SLAUGHTER AND MAY/

APRIL 2026

DIGITAL MARKETING COMPLIANCE - SPRING CLEANING TIPS FOR 2026

QUICK LINKS

For further information on any Data Privacy related matter, please contact the Data Privacy team or your usual Slaughter and May contact.

Digital marketing compliance has become a priority area for organisations to address in 2026. With regulatory focus intensifying across the UK, EU and US and fining powers increasing to unprecedented levels, the risk landscape has fundamentally shifted. It is not all bad news however, with commercial opportunities being presented by new legislative exemptions and evolving consent models.

In this briefing, we examine the key trends in marketing compliance for 2026 across the UK, EU and US across cookies on both websites and apps, the use of pixels and other tracking technologies, as well as dark patterns, hyper-personalisation and children's data.

WEBSITE COOKIES: THE EVOLVING RISK LANDSCAPE

Legal developments and increased fines

Fines for breach of the UK Privacy and Electronic Communications Regulations ("**PECR**") increased in February this year to be on par with UK GDPR fines (i.e. the higher of £17.5 million or 4% of annual worldwide turnover) from its previous maximum of £500,000. If the EU Digital Omnibus is implemented in its proposed form, this would also align the maximum fines for e-privacy non-compliance across the EU with the GDPR maximum. In addition, the UK''s Data (Use and Access) Act ("**DUA**") has lowered the threshold at which the Information Commissioner's Office ("**ICO**") can impose a fine.

There are also legislative changes in the US, with California for instance requiring a mandatory browser-based ad opt-out option from January 2027.

Enforcement

On the enforcement front, the French data protection authority ("CNIL") issued record-breaking cookie fines in September 2025 against Shein of €150 million and Google of €325 million (the maximum for e-privacy fines in France already being aligned with GDPR penalties). In the US, whilst federal enforcement in this area has been limited, state enforcement has increased, with the California Privacy Protection Agency fining Honda $632,500 in part due to its cookie banner design and functionality, and Healthline Media reaching a settlement with the Californian Attorney General for $1.55 million in respect of allegations that its use of online tracking technology on its health information website violated the California Consumer Privacy Act ("**CCPA**").

Civil actions

Class actions look set to continue in this area in a number of jurisdictions, with this exemplified by the combined $56 million settlement filed in California last September by Google and the developers of the Flo app in respect of the collection and use of certain data for targeted advertising. Given the continuing use of wiretapping laws as the base for many claims, the use of cookie banners is expected to continue, and increase, in the US to seek to protect against such actions.

Key practical points

Undertake a cookie audit across all websites and apps: Cookie audits are essential to understand what tracking technologies are deployed across an organisation's digital estate, with many organisations discovering "orphan" cookies that no-one was aware of. This demonstrates the importance of there being a business owner for each cookie (typically the marketing team) who is then responsible for understanding what it does and why this is necessary so that this can be fed into the compliance approach.

Review risk assessments: Historically many organisations have taken a risk-based approach to cookie compliance, but given the above changes to the legal and regulatory landscape, these risk assessments need to be reviewed to determine if previous decisions on the approach remain appropriate.

WEBSITE COOKIES: OPPORTUNITIES

New exceptions under DUA

DUA has introduced new exceptions to the e-privacy consent requirements under PECR. This includes exceptions for analytics for service improvements, user preferences and security updates. Additional exceptions are also expected to be added in future, with the UK Government undertaking a review in close co-operation with the ICO - the ICO has already said that it supports removing consent requirements for privacy-preserving ad measurement technologies. Additional exceptions would be brought in though secondary legislation (so not requiring Parliamentary time or debate) in due course.

The new exceptions are all tightly defined and so need careful assessment to determine if they apply. For example, for the statistical purposes exemption to apply, the sole purpose of the technology must be to collect data for statistical purposes about the use of that organisation’s service, the resulting information must be aggregated statistical information which cannot be used to identify people and that information can only be shared with a third party if they are using it to improve the original organisation’s website or service.

The ICO has added a new chapter to its storage and access technologies guidance to reflect these DUA changes. Importantly, the ICO is clear that the statistical exemption is about how the service is used, not about who uses it. It is not for identifying, tracking or monitoring individuals or groups who use the service, and it does not apply to online advertising.

In part as a result of these DUA changes, market practice in the UK has started to move away from "Reject all cookies" to "Reject non-essential cookies" (or equivalent wording).

Potential EU relaxations

In the EU, the Digital Omnibus proposals include removing the need for consent for cookies used for audience measurement, security maintenance or restoration. If implemented, we expect to see similar changes in cookie banners across the EU. The UK Government is closely monitoring these changes and so we can hope that there will ultimately be some consistency between the UK and EU consent exceptions.

Marketing as a legitimate interest

Whilst direct marketing was given as an example in the recitals to the GDPR of a purpose that could amount to a legitimate interest, which was then reflected in ICO guidance, there had been some concern expressed about reliance on this processing ground for marketing. This was compounded by the Dutch data protection authority’s previous stance (before it was overturned by the CJEU) that purely commercial interests, including selling data for direct marketing, could not constitute a legitimate interest. To address this, DUA has added a provision to the operative provisions reiterating the position in the recitals to put this beyond doubt.

Key practical point

Assess the ability to benefit from relaxations and consider redesigning cookie banners: Organisations should evaluate whether any of the new DUA exemptions apply to their current cookie deployments and redesign their cookie banner on UK landing pages accordingly. More broadly it will be important to monitor the progress of the Digital Omnibus so that any exemptions introduced can also be assessed.

APPS: A NEW FRONTIER

Regulator focus moves to apps

Organisations' cookie compliance efforts have historically focused on websites, but apps are rapidly moving up regulators' agendas, in part due to the sensitivity of data accessible on mobile devices, such as real-time location, contacts and photographs.

This new regulatory focus can be seen through the content of the CNIL's final recommendations on the design and development of mobile apps, released in May 2025, with the CNIL announcing it would begin enforcing against those who did not follow these recommendations.

Similarly, the ICO was clear in its online tracking strategy released last year that it would be looking at online tracking on apps, as well as internet-connected TVs and internet of things devices.

The California Attorney General has also been active, having undertaken a sweep of popular streaming apps and devices to assess compliance with the CCPA. This led to a $530,000 settlement with Sling TV in part for failing to provide an easy-to-use opt-out for consumers to stop the sale of their personal data for marketing purposes.

Interaction with app stores

An additional compliance challenge is the interplay between app/play store consent prompts and an organisation's own consent requirements. On iOS, for example, for an organisation to access the Identifier for Advertisers (**IDFA**), the device user needs to agree to the tracking consent pop up. However, the iOS pop up does not meet the standard for GDPR consent and so the user's journey also needs to include the organisation's own consent management platform pop-up. This will appear either before or after the iOS pop up, with there being pros and cons of each from a compliance and user journey perspective.

The iOS tracking consent approach is currently under review by various EU competition authorities. Organisations should monitor these developments and assess if the outcomes affect their customer consent processes on their apps.

Software development kits (**SDKs**)

SDKs are toolkits that allow developers to easily add features like in-app advertisements, analytics and personalised messaging, enabling platforms to collect user data, connect with ad networks such as Google and Meta and deliver tailored experiences. They are often touted as the "solution" to the need for cookie consent on apps, although practice has not yet fully developed into comprehensive consent models for their usage. However, organisations should be aware that they are essentially licensed trackers that organisations embed into their apps and are still caught by the EU and UK e-privacy consent rules.

Key practical point

Assess requirements across all platforms: The regulatory requirements focus on what the technology does, not which platform it operates on. The same principles that apply to websites therefore apply equally to apps. With the increased focus by regulators on app compliance, it is important that organisations reassess their approach to cookie banners on apps. There is also a commercial need in many cases to embed consent mechanisms within apps given several third parties, such as Google, require consent to have been collected in order to benefit from their advertising services.

PIXELS AND OTHER TRACKING TECHNOLOGIES

Refreshed regulator guidance

Pixels are commonly used to track engagement with marketing emails. The e-privacy rules are often referred to as the cookie consent rules, but this is just short-hand as any technology that stores or accesses information on a user's device, including pixels, will potentially require consent under the UK/EU e-privacy rules.

Emphasising the breadth of the e-privacy rules, the ICO re-branded its "cookies guidance" as guidance on "the use of storage and access technologies". This guidance expressly covers pixels as well as addressing link decoration and navigational tracking, web storage, fingerprinting techniques, and scripts and tags.

The European Data Protection Board (“**EDPB**”) guidelines also emphasise that organisations must assess all tracking technologies, not just cookies, to assess consent requirements. Likewise, last year the Norwegian data protection authority issued guidance on website and app tracking tools and recently, the CNIL published guidance on the use of tracking pixels in emails.

Enforcement

As well as issuing guidance, the Norwegian data protection authority last year took enforcement action last year against six sites for improper data sharing with tracking pixels, resulting in five reprimands and one fine.

In the US, more general laws have been relied upon to bring enforcement action in this area, with the Texas Attorney General filing lawsuits in December against five TV manufacturers under the Texas Deceptive Trade Practices Act alleging that automated content recognition technology in smart TVs was being used to unlawfully collect and monetise consumers' viewing data, tracking habits and delivering targeted ads through real-time identification of on-screen content.

Key practical point

Educate marketing teams on the breadth of the consent rules: It is not the name of the technology that matters but what it does. With this increased focus by regulators on pixels and other tracking technologies, the risk of using them in a non-compliant manner has increased considerably. Educating marketing teams to understand the breadth of the legislation (and the latest developments) is therefore key to ensuring that the compliance requirements for all relevant technologies are assessed and addressed so as to be within an organisations risk appetite.

DARK PATTERNS: BEYOND CONSENT WORDING

Regulatory focus

A dark pattern is any online choice architecture that undermines an individual's true choice. Organisations are generally familiar with the concept of not bundling consents, and more recently with the requirement for a "Reject All" button on cookie banners so that rejecting is as easy as accepting. However, there are other prevalent practices that may also constitute dark patterns. The ICO offers the following example, of a communication that is one-sided and therefore not compliant.

> **Share your search history with us for a more relevant and personalised experience**
>
> *By sharing your search history with us, we can tailor our services specifically to your needs, so you get the information you need exactly when you need it. This will also increase the relevance of the ads you see when you use our other services. If you don't share your search history with us, the information and ads you see may not be as relevant or useful to you.*

With businesses wanting to find new ways to encourage users to provide the required consent, there is a greater risk of these straying into dark pattern territory.

The ICO has expressed concern that online choice architecture can manipulate and influence users to make choices about their personal information that do not align with the user’s actual preferences. This can make it unduly difficult for users to choose freely how their data is processed and deprive them of meaningful control over their personal information. Ultimately, this can lead to more extensive processing about individuals' behaviour, preferences and attitudes and, ultimately, unwarranted intrusion such as unwanted targeted advertising or profiling. This undermining of true choice then means that any consent would not meet the required GDPR standard.

Competition authorities, including the UK Competition and Markets Authority, agree and have warned that harmful online choice architecture distorts consumer behaviour, weakens competition by shifting focus from meaningful factors to superficial tactics, and allows businesses to exploit market power to maintain or increase dominance.

EU’s proposed Digital Fairness Act

The EU Commission plans to put forward legislation to strengthen digital fairness online, with it being proposed that this Digital Fairness Act addresses dark patterns given concerns that EU regulation in this area is fragmented and there is no unified definition of what amounts to a dark pattern. 72% of respondents to the consultation last year on the high-level proposals for this regulation favoured binding rules on dark patterns, whilst digital industry stakeholders have expressed

concern that a distinction must be drawn between deceptive practices and legitimate online persuasive methods. The expectation is therefore that provisions on dark patterns will be included in the draft regulation, which is expected to be released later this year.

US approach

In the US, the Federal Trade Commission views dark patterns as covert consumer manipulation, and in September 2025 imposed a $2.5 billion settlement on Amazon for misleading Prime subscriptions. California and South Carolina have also enacted laws to address deceptive practices.

Key practical point

Data privacy teams need to review the whole customer consent journey, not just the actual consent wording: Although it is important for DP teams to review consent wording, they should also test the user consent journey using a device that does not have existing cookies set for their site. This will enable them to review what a new customer actually experiences within a broader context to check that any persuasive or nudge techniques are within the organisation's risk appetite.

HYPER PERSONALISATION

Data enrichment

Hyper-personalisation necessarily requires data enrichment, that is collecting additional information about individuals, whether from the organisation's own digital estate or elsewhere, to build up more detailed profiles. This creates challenges around transparency and whether legitimate interests can be relied upon as a lawful basis. AI is also likely to be involved as part of profiling the customers which brings in other compliance considerations. During a session at the IAPP UK Intensive this year, a poll revealed that whilst only 10% of the attendees were currently using hyper personalisation, this strategy was included as a strategy to be introduced in the marketing plans of a further 44% of attendees.

Risks of using special category / sensitive data

A significant risk arises where hyper-personalisation strays into the use of special category data. For example, a health and beauty brand might start making inferences about skin conditions to recommend particular skincare products, or about ethnicity to promote certain makeup shades.

The ICO's guidance on direct marketing makes clear that use of special category data can include drawing inferences about people's race, political opinions or health from other information held about them. Any use of special category data is very likely to require explicit consent, in addition to a lawful basis.

Whilst the vast majority of US state privacy laws provide a consumer opt-out right, those same laws typically require opt-in consent for sensitive data (broadly speaking being the equivalent to the EU / UK concept of special category) and some go further. Maryland, for example, prohibits the collection and processing of sensitive data unless strictly necessary to provide or maintain a specific product or service requested by the consumer, and completely prohibits the sale of sensitive data. In addition, the Colorado Privacy Act creates a concept of "sensitive data inferences" to which specific processing rules apply.

The FTC brought enforcement action against companies that have inferred special category data. For instance, it is currently bringing a case against Kochava Inc. for selling geolocation data from hundreds of millions of mobile devices that can be used to trace the movements of individuals to and from sensitive locations. The FTC alleges that Kochava is enabling others to identify individuals and exposing them to threats of stigma, stalking, discrimination, job loss, and even physical violence.

Practical point

Transparency, informed consent and opt-outs are key: Many consumers may be comfortable with hyper-personalisation on the basis that they will then receive more tailored recommendations. However, this will not be the case for everyone and so transparency is key so that consumers can make an informed decision. Organisations pursuing hyper-personalisation strategies must therefore be particularly vigilant about their data collection and profiling practices and ensure robust consent mechanisms are in place, and even more so if special category data is to be used.

CHILDREN'S DATA

ICO's Children's Code

In the ICO's progress update on its Children's Code Strategy in December last year, the ICO confirmed that safeguarding children's privacy is a key priority, and this was reiterated in the Information Commissioner's speech at the IAPP London Intensive in February.

The ICO's Age Appropriate Design Code (commonly referred to as the Children's Code) applies to websites which are "likely to be accessed by children", defined as anyone under 18. This threshold is broader than many organisations appreciate – even where children are not the intended target audience, if children are likely to access the website, the organisation must consider and comply with the Children's Code. This includes ensuring that, when children's data is processed, the highest privacy settings are switched on by default, including, therefore, preventing marketing.

ICO guidance highlights that where there is uncertainty as to whether services are being accessed by children, a cautious risk-based approach should be adopted, including putting in place proportionate measures to prevent or deter children from providing their personal data and taking appropriate action to ensure any age restrictions are enforced. Merely stating in website terms and conditions that the website is not intended for children and that they may only access it with parental consent is unlikely to be sufficient in most cases.

This was emphasised in the recent ICO fines against Reddit and Imgur, with a key failure in both cases being that they relied on a prohibition or restriction in their terms and conditions. The ICO determined that this was insufficient to prevent children's access to a service without other measures, such as an effective age assurance mechanism. For further information on these fines, please see our previous blog, noting that Reddit has since filed an appeal against the fine

DUA changes

DUA has codified aspects of the above. In particular, organisations that provide an online service that is likely to be used by children are explicitly required by law to take children's 'higher protection' needs into account when assessing what are appropriate technical and organisational measures. This includes considering how children can best be protected and supported when using the services, the fact they merit specific protection and that they have different needs at different ages and at different stages of development.

The ICO helpfully confirms that organisations who already conform to the Children's Code should satisfy this requirement.

EDPB stance

The EDPB chose children's data as the topic to highlight on Data Protection Day earlier this year and is currently working on guidelines for the processing of children's data.

US approach

The Children's Online Privacy Protection Act regulates the collection, use and disclosure of personal information from children under 13 and applies to websites and online services that are directed to children, or that have actual knowledge they are collecting personal data from children. It requires websites to obtain verifiable parental consent before collecting, using or disclosing personal information from children and gives parents rights to review personal information collected from a child.

The FTC takes into account numerous factors when determining whether a site is "directed to children", including subject matter, visual content, use of animated characters or child-oriented activities and incentives, music, language, and other characteristics.

Organisations must also consider state laws, with many imposing additional restrictions. For instance, Maryland has introduced an outright prohibition on the sale or processing of personal data for targeted advertising if the organisation knew, or should have known, that the consumer is under 18. Most recently, South Carolina introduced a new law in February this year requiring various privacy and other settings to be set by default for minors. This applies to organisations which exceed certain thresholds relating to revenue or sale of data and whose sites are "reasonably likely to be accessed by children" (i.e. those under 18).

Age assurance

Age assurance techniques present both an opportunity and a challenge. Whilst simply requesting someone input their age is widely recognised as ineffective, more sophisticated technologies using AI collect more data about the individual and so come with their own data protection risks that must be carefully managed.

Practical point

Risk assessments should take account of likely use and access of online services by children: It is critical not only to assess the likely use of a site or app by children, but to ensure that there is a clear document trail to evidence this. This should be coupled with appropriate measures to deter children from providing their personal data, as well as age assurance measures where appropriate. If an organisation is currently relying on a simple input of age, self-declaration or a restriction in terms and conditions, this should be reassessed given regulators' stated expectations in this area.

CONCLUDING THOUGHTS

Marketing compliance is a fast-moving area given technology advancements and the obvious focus of legislators and regulators to manage the resulting privacy risks. Organisations should also consider the potential shifts in approach that agentic AI may bring, including websites seeking to appeal to agents rather than humans (as consumers turn to agents to help with their purchases) and the challenges around consent and opt-ins when it is the agent rather a human accessing the site.

It is therefore important to regularly reassess activities across all areas of marketing against the latest legal changes and regulator guidance to ensure that activities either remain within the organisation's risk appetite, or are adjusted accordingly. Regularly documenting and refreshing data protection impact assessments will be key here, with the added benefit of providing an important documentary trail of the compliance steps that an organisation has taken if a regulator comes knocking.

CONTACT

REBECCA COUSIN
HEAD OF PRIVACY
T: +44 (0)20 7090 3049
E: rebecca.cousin@slaughterandmay.com

CINDY KNOTT
HEAD OF DATA PRIVACY KNOWLEDGE
T: +44 (0)20 7090 5168
E: cindy.knott@slaughterandmay.com