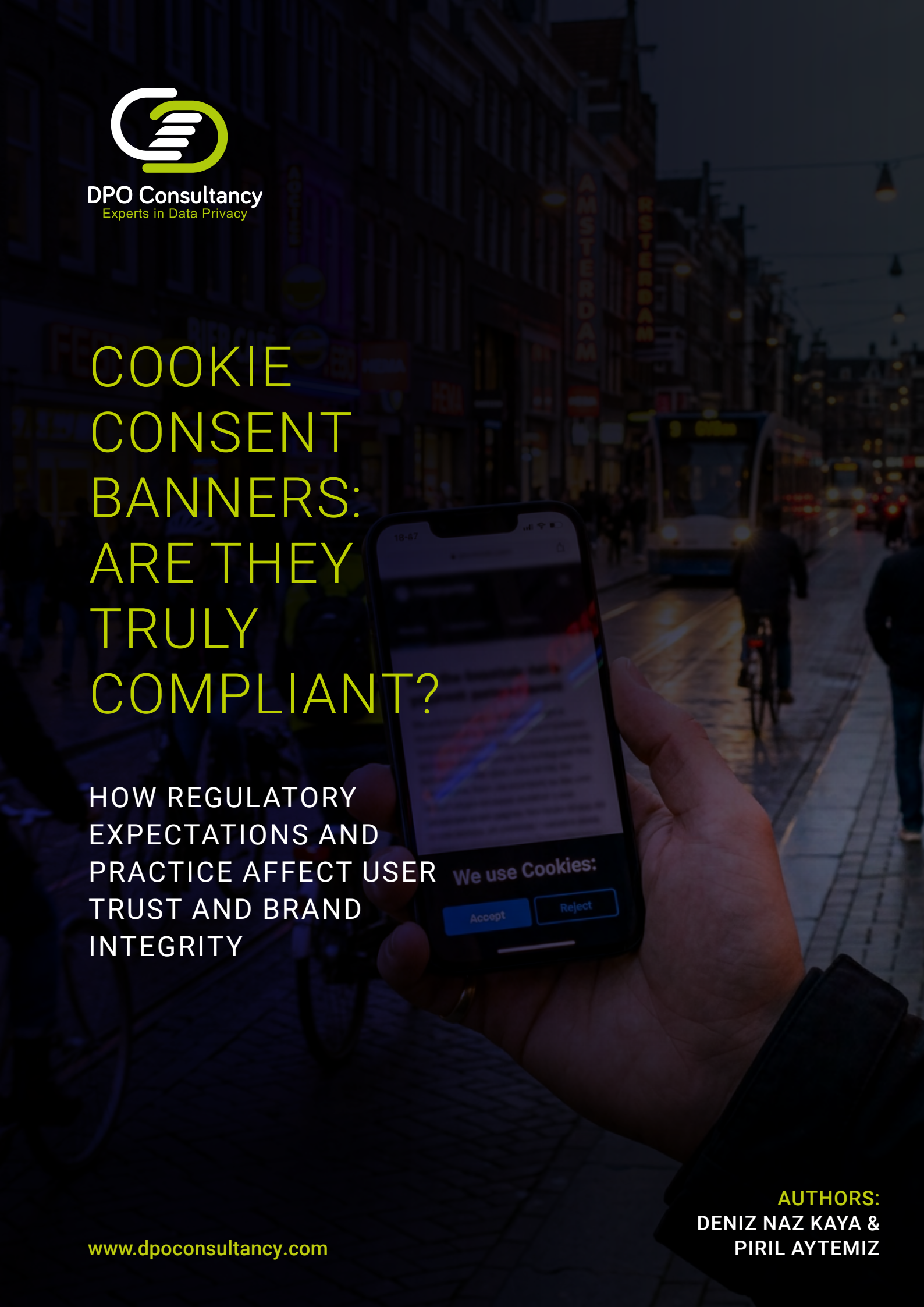
DPO Consultancy
Experts in Data Privacy

COOKIE CONSENT BANNERS: ARE THEY TRULY COMPLIANT?

HOW REGULATORY EXPECTATIONS AND PRACTICE AFFECT USER TRUST AND BRAND INTEGRITY



AUTHORS:
DENIZ NAZ KAYA &
PIRIL AYTEMIZ

www.dpoconsultancy.com

COOKIE CONSENT BANNERS: ARE THEY TRULY COMPLIANT?

The regulation of cookies and similar tracking technologies in the EU operates at the intersection of two key legal instruments: the **General Data Protection Regulation (GDPR)** and the **ePrivacy Directive**. While the ePrivacy Directive (often referred to as the "cookie law") governs the conditions under which information can be stored or accessed on a user's device, the GDPR provides the overarching framework for valid consent and lawful processing of personal data. Together, these instruments establish a harmonized system designed to safeguard users' autonomy, transparency, and control in the online environment.

1. General Data Protection Regulation (GDPR) and ePrivacy Rules on Cookies

1.1. What is consent?

Under the ePrivacy Directive, consent is required whenever an organization seeks to access or store information on a user's device, which includes the placement of cookies or similar tracking technology. This obligation applies regardless of whether the data collected qualifies as personal data; merely accessing the user's terminal equipment triggers the consent requirement.

The standard for consent derives from **Article 4(11) GDPR**, which defines it as a "freely given, specific, informed and unambiguous indication of the data subject's wishes" expressed by a clear affirmative action. For cookies, this means users must make an active choice that reflects genuine intent; silence, inactivity,

or pre-ticked boxes are not valid forms of consent. Continued browsing or scrolling does not constitute consent; users must take an explicit action.

1.2. ePrivacy Directive cookie consent requirements

The ePrivacy Directive translates this standard into clear operational requirements for websites and digital services. Cookie consent must be:

- **Freely given:** Users must have a genuine choice and not face access barriers or marketing pressure.
- **Specific:** Each cookie category must have a clearly defined purpose, such as analytics, personalization, or advertising.
- **Informed:** Information must be clear, comprehensive, and easily accessible.
- **Unambiguous:** Users must take an explicit, affirmative step such as clicking an "Accept" button.

These principles reflect the Directive's goal of preserving the confidentiality of electronic communications and giving users genuine control over tracking technologies on their devices.

Cookie categories and consent granularity

In practice, websites often group cookies into functional categories such as analytics, personalization, and advertising. Each category serves a distinct purpose and involves different levels of data processing. To comply with the ePrivacy Directive and GDPR, users should be able to grant or refuse consent separately for each category, ensuring that consent remains both specific and informed.

1.3. General Data Protection Regulation (GDPR)

The GDPR complements the ePrivacy Directive by establishing lawful bases for processing under Article 6. Of these, consent and legitimate interest are the most relevant to cookies. However, for tracking or advertising purposes, consent is almost always required.

Articles 7 and Recital 32 specify that consent must be freely given, specific, informed, and unambiguous, and must be given by a clear affirmative act. Pre-ticked boxes or implied consent (such as scrolling or inactivity) do not meet this standard. Importantly, controllers must be able to demonstrate that valid consent was obtained, and users must be able to withdraw it as easily as it was given.

Failure to comply can result in administrative fines of up to €20 million or 4% of global annual turnover (Article 83). The GDPR also applies extraterritorially to organizations outside the EU that target or monitor EU residents.

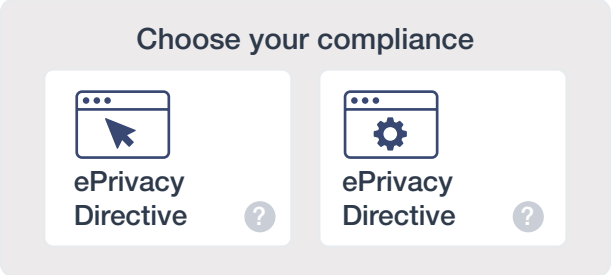
Recital 30 clarifies that online identifiers, such as cookies, IP addresses, or device IDs, can constitute personal data if they can be linked to an individual. Only "strictly necessary" cookies, essential to provide a service explicitly requested by the user, are exempt under Article 5(3) of the ePrivacy Directive.

1.4. Cookie compliance

To comply with both the GDPR and ePrivacy Directive, organizations should:

- Obtain **prior consent** before activating non-essential cookies.
- Provide **plain-language explanations** about the purpose of each cookie.
- **Log and retain consent records** as evidence of compliance.
- Allow users to access services even if they **refuse cookies**.
- Offer a simple and visible way to **withdraw or change consent**.

Effective cookie compliance is not just a legal exercise. It's also a design and communication challenge. Organizations must embed compliance in the **user experience** to build transparency and trust.



1.5. General Data Protection Regulation (GDPR) vs ePrivacy Directive on Cookie Consent

While the GDPR sets the general framework for consent and data processing, the ePrivacy Directive serves as a **lex specialis**, addressing cookie and tracking practices more specifically. The table below summarises the key similarities and differences relevant to cookie consent.

Aspect	GDPR	ePrivacy Directive
Primary focus	Regulates personal data processing.	Regulates confidentiality of electronic communications and device access (cookies, trackers).
Consent standard	Must be freely given, specific, informed, and unambiguous (Art. 4(11), Art. 7).	Must meet the GDPR's consent standard for storing or accessing information on user devices (Art. 5(3)).
Trigger for application	Processing of personal data.	Any storage of or access to information on user devices, even if non-personal.
Scope of data	Personal data only.	Both personal and non-personal electronic communications data.
Legal basis alternatives	Six lawful bases; consent is one option.	Consent required in nearly all cases, except for strictly necessary cookies.
User rights	Focuses on data subject rights (access, erasure, withdrawal).	Focuses on control over device access and communication privacy.
Precedence	Applies generally.	Takes precedence as lex specialis in cookie and tracking contexts.
Regulatory goal	Ensure lawful and transparent processing.	Protect privacy in electronic communications and prevent covert tracking.

2. Compliance Failures

Although the regulatory standards are clear, many websites continue to use non-compliant banners. These failures are typically design-driven, prioritising data collection over genuine consent.

2.1 Lack of Equal "Accept" and "Reject" Options

Many banners still lack clearly visible and equally prominent "Accept" and "Reject" buttons. This undermines the principle of freely given consent and remains one of the most common violations observed by European DPAs.

2.2 Failure to Block Cookies Before Consent

Under GDPR and ePrivacy rules, no non-essential cookies may be placed before a user consents. Yet, many websites activate tracking scripts on page load, often due to third-party tools or poor configuration.

2.3 Inability to Withdraw or Modify Consent

Users must be able to withdraw or modify consent at any time, easily and visibly. In practice, many banners lack a persistent icon or link for reopening cookie settings.

2.4 Outdated or Incomplete Information

Consent cannot be informed if the underlying cookie policy is outdated. Many websites fail to refresh their cookie lists regularly, meaning users consent to inaccurate information.

2.5 Use of "Dark Patterns"

Manipulative interface designs, such as bright "Accept" buttons or hidden rejection options, remain widespread. The European Data Protection Board (EDPB, 2023) and multiple national DPAs have explicitly warned that such "dark patterns" invalidate consent.

2.6 Other Failures

Other recurring issues include missing consent logs, misclassification of cookies as "necessary," reliance on implied consent banners, and the use of cookie walls that restrict access to users who refuse tracking. Cookie walls refer to mechanisms that block access to a website or service unless the user agrees to non-essential cookies. Such practices are generally considered unlawful unless a genuine, tracking-free equivalent is offered.

Integrative Discussion

These failures illustrate a persistent gap between **regulatory expectations** and business implementation. Some stem from technical or UX complexity, but many reflect a lack of governance or awareness. Achieving compliance requires more than legal text; it demands **ethical design, documentation, and regular audits**.

To see how these challenges play out in practice, the next section reviews key enforcement actions by European DPAs.

Data Protection Authorities

3. Enforcement Actions of Data Protection Authorities (DPAs)

Growing enforcement activity across Europe signals that regulators view cookie compliance as a cornerstone of privacy protection. The Dutch and Belgian authorities have led the way in addressing misleading or non-transparent banners.

3.1 The Dutch Data Protection Authority's Structural Monitoring Program

In April 2025, the Autoriteit Persoonsgegevens (AP) launched a long-term plan to monitor 10,000 organizations over several years structurally. Each year, 500 entities will be required to amend or remove non-compliant banners or risk investigation and fines.

The AP also issued nine design rules for lawful cookie banners, prohibiting pre-ticked boxes, hidden rejection buttons, and additional clicks to refuse cookies. Consent must be as easy to refuse as to give. This marks a shift from reactive enforcement to continuous regulatory oversight, promoting higher compliance standards across the Dutch industry.

3.2 The Belgian Data Protection Authority's Targeted Decisions

The Belgian DPA (GBA/APD) has taken a case-driven approach. In 2024, it issued key decisions against Mediahuis and RTL Belgium for misleading cookie banners.

- Mediahuis (Decision 113/2024): The company lacked a "Reject All" button and used visually dominant "Accept All" options. The DPA found this design invalidated consent and ordered revisions, threatening fines of €25,000 per day per website.
- RTL Belgium (Decision 131/2024): Similar issues were identified, leading to a mandatory redesign ensuring equal prominence of consent options.

Both decisions confirmed that dark patterns breach the GDPR's fairness principle and that legitimate interest cannot replace consent for tracking cookies.

3.3 Comparative Analysis and Emerging Trends

- The Dutch AP applies a preventive, large-scale monitoring strategy, focusing on systemic compliance.
- The Belgian DPA follows a case-by-case enforcement model, relying on rulings to clarify standards.

Despite methodological differences, both converge on key principles:

- Consent must be easy to give and withdraw.
- Design neutrality is essential.
- Transparency and user control are non-negotiable.

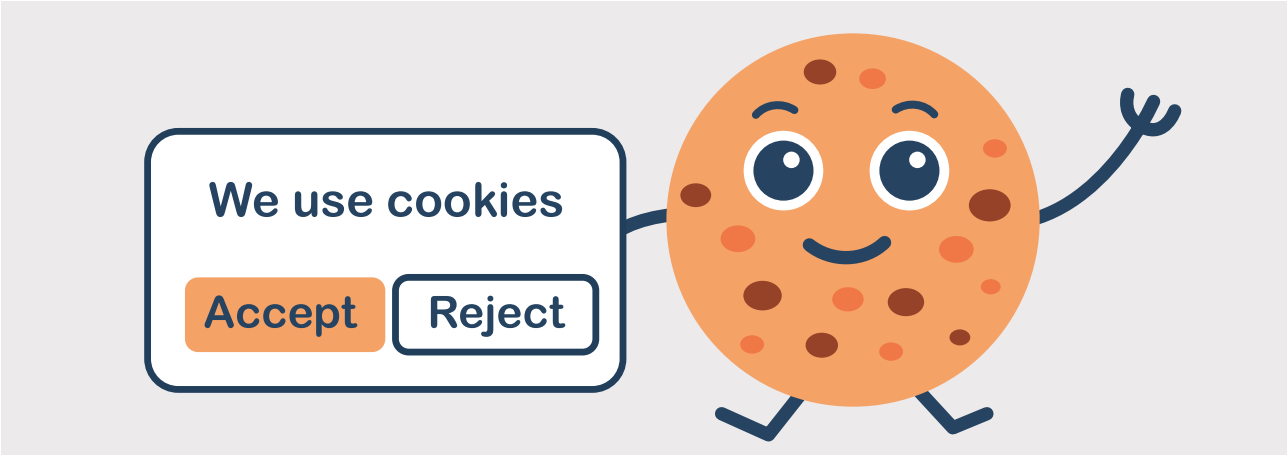
These enforcement trends are shaping a more consistent EU-wide approach, even as companies explore alternative consent models, such as "pay-or-okay."

4. Mini Study: Real-World Cookie Banner Compliance

To understand how theoretical and regulatory requirements are translated into practice, a brief compliance review was conducted on seven widely used websites across various sectors. Each website's cookie banner was examined against seven GDPR and ePrivacy-based criteria, using a five-point rating scale (1 = Non-Compliant, 5 = Fully Compliant). The review was performed using private browsing mode to ensure a first-time visitor experience.

4.1 Evaluation Criteria

1. **Consent Timing:** Are non-essential cookies blocked until consent is given?
2. **Reject Option:** Is a "Reject All" button available on the first layer?
3. **Equal Visibility:** Are "Accept" and "Reject" options presented with equal prominence?
4. **Granularity:** Can users choose cookie categories individually?
5. **Transparency:** Is the purpose of each cookie explained clearly?
6. **Withdrawal:** Can users easily revisit or change consent preferences?
7. **Design Neutrality:** Are there no dark patterns or manipulative visuals?



4.2 Findings

Website	Reject Option	Equal Visibility	Cookies Blocked Before Consent	Easy With-drawal	Dark Patterns	Trans-parency	Overall Rating (1–5)	Comments
zalando	✓ Yes	✓ Equal prominence	✓ Blocked	✓ Persistent icon	✓ Neutral	✓ Clear explana-tions	**5/5**	Fully compliant banner with balanced design, clear information, and active consent management options.
KLM	✓ Yes	✓ Equal	⚠ Some analytics pre-load	✓ Link in footer	✓ Neutral	✓ Clear	**4/5**	Strong implementation overall, though minor delay before cookie blocking fully applies.
bol.	⚠ Partially (via "Settings")	⊗ Accept more prominent	⚠ Some pre-loading	⊗ No visible return option	⊗ Colour bias	✓ Clear text	**2.5/5**	Uses "Manage settings" instead of "Reject all." Dark pattern risk due to highlighted "Accept all" button.
LinkedIn	⚠ Indirect ("Reject non-essential")	⊗ Accept stands out visually	⊗ Sets cookies early	⚠ Manage-able via settings	⊗ Bright accept button	✓ Some info	**2.5/5**	Borderline compliance; uses multi-step settings and visually emphasised acceptance.
NETFLIX	⊗ No direct reject	⊗ Accept dominant	⊗ Cookies set by default	⊗ No modifi-cation option	⊗ Colour contrast bias	⚠ Basic info	**1.5/5**	Primarily informational banner. Does not meet GDPR consent standards.

Findings: Only Zalando and KLM demonstrated near-full compliance. The majority still relied on designs that obscure refusal options or pre-set cookies before consent, echoing the issues highlighted in DPA enforcement actions.

4.3. Key Takeaways for Organizations

- Compliance requires both **legal accuracy** and **user-friendly design**.
- **Dark patterns** remain the most common violation.
- Regular **audits and UX testing** are crucial to ensure ongoing compliance.
- Proactive compliance can serve as a **trust and brand differentiator** in an increasingly privacy-conscious market.

5. What This Means for Organizations

European regulators now assess not just the legal text of cookie notices but their design, accessibility, and fairness. Businesses should:

- Conduct cookie audits every 6 to 12 months.
- Implement banner designs where rejection is as easy as acceptance.
- Maintain verifiable consent logs.
- Keep cookie policies current and understandable.

Cookie compliance is now a **core element of digital governance**, not a checkbox exercise.

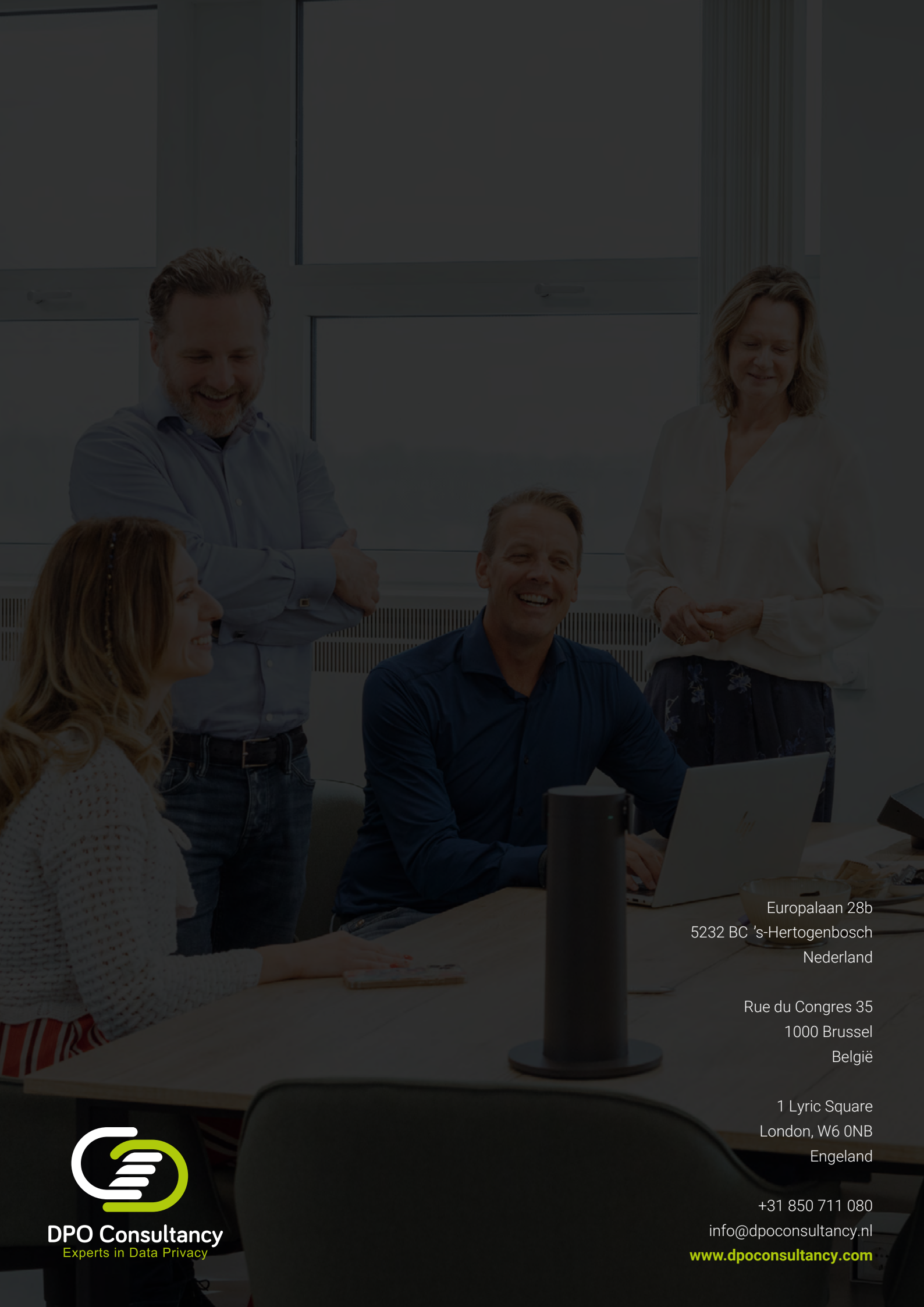
Conclusion

This analysis shows that despite widespread awareness, real-world compliance with cookie consent rules remains inconsistent. The message from regulators is clear: *"cosmetic compliance" is no longer enough.* Organizations must adopt transparent, user-friendly designs backed by sound governance.

Practical compliance checklist:

To ensure alignment with the GDPR and ePrivacy Directive, organizations should:

- Obtain consent through a clear affirmative action, no pre-ticked boxes or implied consent.
- Provide granular options for each cookie category (e.g., analytics, personalization, advertising).
- Offer equal access to users who refuse non-essential cookies, avoiding unlawful cookie walls.
- Maintain detailed consent logs to demonstrate accountability.
- Regularly review and update cookie banners and policies to reflect current practices.



DPO Consultancy
Experts in Data Privacy

Europalaan 28b
5232 BC 's-Hertogenbosch
Nederland

Rue du Congres 35
1000 Brussel
België

1 Lyric Square
London, W6 0NB
Engeland

+31 850 711 080
info@dpoconsultancy.nl
www.dpoconsultancy.com