even among those with banners, the majority either nudged users toward "accept" or made rejection harder, with very few offering a straightforward opt-out (Source: arxiv.org). This suggests a large fraction of sites simply violate the law by not informing users at all. Another study by Matte et al. (2019) crawled nearly 23,000 European sites using the IAB TCF framework and found at least one legal violation on *54% of sites* tested (Source: arxiv.org). Common infractions included pre-checked consent boxes and failing to honor an opt-out selection (about 27 sites even stored positive consent after explicit opt-out) (Source: arxiv.org). These results indicate that a majority of sites, at least in the sampled populations, were not properly respecting consent requirements.

- **Automated Detection Tools**: Researchers have developed tools (e.g. "Cookiescanner" (Source: arxiv.org) to detect and evaluate cookie banners at scale. Their findings reinforce that many banners are implemented incorrectly. Gundelach & Herrmann (2023) note that "many website operators do not comply with the law and track users prior to any interaction with the consent notice, or attempt to trick users into giving consent through dark patterns" (Source: arxiv.org). This study scanned the top 10,000 websites and found that manual filters often missed banners (suggesting the problem is widespread) and that detecting "decline" buttons automatically remains challenging. Overall, specialized scanning found numerous instances where banners lacked a decline option or struggled to give equal weight to reject/accept choices (Source: arxiv.org). These systematic analyses provide empirical support for enforcement actions: regulators had anticipated that compliance would be lax, and the data show that indeed over half of sites had some banner issue.

- **Privacy Complaints and Regulatory Attention**: Regulatory agencies themselves report it is **complaints-driven**. For instance, a privacy law firm blog summarizes that the ICO's heightened attention in 2023 was triggered in part by "increasing complaints from data subjects" and advocacy campaigns (Source: www.dataprotectionlawhub.com). Citizen surveys also back the need for transparency: an EU public consultation found that over 96% of respondents want to be asked before third-party cookies are used on their device. In short, both bottom-up public pressure and top-down policy changes (like the draft ePrivacy Regulation) point to a consensus that cookie consent must be taken seriously.

Fine Statistics

While we lack a central repository of all cookie-related fines, the known examples allow some quantification:

- **Magnitude**: The fines imposed by DPAs for cookie breaches have ranged from tens of thousands to hundreds of millions of euros. Aside from Google/Shein (hundreds of M€) and Yahoo (10M€), many fines in 2019–2023 were in the low-six-figure range. For example, earlier CNIL fines included €150k–€200k against smaller sites. France's decisions often start around €100–150k for medium sites (Source: www.cnil.fr). Similarly in Italy and Spain, fines of around €100k have been reported for first-time or medium-scale offenders. The Belgian Roularta fine of €50k was on the lower end but still significant for a mid-sized publisher (Source: iapp.org).

- **Percentage of Turnover**: In large cases, fines approach statutory limits. Notably, CNIL framed the Google/Shein fines as **approximately 2% of European revenue** (Source: www.reuters.com). (Shein explicitly noted their fines correspond to ~2% of its 2023 EU turnover (Source: www.reuters.com).) This suggests DPAs are indeed inclined to hit the maximum bracket for blatant consent breaches by major players. Smaller organizations typically receive relatively lower absolute fines, but always proportional to their size under the "effective, proportionate, dissuasive" mandate of GDPR.

- **Aggregate Data**: As cookie enforcement has intensified only in the past few years, systematic data may emerge later. However, regulatory notices and press releases indicate *COVID-era inactivity* (2019–2020) gave way to a flurry of cases in 2021–2025. For example, France's CNIL had a "cookie crackdown" action plan from 2019, and by 2022–2023 it was imposing fines almost monthly (especially as its legal deadline required major sites to comply by Sept 2020 (Source: www.cnil.fr). In the UK, the ICO's actions remain more advisory, but spreadsheets of PECR notices show an uptick in cookie-related cases being logged in 2023–24. The overall trend is clear: **enforcement is rising steeply**, and penalties are climbing.

CATEGORY	EXAMPLES / DATA
Academic compliance studies	Kampanos & Shahandashti found <50% of sites show any cookie notice, even though >60% use 3rd-party cookies (Source: arxiv.org). Matte et al. found ~54% of tested sites violated consent requirements (Source: arxiv.org). These large-sample studies confirm high non-compliance rates.
Major fines (EU)	CNIL fines: Google €325M, Shein €150M (2025) (Source: www.lemonde.fr) (Source: www.cnil.fr); Yahoo €10M (2023) (Source: www.cnil.fr); numerous smaller fines (in 5-6 digits) to others. Belgian DPA: Roularta €50k (2022) (Source: iapp.org). (Fines often hit ~2–4% of turnover (Source: www.reuters.com).)
Enforcement trends	CNIL announced dozens of orders for site compliance. Dutch AP issued warnings to 50 firms (2025) (Source: www.hoganlovells.com). UK ICO sent notices to major sites (2023) (Source: syrenis.com). Privacy NGO NOYB filed ~500 complaints across EU targeting banners (Source: www.sovy.com).
Penalty mechanisms	DPAs use: one-time fines, **daily fines** (e.g. Google: €100k/day (Source: www.cnil.fr); Belgian news: €50k/day (Source: noyb.eu), injunctions/orders to fix. Settlements (e.g. Belgian news paid €10k each instead of compliance (Source: noyb.eu) highlight enforcement creativity.

Case Studies and Examples

To illustrate how the law is applied, we describe a few detailed examples of regulatory actions:

- **Google (France, 2025)**: Arguably the most publicized enforcement action involved Google. On Sept 1, 2025 CNIL announced a €325M fine (Source: www.cnil.fr). The investigation was prompted by a complaint from NOYB; CNIL inspectors examined Google's Gmail service and account signup process (Source: www.cnil.fr) (Source: www.cnil.fr). The findings were striking: Google was inserting ads into Gmail inboxes disguised as personal emails, but more relevant here was how it handled cookies. CNIL charged that Google "coerced" users into accepting tracking cookies (a "cookie wall") when they created accounts, and that Gmail's interface nudged users toward consent (Source: www.techradar.com) (Source: www.cnil.fr). In short, the banner/design deprived users of free choice. In imposing the fine, CNIL cited repeated negligence (Google had been fined for similar issues in 2020 and 2021), the sheer scale of users affected (over 74 million), and the high revenues of Google. Importantly, the sanctions included an order for Google to implement needed changes within six months; failing that, Google faces an additional €100,000 per day (Source: www.cnil.fr). Google publicly responded by committing to make analytics changes, emphasizing that only a small fraction of users see "ads" in Gmail. (This case underscores that even the biggest tech firm is not immune: compliance with consent rules is mandatory irrespective of company size.)

- **Shein (France, 2025)**: In the same announcement, CNIL fined Shein's EU subsidiary €150M (Source: www.cnil.fr). Shein is an online fast-fashion retailer targeting French consumers (about 12 million monthly visitors in France, according to CNIL). A 2023 website inspection found widespread breaches: Shein was placing tracking cookies on visitors' devices *without consent*. Users who opted out were ignored, and the banner did not allow easy withdrawal of consent (Source: www.reuters.com) (Source: www.cnil.fr). The regulators specifically mentioned "placing some cookies without the consent of internet users, by not respecting their choices and by not informing them properly" (Source: www.cnil.fr). Shein contested the fine as disproportionate and politically motivated (arguing it had since remedied its practices and that its ad-dependent business model had been unfairly targeted) (Source: www.reuters.com). The fees corresponded to roughly 2% of Shein's FY2023 revenue in Europe (Source: www.reuters.com). Shein has indicated it will appeal, but the fine sends a strong message: large e-commerce actors are under scrutiny for consent compliance just like tech platforms.

- **Yahoo (France, 2023)**: Prior to the Google/Shein decisions, the CNIL had already demonstrated willingness to fine big players for cookie faults. On Dec 29, 2023 CNIL fined Yahoo EMEA €10M (Source: www.cnil.fr). By its own account, Yahoo failed to "respect the choice of Internet users who refused cookies on its 'Yahoo.com' website" and made it impossible to withdraw consent on Yahoo Mail (Source: www.cnil.fr). The fine followed dozens of user complaints. Again, the problem was essentially that Yahoo's sites kept dropping tracking cookies even after refusal, and users were funneled into consent via UX tricks. CNIL noted that it had given a formal notice back in 2020, yet problems persisted. The €10M fine was notable as a rare case against a major US tech brand (Yahoo is now part of Apollo), and it demonstrated that old obligations still carried weight. Yahoo claimed it had gotten compliant by late 2023, but had failed before. The sanction forced Yahoo to rework its banners to give equal weight to "reject".

- **Mediahuis (Belgium, 2024)**: In September 2024, after NOYB complaints, the Belgian DPA (Commission de la Protection de la Vie Privée) issued decisions against the publisher Mediahuis (which operates news sites such as De Standaard, Het Nieuwsblad). The DP ordered each site to add a clearly labeled "reject" button in the first layer of the cookie banner and to scrap any misleading color coding (e.g. making "reject" gray on gray background) (Source: noyb.eu). Prior to that, NOYB had charged these sites with using illegal banners for years, but authorities had previously settled by accepting a mere €10,000 payment from Mediahuis – without any compliance fix (Source: noyb.eu). Under pressure, the DPA reversed course and imposed strict conditions: "If Mediahuis fails to comply, it faces a penalty of €50,000 per day per website" (Source: noyb.eu). This created a powerful incentive to redesign the banners. The case highlights not so much the monetary fine (the order itself had no fixed punitive sum, just the threat of €50k/day), but the **dramatic enforcement leverage** given to regulators.

- **Roularta (Belgium, 2022)**: As an earlier Belgian example, in May 2022 the APD fined Roularta €50k (Source: iapp.org). Roularta (an owner of magazines and websites) was found not to have obtained valid cookie consent as required by GDPR/PECR. The DPA's Litigation Chamber explicitly stated that Roularta "did not meet the conditions for collecting user consent" for cookies (Source: iapp.org). While €50k is a small line item for a publishing group (albeit probably a significant percentage of their ad revenue on those sites), it was a data protection enforcement – and the APD warned others that further complaints could lead to larger fines. The case underlines that even traditional media companies must heed digital consent rules.

In each of these examples, the **absence or inadequacy of a cookie banner** was the crux of the violation. Penalties ranged from compliance orders and relatively modest fines (Belgium, €50k) to blockbuster fines (France, €325M). Organizations penalized often included a mix of domestic and international firms – and in many cases, legal actions were driven by EU jurisdiction (e.g. Google and Shein infractions were considered under French law because those companies were targeting the French market).

Multiple Perspectives and Context

In considering the penalty issue, it's important to recognize multiple viewpoints:

- **Regulatory Perspective**: DPAs see cookie consent as a critical privacy baseline. They emphasize that user autonomy over tracking is non-negotiable. The heavy fines in France and elsewhere send a deterrent message that even large players cannot flout consent rules. DPAs also highlight that cookie consent is often the "first step" towards comprehensive GDPR compliance: ignoring banners often correlates with other data abuses. For example, France's CNIL imposed cookies fines as part of a broader campaign on tracking non-compliance (Source: www.cnil.fr). Regulators have openly warned businesses: "no excuse" exists for not providing a proper reject option (Source: www.mishcon.com). They also acknowledge user complaints – DPAs note the flood of complaints about banners as justification for action. As one expert summary put it, Europe's regulators have responded to user "rage" over persistent or deceptive banners by cracking down (labels like "clickspamageddon" reflect public sentiment). In regulatory guidance, the emphasis is on transparency and ease of refusal: rejecting cookies must be "just as easy" as accepting (Source: www.cnil.fr).

- **Corporate Perspective**: On the business side, opinions vary. Many companies grudgingly accept cookie banners as a legal necessity, though they often view them as a UX burden and a barrier to data-driven marketing. Some executives have publicly complained that the rules degrade user experience, cause banner fatigue, and hamper online advertising. Indeed, trade groups in Europe have lobbied for more lenient rules (e.g. exempting analytics cookies from consent, or allowing them by default). For instance, the UK Data Reform Bill proposed that analytics cookies be "permitted without consent," reflecting industry pressure to reduce banner demands (though critics say this undermines user choice) (Source: www.mishcon.com). Many sites use banner solutions provided by Consent Management Platforms (CMPs), and industry blogs frequently discuss "consent rates"

and ways to maximize opt-ins. Nevertheless, the dominant corporate view is that compliance is mandatory: after the Google/Shein fines, firms with any European traffic will want robust consent flows to avoid a similar fate. Some companies do complain that regulators grant unfair advantage to local competitors who comply, e.g. Shein labeling its fine "politically motivated" because it competes with French retailers (Source: www.reuters.com). But ultimately, the view is that ignoring banners risks fines and reputational harm.

- **Consumer/Privacy Advocate Perspective**: Privacy activists and many consumers view cookie banners themselves with ambivalence or annoyance, but generally support the concept that consent must be meaningful. Organizations like NOYB concentrate on making those banners actually respect user autonomy. They condemn "take it or leave it" cookie walls and hidden opt-out buttons. NOYB's campaign slogan referred to "cookie banner terror" and has already resulted in hundreds of complaints (Source: www.sovy.com) (Source: noyb.eu). Privacy NGOs argue that companies' use of dark patterns undermines the law's intention. A common militant position is that any barrier to service if cookies are refused (a hard cookie wall) is never valid consent. This perspective pushes for strict enforcement and affected CNIL enforcement of cookie walls as data-protection breaches (Source: www.lemonde.fr). On the user side, evidence shows most people simply click "accept" just to clear the nag, suggesting that consent notices may not be serving privacy much anyway. Still, advocates argue that the legal framework must force better design: as one lawsuit caption put it, "users should have a clear, yes or no option" (Source: www.sovy.com). NOYB and others have explicitly said they view fines like Mediahuis' settlement (€10k, no changes) as unacceptable; they want real change enforced by the DPAs ((Source: noyb.eu)) . In short, from a privacy viewpoint the question of "penalty" is less about dollar amounts and more about whether enforcement will *finally* yield genuine compliance rather than token settlements.

- **Legal/Academic Perspective**: Legal scholars note that cookie consent laws are technically complex. For example, there is debate over whether tracking consent might sometimes be obtained on "legitimate interest" grounds rather than opt-in (a view rejected by most DPAs). There have been several court cases: the German Regional Court of Munich (2020-21) found that a news site's banner (Focus Online) did *not* obtain valid consent because it did not make refusal as easy as consent (Source: blog.eprivacy.eu) (Source: blog.eprivacy.eu). At a higher level, academics focus on user testing and automated compliance checks. They conclude that enforcement is warranted: for instance, Gundelach & Herrmann's research indicates many sites track users *before* banner interaction, confirming that regulators might already be investigating these exact problems (Source: arxiv.org). Lawyers also point out that as GDPR Article 83 fines are expressed as maximum percentages, national authorities have discretion. Early cookie cases tended toward smaller fines possibly due to the novelty of enforcement, but the recent shift to multi-million penalties suggests authorities are interpreting "effective, proportionate" to mean "dissuade other companies by hitting them hard."

- **Industry Analysts / Future View**: A final perspective is the future of cookie consent itself. Some experts now question whether cookie banners (the traditional "ePrivacy approach") are sustainable. Indeed, European commission officials have acknowledged "consent fatigue." There are proposals to overhaul the ePrivacy Directive (the so-called ePrivacy Regulation, under discussion since 2017). One news piece reported that the EU plans to revise cookie rules by 2025 in light of user complaint (so-called "clickspamageddon") (Source: www.tomshardware.com). Potential changes include making analytics cookies exempt or developing standardized browser-level consent signals. The outcome could alter what penalties are in store: for example, if analytics cookies become "implied consent," some currently $bill+ fined behavior might become legal. However, most consent experts caution that enforcement of *transparent, non-coercive consent* will remain central, even if some rules are loosened. Any future changes will likely preserve user choice for tracking (advertising/tracking cookies), so failing to show a banner (or providing a sham banner) could still be punishable.

Implications and Future Directions

Practical Implications for Organizations

The immediate implication of these penalties is that **organizations must treat cookie banners as serious compliance projects**. The days when a website operator could dismiss cookies as "just annoyance" are over, at least if the business has any exposure to EU/UK markets. Companies should audit their banners and cookie usage proactively. This means ensuring *all* non-essential cookies are behind a banner that meets the legal tests: informing the user, offering an easy "reject" or granular choices, and recording valid consent before firing any tracking scripts. Compliance teams should track the announcements of enforcement actions and model their banners on best practices (for example, giving equal prominence and styling to accept and reject, and

avoiding “cookie walls” that force acceptance). Some firms will upgrade to new consent-management platforms. Lawyers also advise that consent logs and banner design decisions should be documented as evidence of compliance efforts, in case of future investigations.

Given the rising stakes, risk managers are recalculating exposure. A small business in Europe could incur fines in the **tens of thousands** for non-compliance, a mid-size business in the **low six figures**, and large multinationals potentially facing **eight- or nine-figure** penalties if blatant violations persist. Insurance products for cyber/privacy risk may start accounting for cookie consent duty in their policies. Moreover, given that DPAs often coordinate (the European Data Protection Board can facilitate cross-border enforcement), even companies operating primarily in one country should heed the strictest approach: most likely the French model right now. Multinationals, as we saw with Google, can be hit in any jurisdiction where their products or services reach.

Beyond fines, companies should note that reputational damage is also a penalty. Media coverage of big fines can weaken user trust. At a minimum, a privacy notice or cookie policy misstep triggers a flow of user complaints, which in turn invites regulators. The **opportunity cost** of not showing a banner is multiple: regulatory fines, remediation expenses (redesigning the website on short notice), lost user trust, and possible civil suits. In highly regulated industries like finance or healthcare, cookie consent is one aspect of overall data handling scrutiny; repeated failures might even lead authorities to audit other practices. In summary, the cost of compliance (investing in a proper banner and design) is far lower than the subject penalties.

Broader Context and Developments

Several broader forces will shape how cookie consent enforcement evolves:

- **Evolving Privacy Laws**: In Europe, the upcoming ePrivacy Regulation (if adopted) will likely codify many of the consent standards into a single regulation. Proposed changes include clarifying definitions of “cookie wall” and possibly expanding exemptions (e.g. for certain analytics). If passed, it may also replace or integrate national cookie laws. Whatever the final form, enforcement powers are likely to increase. Similarly, in the UK, the Data Protection and Digital Information Bill signals stiffer penalties (and might ease some cookie rules, e.g. analytics consent). Organizations should watch these legislative tracks as they will impact compliance obligations and potential penalties.

- **Technology Shifts**: The tech industry is moving away from third-party cookies for tracking (e.g. Google’s deprecation of third-party cookies in Chrome, and privacy-focused changes in browsers). In the coming years, fewer sites may use cookie-based advertising; instead, new methods (browser APIs or local storage) may arise. Regulators have signaled that “consent or pay” paywalls should not be allowed even using new technologies. Thus, even as the technical means change, the principle of user choice remains. Encryption, fingerprinting, and server-side tracking will likely be targeted by law with similar consent rules (GDPR covers any “processing” of personal data, not only cookies).

- **International Trends**: Outside Europe, some countries are beginning to focus on user consent. For example, India’s PDP Bill (once enacted) will emphasize user consent for personal data. In Asia-Pacific, awareness of EU cookie rules is growing. Interestingly, some multinational companies are simply applying GDPR-like consent everywhere to simplify policy (so in practice many non-EU sites now display cookie banners). If more privacy laws (US state laws or Asia-Pacific) start explicitly mentioning tracking, the notion of “banner penalty” might spread globally. However, as of now, the most severe penalties remain European.

- **Enforcement Campaigns**: DPAs have indicated cookie revenue as a special campaign. For instance, CNIL’s 2019-2025 “cookie action plan” has involved issuing guidelines, formal notices, and fines in waves. Privacy NGOs like NOYB galvanize more complaints (NOYB’s “cookie banner campaign” filed 850 complaints across Europe). It is likely DPAs will continue using both carrot (guidance, temporary reprieves) and stick (fines, public announcements) for the foreseeable future. As the Stephenson Harwood blog noted, regulators see cookie enforcement as a priority area (Source: www.dataprotectionlawhub.com) (Source: www.dataprotectionlawhub.com).

- **Judicial Clarifications**: Courts will further clarify borderline issues. Already, the CJEU (in 2020) indicated that pre-ticked checkboxes and link-only information were invalid forms of consent. Lower courts (like Munich’s Focus Online case) continue this trend. If higher courts in member states (and possibly the CJEU) tackle cookie banner design questions, jurisprudence will solidify the liability contours. These decisions could impact penalty assessments: if a court holds a banner unlawful, a regulator can confidently impose a fine knowing the legal basis is firm.

Conclusion

The penalty for not showing a proper cookie consent banner can be severe. Under prevailing privacy laws, a missing or deficient banner means user consent has not been validly obtained – a violation that can trigger the full weight of data protection sanctions. In Europe, regulators explicitly treat cookie consent breaches as GDPR violations, subject to the highest tiers of fines. Case studies have shown penalties ranging from tens of thousands of euros up to hundreds of millions, depending on the scale and intent of the violation. We have seen regulators impose massive fines (e.g. €325M on Google, €150M on Shein in 2025) and daily penalties (e.g. €100k per day) for failures to obtain cookie consent (Source: www.lemonde.fr) (Source: www.cnil.fr). Even more routine fines (in the low six figures) have been common for smaller actors.

These outcomes reflect a consistent message: **cookie consent is not optional, and the authorities will enforce it vigorously**. Organisations neglecting banner requirements risk not only financial penalties but also forced operational changes (removing unauthorized cookies) and reputational harm. The burden rests on web operators to ensure their consent mechanisms meet the legal standards of being informed, freely given, and easily withdrawn (Source: ico.org.uk) (Source: www.cnil.fr).

Looking ahead, while the user experience of cookie banners may evolve (with possible regulatory reforms aiming to reduce “banner fatigue”), the fundamental expectation remains: users must have clear control over tracking cookies. Regulators have signaled that non-compliance will continue to attract scrutiny and sanctions. In sum, the “penalty” is that failing to display a compliant banner is a breach of law – and those breaches are increasingly met with **strict, often quite hefty, sanctions** (Source: www.reuters.com) (Source: www.cnil.fr). Organizations would be well-advised to not only display cookie consent banners but to implement them in accordance with guidance and past enforcement precedents.

Tags: cookie consent penalties, gdpr, cookie law, eprivacy directive, data protection, cnil, cookie compliance

---