gunnercooke

Cookies and Targeted Advertising – UK Regulation

Targeted advertising and the use of technologies such as 'cookies' are undergoing intense scrutiny by data protection regulators and competition authorities globally. They are also in the sights of individuals who are becoming increasingly aware and concerned about the way '*ad-tec*[1]*h*' collects and uses data, and how that matches up with personal data protection rights.

'*Cookies*' and data used in targeted advertising are regulated in the UK by the 'Cookies Law', officially named the *Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)* ('PECR'). Where personal data is also processed, the *retained EU law version of the General Data Protection Regulation (EU) 2016/679* ('UK GDPR') and the *Data Protection Act 2018* ('DPA 2018') (together 'GDPR') also apply.

'Cookies' is the term most used when referencing tracking technologies[2]. However, guidance[3] from the EU and the UK broadly interpret PECR to apply to any technology or technique which stores information (or accesses stored information) on an individual's 'device[4]' including:

- web storage
- tracking pixels
- link decoration and navigational tracking
- 'Internet of Things' device reporting
- scripts and tags
- fingerprinting.
- site-based (not device-based) tracking URLs, even where a website rather than an individual is identified
- tracking which collects IP addresses originating from an individual's "terminal equipment[5]"

---

[1] The advertising technology ecosystem. See related articles for a description of how this ecosystem collects data using cookies and similar technologies, 'auctions' and sells it, and the data risks involved.

2 See related articles for a description of these tracking technologies.

3 Both PECR and UK GDPR derive from EU law. As neither the EU nor the UK have updated their respective versions of these laws, the regimes in both regions remain largely in sync. *ICO: Guidance on the use of storage and access technologies; EDPB: Guidelines 2/2023 on Technical Scope of Article 5(3) of ePrivacy Directive (16 October 2024); EDPB social media targeting guidelines*

[4] 'Devices' is interpreted widely to include computers, mobiles, wearable technology, smart TVs, and connected devices.

[5] 'Terminal equipment' is broadly interpreted to include devices and network equipment such as a router.

where this information originates from the terminal equipment of a subscriber or user

- unique identifiers sourced from personal data provided by individuals (regardless of how long the information is stored on the terminal equipment).

To use 'cookies' in compliance with PECR and GDPR, businesses must:

- Obtain user consent to the use of these devices or technologies. Non-essential cookies can only be placed after consent is given.
- Ensure the consent is "*freely given, specific, informed, and unambiguous*", both for the placement of the cookie/device and for each purpose and use of the data collected. This means that users must be given a description of the cookies (or tracking technologies or devices that have been used), including the purposes and duration. Any third-party cookies used must be clearly and specifically named. It also means that the user must consent to all the uses and purposes which will be applied to the personal data collected by the cookie. Where third party cookies are used, the data they gather and how they will use it must also be disclosed and consent obtained.
- The consent must be a clear affirmative action or statement, such as clicking a box to accept the cookies/technology.
- The user must be able to withdraw consent as easily as they gave it. Any data gathered must be deleted after content is withdrawn.
- Where personal data is collected, implement systems 'by design and default' into their tech stack or procedures to meet the obligations set out in UK GDPR and the DPA 2018.
- Where certain categories of personal data is collected, such as 'sensitive' personal data or data about children, ensure the appropriate additional measures and protections are applied.

Invalid options include:

- Refusing to allow users to access the website if they refuse to consent to non-essential cookies.
- 'Nudge behaviour', where the user is influenced to accept the cookies rather than rejecting them. For example, by emphasising "agree" over "reject" or "block".
- Consent choices where the user cannot make a choice, for example where the option to reject is on another page or under 'more information', even where the user can reject if it diverts to these pages.
- Bundling the 'reject' and 'accept' options in such a way so that the user cannot consent to each use individually is likely to be invalid, as it is not 'specific or informed'.
- Requiring users to visit other websites, for example to disable cookies, is invalid.

- 'Deemed consent' by accessing and using the website or by burying the details about the cookies in the terms and conditions, is invalid.

How we can help:

Artificial intelligence and technological advancements are changing the face of digital marketing, e-commerce and targeting advertising. Parliaments are passing new laws to protect against the risks these advancements might pose. Regulatory investigations and lawsuits by individuals are forcing stricter compliance with legal requirements and industry best practice.

We advise businesses on their evolving obligations in this dynamic environment, help them comply, and assist with defensive action.

On Ash's website, she has compiled a list of *data regulator approved* compliance templates and checklists for you to download.