March 2025

WHY 2025 IS THE YEAR TO REFRESH YOUR MARKETING COMPLIANCE

A version of this briefing first appeared in the Privacy Laws & Business UK Report, Issue 138 (March 2025)

The value of the UK advertising market is the largest in Europe and is growing, with digital marketing spend in the UK projected to rise from £32 billion in 2024 to £44 billion in 2028 according to research by PWC. Despite its clear commercial importance, for years digital marketing was an area of regulatory uncertainty. Long promised reforms to the e-marketing rules repeatedly stalled with the iterations of the Data Protection and Digital Information Bill in the UK, and the EU's failure to progress the e-Privacy Regulation.

Equally, early regulatory efforts to examine ad-tech practices in the UK did not develop into concrete guidance, with a 2020 ICO consultation on a statutory direct marketing code of practice resulting in piecemeal guidance updates, but no final code. While the ICO routinely enforced some breaches of the marketing rules (as discussed in our previous article and blog), other areas, such as cookies, were not a focus. Instead, the ICO stated previously that: "[c]*ookie compliance will be an increasing regulatory priority for the ICO in the future*". And that time is now.

In this article, we outline how the legal landscape for digital marketing and cookies has moved on (especially since our previous article on the consequences of consumers paying with data) and the practical steps organisations should be taking to manage their digital marketing risks.

Data (Use and Access) Bill updates UK e-marketing regime

In the UK, the Data (Use and Access) Bill (**Data Bill**) will align the maximum fines for breaches of the Privacy and Electronic Communications Regulations (**PECR**) in relation to electronic direct marketing and the placing of cookies and other storage and access technologies (all of which for simplicity we will refer to as "**cookies**") with those under the UK General Data Protection Regulation (**GDPR**). They will therefore increase from the current £500,000 to the higher of £17.5 million or 4% of annual worldwide turnover. The Data Bill is currently progressing through Parliament and is expected to receive Royal Assent by the summer.

However, the Data Bill also includes some more positive changes for marketing that may mitigate some existing areas of risk and uncertainty as set out below (for further discussion of the Data Bill, see our blog).

Key marketing changes

1. Greater prominence of the acknowledgement that processing data for direct marketing purposes can amount to a legitimate interest, with text on this moving from the recitals to the main body of the GDPR.

2. Expanding the exceptions to PECR's general consent requirement for cookies to cover analytics cookies used only for web-usage monitoring with a view to service improvements, certain user preferences and security update cookies amongst others.

3. A new regulation-making power for Government to add additional cookie exceptions at a later date. This may be used in future to add a broader exception for ad and audience measurement as the Government reportedly confirmed they will continue to work with industry on this exception. The ICO has also confirmed it would support the Government to remove the consent requirements for privacy-preserving ad measurement.

4 Allowing charities to rely on the soft opt-in for direct marketing to further their charitable purposes to existing or interested supporters (an amendment that the ICO supports). However, as currently drafted, this will not cover commercial organisations looking to promote their own aims and ideals, such as ESG goals.

5 Proposals to broaden the meaning of "disproportionate effort" and add an exemption to the GDPR transparency requirements (under Article 14) to facilitate the use of open electoral register data in direct marketing to address concerns that this may be curtailed following the decision in the Experian case.

While it is uncertain whether these amendments will be taken forward, Parliamentary debate suggests that the Government will facilitate discussions between industry and the ICO on the issue, with the possibility of ICO guidance being amended instead.

EU e-Privacy reform stalled

In contrast to the UK position, new regulation on digital marketing remains stalled in Europe, with the long-promised e-Privacy Regulation formally having been withdrawn in February this year, although there is speculation that a Digital Advertising Act may ultimately be tabled in its place.

ICO focus on cookie compliance

Having succeeded in driving changes to the top 100 UK websites' cookie banners through 'call to action' letters and follow-up engagement through 2024, the ICO announced in January its extension to the UK's top 1000 websites (see our blogs for details of the initial audit and its outcome). It also announced its new online tracking strategy (**Online Strategy**) which outlines how the ICO wants to ensure individuals have meaningful choice over how they are tracked online, with online advertising being a key focus for the regulator in 2025. Notably, the ICO's accompanying statement states that it plans to affect changes through "advice, guidance and targeted enforcement", with the Online Strategy outlining the concrete steps the ICO will take in each area. Additionally, the ICO has also confirmed it is investigating data management platforms for non-compliance, following its audit of those players last year.

Cookie guidance crystallising

Regulatory focus on cookies, as well as broader changes in the tech-landscape, such as the introduction of Apple's App Tracking Transparency and Google's (now rescinded) promise to deprecate third-party cookies in Chrome, has led many organisations to seek alternatives. So called "cookie-less" solutions are often being touted as 'privacy compliant', yet in many cases privacy teams have been struggling to conclude that such solutions address the challenge of requiring consent.

To address uncertainty and intervene in this market-shift, in December the ICO published a draft updated version of its cookies guidance (**Cookies Guidance**), renamed to refer to "storage and access technologies" rather than cookies to emphasise its broad application to all tracking technologies (which we first discussed in our blog). The Cookies Guidance clarifies the application of the PECR rules to non-cookie technologies (including fingerprinting, scripts, tags and link decoration), as well as offering new guidance, as summarised in the box below.

In the EU, the European Data Protection Board's (EDPB's) report on cookie banners, released at the beginning of 2023, outlined the DPAs' shared understanding and interpretation of the issues, including around accept/reject-all buttons and cookie banner design. The EDPB has since issued finalised guidelines on the scope of Article 5(3) of the e-Privacy Directive which also confirmed that "storage and access technologies" capture emerging tracking technologies.

Guidance on consent mechanisms

Granular guidance on how consent mechanisms should be presented and operated, building on the ICO's work with the Competition and Markets Authority (CMA) on harmful online design in 2023. For example, as well as the requirement for a 'reject all' button on the top layer of the consent mechanism which is becoming market-standard, the Cookies Guidance emphasises that consent mechanisms must be equally visible on different devices (such as mobile and desktop). On the second layer of the mechanism, users must be able to toggle on/off specific purposes, with 'off' being the default, and able to revisit their preferences at any time.

Repeatedly prompting for consent

Organisations must not repeatedly prompt users for consent, particularly where they have previously declined, with the ICO giving six months as a general

guideline after which consent should be re-requested. Helpfully this period reflects that suggested by a number of EU data protection authorities (DPAs), including France, Ireland and Italy, although some others, including Spain, take a different approach. This issue of re-requesting consent has also been highlighted by privacy campaign group, NOYB, in a complaint to the French DPA against social media company BeReal for prompting users to interact with its app consent mechanism daily, unless (or until) the user consents to all tracking.

Online advertising

Consent is required for cookies used for online advertising as they do not fall within the 'necessary' exception under PECR as they are not technically required for the provision of services, even though they may be necessary to the organisation's business model.

Ad measurement

Separate consent for ad measurement is not necessary where consent for online advertising is sought.

Third-party recipients

Consent to personalised ads is only valid if third party recipients' names are shared with individuals on sign-up and where the withdrawal of consent can be communicated to those third parties. This also reflects one of the issues the Belgian DPA found with the previous version of the IAB's Transparency and Consent Framework, leading to additional requirements in the most recent version (2.2) to make it easier for users to withdraw their consent and for their preferences to be communicated along the processing chain.

Contextual advertising

The ICO sees 'contextual advertising' as a less privacy intrusive alternative to behavioural advertising.

'Take it or leave it' cookie walls

Confirmation of the ICO's position that 'take it or leave it' cookie-walls, where a user is presented with an option to consent to cookies or leave the site, are generally non-compliant as they do not result in freely given consent.

EU/UK exports cookie banners to US

Despite lacking specific laws on cookies, the US has seen a rise in class actions alleging that the collection of data via cookies, and the subsequent sale of such collected personal data, is unlawful, including under wiretapping laws. For example, Oracle agreed to settle such an action in July 2024 for $115 million and has subsequently stopped supporting its ad tech products. These actions have led to an increase in the use of cookie banners in the US as a risk mitigation technique.

EU regulators go big on fines

EU regulators are actively focusing on digital marketing, but unlike the ICO they have issued significant fines against infringers. For example, in October 2024 the Irish DPA issued a €310 million fine against LinkedIn in connection with targeted advertising (currently under appeal) and the French DPA issued a €50 million fine against Orange in December 2024 for displaying adverts in emails without valid consent.

We are also seeing EU DPAs seeking to drive cookie compliance more broadly. For example, at the end of last year the French DPA issued a suite of orders calling out misleading and non-compliant cookie banners by a number of publishers and the Dutch DPA launched a new public awareness initiative to inform individuals about cookies and encourage organisation to comply with the rules. While approaches across the bloc undoubtedly still vary, organisations should be on notice that approaches to cookie enforcement in the EU are coalescing.

ICO decides consent or pay may be ok

Most recently, the ICO has published new guidance on 'consent or pay' models (**COP Guidance**) (discussed in more detail in our blog). It provides that consent or pay models can be compliant with data protection laws if organisations can demonstrate that a user has freely consented to personal advertising taking into account the ICO's detailed guidance around:

- whether there is a power imbalance between the organisation and the individual;
- whether the fee is appropriate;
- whether the organisation is offering an equivalent product or service under the two options; and
- whether the organisation has complied with its privacy by design obligations, such as in relation to the design of consent banners.

The ICO reaffirmed that contextual advertising may be a suitable alternative to personalised advertising and could

be presented as an additional choice to users, such as where there is a power imbalance. The COP Guidance has been welcomed by industry as leaving the door open to consent or pay models, although some uncertainty remains, such as around what an appropriate fee will look like in practice.

The ICO's guidance follows on from that issued by the EDPB in the context of large online platforms in April last year. This found that such platforms will likely be unable to obtain freely given consent if payment is the only other option. Subsequently, Meta challenged the legality of this opinion (and all EDPB opinions) and the outcome of this is awaited. Nevertheless, the EDPB is preparing guidance on consent or pay models with broader application (beyond those operated by large online platforms) which is expected to be published later this year.

Overlap in the web of digital regulation

Of course, digital marketing is also subject to other laws and codes of practice, so it is important to avoid taking a siloed approach when considering e-marketing compliance, and consider for instance:

Competition laws: The CMA has indicated that competition investigations in relation to online advertising will be an area of focus for 2025 and 2026 and it was of course the European Commission that made the preliminary finding that Meta's previous consent or pay model did not comply with the EU Digital Markets Act.

Consumer protection laws: In the UK, the Digital Markets, Competition and Consumers Act 2024 (**DMCC Act**) is modernising consumer protection laws to reflect the online world as discussed in our previous article. Whilst in the EU, the new European Commission is gearing up for its upcoming 2025-2030 Consumer Agenda and the Consumer Protection Cooperation Network (coordinated by the European Commission), is already investigating several pan-European complaints and pro-actively conducting "compliance sweeps".

Advertising standards: In the UK, the Advertising Standards Authority is responsible for enforcing the advertising codes that are written by the Committee of Advertising Practice and the Broadcasting Committee of Advertising Practice. These codes therefore need to be borne in mind, particularly as they not only cover content, but also for instance the volume of marketing, with the version currently under consultation stating that "Marketers must not make persistent and unwanted marketing communications by any means [emphasis added]" rather than "by telephone, fax, mail, e-mail or other remote media". Meanwhile, in the EU, the European Commission is holding workshops on the potential benefits and implications of voluntary codes of conduct for online advertising, to contribute to transparency in the online advertising value chain, building on the existing binding provisions on advertising in the EU Digital Services Act.

Practical steps

All these developments result in a more certain position than ever before as to the legal position and regulators' expectations, and so help organisations to better ensure compliance. Organisations should now therefore review their approach to digital marketing against this by taking a variety of possible practical steps as set out below.

 **Review consent**	Organisations should review their consent banners against ICO expectations outlined in the latest Cookies Guidance, while noting details may still change following consultation. Organisations also need to review their data sharing practices with third parties, including how updates to user consent are managed and communicated with them. In addition, organisations operating or considering 'consent or pay' should evaluate their approach in light of the COP Guidance.
 **Cookie audits**	The Cookies Guidance emphasises that mechanisms must 'function as intended' so that cookies are only set when valid consent is gathered. This is a key challenge in practice – for example, a 2024 report by Privado found that 74% of the top websites in Europe fail to honour user opt-in requests. Organisations should consider commission an audit of their cookies and potentially reevaluate where ownership of cookies sits within the organisation to ensure greater oversight of technologies being placed and how well existing processes to monitor cookie functionality are working.
 **Tracking pixels**	The use of email tracking pixels has been widespread, with internal marketing teams keen to use them to track campaigns. The new Cookies Guidance directly addresses the use of email pixels in this context and the ICO's accompanying LinkedIn campaign has highlighted the issue, showing this is now squarely on the regulator's radar. Organisations should therefore consider when and how they are obtaining consent to the use of these pixels, as well as how easy it is for individuals to change their consent preference.

Consent routes	Organisations may also wish to review their approach to obtaining consent for digital direct marketing, whether explicit consent or soft opt-in, and reconsider any risk-based decisions taken in this area, in light of the heightened penalties under the Data Bill. We are seeing an increasing number of organisations shifting to rely on express consent to take advantage of the greater flexibility it provides for ongoing use of the data (e.g. amongst different members of corporate groups and wider ranges of products and services), particularly given the reduction in data availability from other sources, such as third-party cookies. In addition, organisations updating their user journeys to comply with the new rules around subscriptions introduced in the DMCC Act can use this as an opportunity to review their marketing consent journey at the same time.
Apps	To date the compliance focus has been on websites, but the ICO stated in its Online Strategy that it intends to ensure that individuals also have meaningful control over tracking for personalised advertising on apps and connected TVs. Whilst it was known that the same e-marketing rules applied to these, organisations had typically not paid the same level of attention to this. However, with the ICO having apps firmly in its sights, it is important that organisations include their apps in their compliance reviews.

Conclusion

Against this backdrop of fast-paced developments, crystalising risk and more concrete guidance, marketing compliance should be a priority area for organisations to revisit in 2025. Failure to do so could result in enforcement action or, perhaps just as significantly, missing commercial opportunities presented by the new era.

CONTACT

REBECCA COUSIN
PARTNER
T: 020 7090 4738
E: Rebecca.Cousin@slaughterandmay.com

BRYONY BACON
SENIOR KNOWLEDGE LAWYER
T: 020 7090 3512
E: Bryony.Bacon@slaughterandmay.com

ROSIE WILSON
ASSOCIATE
T: 020 7090 5483
E: Rosie.Wilson@slaughterandmay.com