Half-baked no more: Reheated rules on cookies and consent

The Data (Use and Access) Act has introduced a number of changes to the UK's ePrivacy regime. **Nicola Fulford** and **Robert Fett** of Hogan Lovells analyse the upcoming changes.

The long-awaited amendments to the UK's data protection regime received Royal Assent on 19 June 2025. These include a number of changes to the UK's implementation of the ePrivacy Directive, the Privacy and Electronic Communications Regulations 2003 (PECR). The changes which will have the widest impact, and which are the focus of this article, are

1. the loosening of the consent rules for analytics cookies,
2. the ability of charities to rely on the soft opt-in for electronic direct marketing, and
3. the alignment of the maximum penalties with those under the UK GDPR.

The Act also made some technical changes to definitions, a change in the deadline for communications providers to notify personal data breaches from 24 hours to 72 hours, and changes to the powers of the Information Commissioner's Office (ICO) (soon to become the Information Commission) to enforce PECR to more closely match powers under the UK GDPR. Lastly, it includes measures to encourage the development of sectoral codes of conduct in relation to PECR.

Analysing analytics cookies, and other goodies

The Act formalises some of the current exemptions to the cookie consent requirements under PECR which current ICO guidance had previously shoehorned into the two existing PECR exemptions – transmission of a communication, and provision of a requested service. The Act introduces several important new exemptions.

Most of the changes relate to protecting the security of the service, where there are now explicit exemptions. Consent will not be required where the access or storage is necessary to (i) ensure that the security of the terminal equipment is not adversely affected by the provision of the service requested, (ii) prevent or detect fraud in connection with the provision of the service requested, or (iii) automatically authenticate the identity of the subscriber or user.

Other exemptions now made more explicit are access or storage to detect technical faults in connection with the provision of the service requested, to maintain a record of selections made on a website or information put into a website (e.g. shopping baskets and cookie consent selections), and to enable or enhance the website appearance or functionality (e.g. language preference, screen sizes and colour themes). The definition of "website" has been clarified to include mobile applications and any other platform by means of which an information society service is provided.

Although these clarifications are much welcome, in practice such uses have historically been enabled under interpretations of the ICO's guidance. The most interesting and welcome addition to the list of exemptions is Section 5 of Schedule A1 to PECR which provides an exemption where the sole purpose of the storage or access is to enable the collection of information for statistical purposes to make improvements to the service or website. ICO guidance makes clear that this covers aggregate statistics, such as understanding user journeys through your website, and which areas of a website visitors spend most or least time on, rather than tracking individuals or for online advertising. In particular, it can be used for assessing average scroll depth (the extent to which visitors engage with the content), navigating of web pages, understanding device types, A/B testing (to compare the performance of two versions) and how users have reached the service (e.g. URL or web search). It is important to note that to comply with this exemption, such information must not be shared with any other person except for the purpose of enabling that other person to assist with making improvements to the service or website. Controllers would be wise to ensure that contracts with analytics providers contain such restrictions if relying on this exemption.

Finally, there is an exemption to assist with enabling the geographic location of a user to be ascertained where the user has indicated that they are in need of emergency assistance. This is similar to the emergency calls exception in Regulation 16 of PECR. The new exemption includes using GPS-based location information from smartphones, tablets, sat-navs or other devices. GPS location data was not previously covered by the PECR definition of location data, as it was not collected by a network or service.

A sweet treat for electronic marketing by charities

PECR previously excluded charities from capitalising on the soft opt-in rule to market to their existing individual donors and supporters electronically without consent. This clearly put charities in an unfair position compared to their commercial counterparts as they could not market their events and fundraising activities to individuals who have previously supported the charity, and who could always have opted out if they didn't want such emails.

The Act will align the rule for charities with that of commercial organisations. The change to PECR will, when it comes into force, allow charities to send direct electronic marketing without consent provided that:

1. the sole purpose of the direct marketing is to further one or more of the charity's charitable purposes;
2. the charity obtained the contact details of the recipient in the course of the recipient (i) expressing an interest in one or more of the charity's charitable

purposes; or (ii) offering or providing support to further one or more of those purposes; and
3. the recipient has been given a simple means of opting out, at the time that the details were initially collected, and at the time of each subsequent communication.

Whilst this change is welcome, it raises some strategic questions for charities about how they can best capitalise on this change.

First, the soft opt-in exemption can only be applied to recipients who had the chance to opt-out when they provided their contact details, meaning that the charity is unlikely to be able to apply the rule to its existing supporters unless the charity can develop processes which it can use to ask supporters to update their contact details or confirm that they are still correct. This would provide the charity with the opportunity to meet the conditions for the soft opt-in rule i.e. providing an opportunity for the supporter to opt-out when the contact details were first provided. However, any such solution will need to respect the rule that "sending electronic messages asking for consent to marketing is itself marketing."

Second, charities will also need to carefully navigate the timing of when they switch from seeking consent, to offering an opt-out in order to maximise the number of supporters who opt-out rather than consent. This will help maximise the number of individuals to which the charity can apply the more relaxed rules. This will probably depend on how frequently the charity sends marketing emails, how quickly it can update its systems to provide an opt-out, the timeline for the Secretary of State to bring the new rules into force, and its existing rate of consent.

Third, strictly speaking, the soft opt-in only applies when "the charity" obtained the contact details. This is unfortunate since many charities rely on third parties (e.g. online donation platforms) to receive donations. Although we are still awaiting ICO guidance on how the soft opt-in applies to charities, the language mirrors the current provisions for businesses, with the ICO stating in its current guidance "You must obtain the contact details directly from the person you want to send the marketing to. If someone else obtains the contact details, then the soft opt-in doesn't apply. For example, there is no such thing as a third-party marketing list that is 'soft opt-in compliant'". However, the ICO may take the view that, provided that the donation platform provides an opt-out mechanism on behalf of the specific charity at the time of donation, and the charity offers an opt-out in its marketing emails, then this will be sufficient. Charities may wish to discuss the available options with their donation platform partners.

Finally, whether before or after the changes to PECR, consent is not required to send direct marketing to corporate partners (i.e. an individual person at a company that, as a company, is supporting the charity in whatever way, as compared to an individual person who volunteers or donates in their own capacity). This is because PECR (whether before or after the Act) did not require consent to send electronic direct marketing to such persons.

FLAG YOUR DUAA ISSUES WITH *PL&B*

Write in with your experiences of DUAA – positive or negative – to be reported in *PL&B UK Report* either by means of an interview or anonymously. Please contact Laura Linkomies, Editor, at laura@privacylaws.com

ICO turns up the heat

Although Parliament saw fit to leave us with a few sweet treats in the form of the exemptions described above, as part of the drive to harmonise the ICO's enforcement powers under PECR, fines for breaches of PECR will increase to align with UK GDPR levels – up to £17.5m or 4% of annual worldwide turnover (whichever is greater). This far exceeds the existing maximum fine of £500,000. For this reason, organisations would be wise to bring cookie and direct marketing rules back to the top of their agenda. Also, in addition to the UK, enforcement of cookie rules has become an ever more important challenge globally, and marketing has historically been a focus for the ICO.

How much longer will the rules be baking for?

Although the Act has received Royal Assent, the rules are not yet fully baked. The Act will come into force in stages via secondary legislation put forward by the Secretary of State (see p.1). The government has indicated that the changes to PECR regarding cookies and direct marketing described above will come into force towards the end of 2025.

The ICO is due to provide updated guidance on direct marketing rules in relation to these changes. The final guidance is due for publication in winter 2025/2026. The ICO will however consult on the guidance beforehand, and therefore organisations will have the opportunity to see the draft guidance earlier, and to provide comments.

AUTHORS

Nicola Fulford is a Partner and Robert Fett is a Senior Associate at Hogan Lovells.
Emails: nicola.fulford@hoganlovells.com
robert.fett@hoganlovells.com

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

DUAA data protection aspects in force by the end of this year

Laura Linkomies reports on the steps DSIT and the ICO are taking to implement the law, and issue guidance.

The Data (Use and Access) Act (DUAA) amends, but does not replace, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR).

The government has now issued commencement regulations. While some of the provisions have already entered into force, the data protection part of the Act will be mostly brought into force approximately six

Continued on p.3

ICO fines 23andMe £2.31m – what have we learned?

Taylor Wessing's **Mike Vallance** looks at the ICO's final conclusions on the DNA testing site 23andMe data breach and at key takeaways.

The 23andMe data breach has caught the attention of the privacy community as a clear and stark reminder of the damage that can be caused by a data breach. On 17 June 2025, the UK Information Commissioner's Office (ICO) announced a revised fine of £2.31 million to be imposed on the prominent consumer genetics company[1] following a data breach that exposed sensitive genetic and health information of

Continued on p.5

Future *PL&B* Events

Maximising opportunities from the Data (Use and Access) Act 2025
1 October 2025, Host: Linklaters, London
www.privacylaws.com/UK2025

Minding the (US-European) Privacy Gap
4 November 2025, Host: Latham & Watkins, London
www.privacylaws.com/USA2025

Meet the *PL&B UK Report* Correspondents
3 December 2025, Host: Stephenson Harwood, London
www.privacylaws.com/correspondents2025

Issue 141 **SEPTEMBER 2025**

See the publisher's blog at privacylaws.com/blog2025sep

UNITED KINGDOM
report

ISSUE NO 141 **SEPTEMBER 2025**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Nicola Fulford and Robert Fett
Hogan Lovells

Mike Vallance
Taylor Wessing

Katie Hewson, Joanne Elieli and Alison Llewellyn
Stephenson Harwood

Geraldine Scali and Anna Blest
Bryan Cave Leighton Paisner LLP

Nel Anna Krzeslowska
PL&B Correspondent

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.
Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2047-1479

comment

ICO on the fast track

The new Data Use and Access Act 2025 (DUAA) may not be radically different from the Data Protection Act 2018, yet it requires the ICO to conduct a full review of its existing guidance as the majority of the data protection provisions of the Act are expected to be in force just before the end of 2025. Updates are expected in a rapid fashion – ICO consultations are already underway on legitimate interests and complaints procedures (p.4). In the summer, the regulator was also seeking views on its data transfer guidance under the UK GDPR. This is a hot potato considering for example the recent Ireland DPC fine on TikTok's transfers to China. When reading the response by law firm Hogan Lovells, I feel that many may join them in spirit in asking the ICO to adopt and promote a more streamlined approach to transfer risk assessments, especially when the data in question is not sensitive.

The regulator is now working on updating guidance for automated profiling tools to help users who use them to meet their obligations under the Online Safety Act 2023 (p.16). Data Subject Access Request (DSAR) guidance will also be looked at in light of the DUAA – although much of it is already adopted by the ICO in its day-to-day work (p.13). However, organisations may wish to review their DSAR policies now to prepare for the new data subjects' right of complaint.

The DUAA will enhance the ICO's enforcement powers (p.10), and especially under PECR, where fines for breaches increase to UK GDPR levels – up to £17.5m or 4% of annual worldwide turnover (p.8).

I look forward to our half-day conference on 1 October to hear more about work on DUAA implementation (see p.15). Before that, I am delighted to be able to attend the Global Privacy Assembly in South Korea later this month, and to report for our sister publication, *PL&B International Report*.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data (Use and Access) Act 2025, the UK GDPR, the Data Protection Act 2018, Privacy and Electronic Communications Regulations 2003 and related legislation.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Versions
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked a specified number of days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

"Fantastic documents which provide a useful snapshot of the data protection landscape all in one place that can be easily digested around your busy working day. The split between International and UK allows you to focus on areas of interest as you require."

Angela Parkin, Group Director of Data Protection, Equiniti

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 39th year. Comprehensive global news, currently on 180+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.