

#DPPC25

ico.

Information Commissioner's Office

DPPC 20  
25

[ico.org.uk/DPPC](https://ico.org.uk/DPPC)



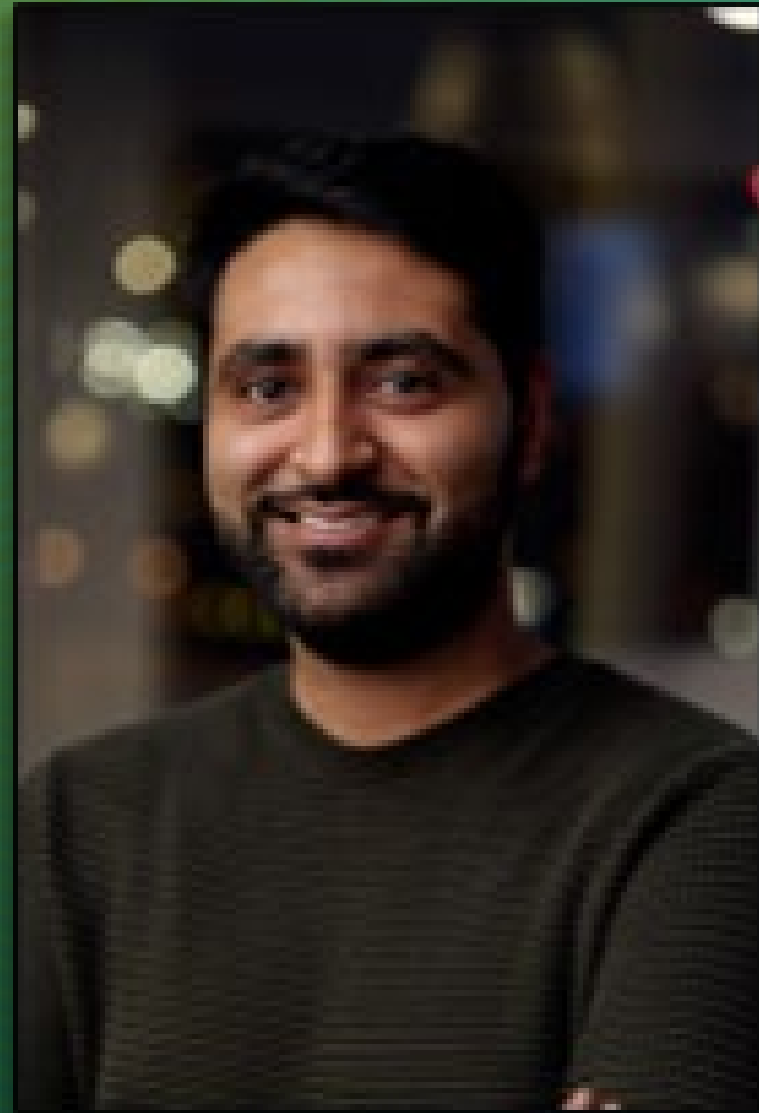
# Mind Your Banners

The ICO's approach to storage and access technologies



# Who we are

---



Adam Surtee  
Senior Policy Officer



Flo Greatrix  
Principal Policy Adviser

# Agenda

---

- Taking Control: An overview of our online tracking strategy
- Updated draft guidance on Storage and access technologies
- Post Data (Use and Access) Act 2025 changes to the Guidance (+post DUAA)
- Q&A



# Our Online Tracking Strategy



# Timeline of key ICO activity

20  
25

Guidance  
on cookies  
(V1 in  
2003)

Report on  
Adtech and  
real time  
bidding

ICO opinion  
on online  
Advertising

Google  
Privacy  
Sandbox

Cookies  
Letter  
project  
phase 1

Storage &  
access  
guidance

OT  
Strategy  
Consent or  
Pay  
guidance

2019

2021

2023

2024

2025

# Online Tracking Strategy

- We expect organisations to give people **meaningful control** over how they are tracked online.
- Our strategy, published in January 2025, set out how we will achieve a fairer online tracking ecosystem for people and business. We are doing this by:
  - Clarifying how the law applies and our expectations in guidance and other publications;
  - Engaging with industry to shape a more compliant and privacy-oriented ecosystem;
  - Scrutinising the compliance of organisations across the online tracking ecosystem; and
  - Investigating and enforcing against organisations that do not comply.



# What we've done so far

## ICO warns organisations to proactively make advertising cookies compliant after positive response to November call to action

Date **31 January 2024**

Type **Blog**



**Stephen Almond, Executive Director, Regulatory Risk**, leads the ICO's team responsible for anticipating, understanding and shaping the impacts of emerging technology and innovation on people and society.

Last November we wrote to 53 of the UK's top 100 websites, warning that they faced enforcement action if they did not make changes to advertising cookies to comply with data protection law.

We've had an overwhelmingly positive response to our call to action. Of the 53 organisations we contacted, 38 organisations have changed their cookies banners to be compliant and four have committed to reach compliance within the next month.



About the Information Commissioner's Office / Media centre / News, blogs and speeches / Our response to Google's policy change on fingerprinting

## Our response to Google's policy change on fingerprinting

Date **19 December 2024**

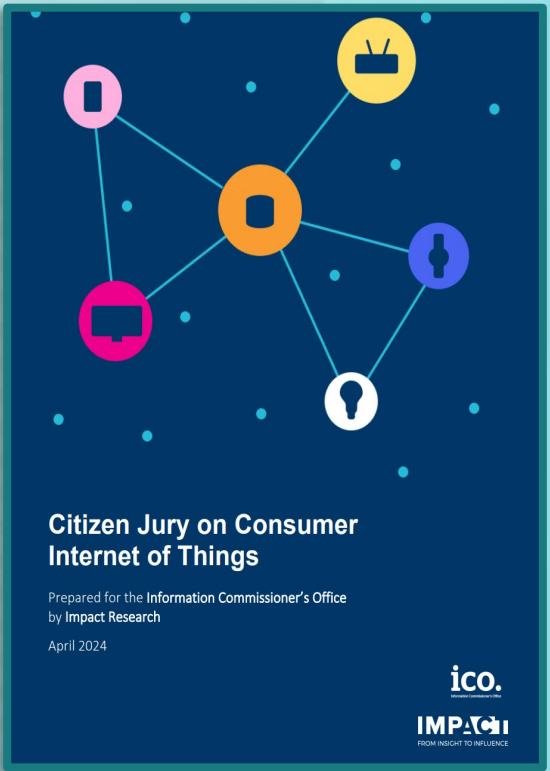
Type **Blog**



**Stephen Almond** is the ICO's executive director of regulatory risk.

Yesterday, Google announced to organisations that use its advertising products, that from 16 February 2025, it will no longer prohibit them from employing fingerprinting techniques. Our response is clear: businesses do not have free rein to use fingerprinting as they please. Like all advertising technology, it must be lawfully and transparently deployed – and if it is not, the ICO will act.

Fingerprinting involves the collection of pieces of information about a device's software or hardware, which, when combined, can uniquely identify a particular device and user.



## New guidance to help smart product manufacturers get data protection right

Date **16 June 2025**

Type **News**

We are calling on all manufacturers and developers of smart products to prioritise people's privacy with new guidance published today (16 June).

From smart speakers and fitness trackers to Wi-Fi fridges and interconnected air fryers, smart products often collect large amounts of personal information from users – including sensitive information – so manufacturers and developers must ensure their products are designed with data protection in mind.

For the first time, we have published [draft guidance](#) on Internet of Things (IoT) products and services, which will provide regulatory certainty to the industry, outlining clear expectations to comply with data protection law and use people's personal information responsibly.

Last year, we asked the public for their [views on smart products in a series of workshops](#). People shared concerns that products collect too much information, and said that they feel powerless to control how their personal information is used and shared.

These concerns are addressed in the guidance, which covers areas such as how to ask for informed consent, how to provide transparent privacy information and what tools need to be available for people to exercise their rights over their data.

Stephen Almond, Executive Director for Regulatory Risk at the ICO, said:

“People rightly have a greater expectation of privacy in their own homes so they must be able to trust that smart products are using their personal information responsibly and only in ways they would expect. This is not just about compliance – it's about building a fair and transparent online world where people are given meaningful control over how their data is used.

## Action taken against Sky Betting and Gaming for using cookies without consent

Date **17 September 2024**

Type **News**

We have [issued a reprimand to Bonne Terre Limited, trading as Sky Betting and Gaming](#), for unlawfully processing people's data through advertising cookies without their consent.

From 10 January to 3 March 2023, Sky Betting and Gaming was processing people's personal information and sharing it with advertising technology companies as soon as they accessed the SkyBet website - before they had the option to accept or reject advertising cookies. This meant their personal information could be used to target them with personalised adverts without their prior consent or knowledge.

We investigated whether Sky Betting and Gaming was deliberately misusing people's personal information to target vulnerable gamblers, following [a complaint from Clean Up Gambling](#). While no evidence of deliberate misuse was found, the regulator concluded that Sky Betting and Gaming was processing personal data through the use of certain cookies in a way that was not lawful, transparent or fair.

**ico.**  
Information Commissioner's Office

The ICO exists to empower you through information.

[Cymraeg](#)

[Home](#) [For the public](#) [For organisations](#) [Make a complaint](#) [Action we've taken](#) [About the ICO](#)

[About the Information Commissioner's Office](#) / [ICO and stakeholder consultations](#) / [ICO consultation on the draft updated guidance on storage and access technologies](#)

## ICO consultation on the draft updated guidance on storage and access technologies

Closing date **14 March 2025**

Type **ICO consultation**

Status **Open**

The Information Commissioner's Office (ICO) is consulting on this [draft updated guidance on storage and access technologies](#) (previously known as the 'detailed cookies guidance').

Your responses will help us to provide any additional further clarity required in the final guidance update.

[Respond to the consultation via SmartSurvey here.](#)



## Critics say new Google rules put profits over privacy





# What does non-compliance look like?

20  
25

1

## **Deceptive / Absent choice**

No options to opt out of processing / tracking taking place despite user objections.

2

## **Uninformed choice**

Information not presented simply or clearly with the purposes for which users are agreeing.

3

## **Undermined choice**

Where privacy information is presented clearly, we know it is not always processed in that way.

4

## **Irrevocable choice**

Even where all the above are not happening, there is no meaningful way for users to change their mind.

# 2025 plan of action

## Online Tracking Strategy

Clarifying how the law applies and our expectations

Engaging with industry to shape a more compliant and privacy-oriented ecosystem

Scrutinising compliance of organisations in online tracking

Investigating and enforcing against organisations who do not comply

Consent or pay guidance

Engagement with consent management platforms

Testing the UK's top 1000 websites

IoT action where users don't have meaningful control

Storage and access technologies guidance

Meta Sandbox

New cookie tool compliance assessment at scale

Other related enforcement

Guidance on consumer IoT

Minimum viable adtech product

Guidance for the public

Google Privacy Sandbox

Adtech certification scheme



# July 2025 strategy updates

Launched call for views on proposals to relax our enforcement approach where the use of storage and access technologies for advertising poses low privacy risks.

Published guidance on 'consent or pay' models.

Published draft guidance for consumer IoT products and Services

Engaged with IAB UK on its Data Deletion Framework

Preparing guidance to help people understand and control the use of their information online.

Committed to reviewing the cookie banners for the top 1,000 most visited sites in the UK

Launched a consultation for proposed updates to our storage and access technologies guidance following the passing of the Data (Use and Access) Act 2025.

# Updated draft guidance on storage and access technologies



# Guidance timeline

**December 2024**

ICO published updated draft guidance on storage and access technologies – the first update since 2019

**March 2025**

Closed consultation on draft updated guidance

**July 2025**

Updated draft guidance to reflect DUAA changes to Reg 6 PECR

**26 September 2025**

Consultation on DUAA chapter closes

**TBC 2026**

Final guidance on storage and access technologies published

**June 2025**

Data (Use and Access) Act becomes law

**TBC 2026**

Anticipated secondary legislation to make further changes to reg 6 PECR



# December 2024 update

- In December we published a significant update to the previous detailed cookies guidance, pre-DUAA.
- It provided added clarity on our expectations for using other storage and access technologies as well as cookies.
- It was written using 'must', 'should', or 'could' language to provide regulatory clarity.
- The guidance reflects recent case law and our positions on key topics, including on our expectations for online advertising.
- We ran a 12-week consultation on this draft guidance.



# Reg 6 PECR: not just about cookies!

---

PECR applies to any technology that stores information, or access information stored, on someone's device.

This includes but is not limited to cookies. We've updated the guidance to better reflect other common technologies and techniques, in particular:

- tracking pixels;
- link decoration and navigational tracking;
- web storage;
- fingerprinting techniques; and
- scripts and tags



# Key changes to the guidance

---

We've added **more detail on the strictly necessary exemption**. This includes a list of activities likely to meet the exemption:

- ✓ ensuring the security of terminal equipment;
- ✓ preventing or detecting fraud;
- ✓ preventing or detecting technical faults;
- ✓ authenticating the subscriber or user; and
- ✓ recording information or selections the user makes on an online service.

We have added new, detailed examples of when the exemption is likely to apply or not apply which may be helpful for dealing with customer queries.



# Key changes to the guidance 2

- We've added more on the **duration of storage and access technologies**, and our views on **re-requesting consent**. For example, the guidance says:

You **should not** repeatedly ask or prompt people to specify their preferences as a matter of course. This is particularly the case when someone has refused consent. It is unfair to repeatedly request their consent just because you want them to respond differently.

We recommend that fresh consent is requested every six months. If a user has declined consent, you **should** only choose to seek their consent again after six months.



# Key changes to the guidance 3

- We have a **new sub-section devoted to online advertising:**

[For organisations](#) / [Direct marketing and privacy and electronic communications](#) / [Guidance on the use of storage and access technologies](#) / [How do the rules apply to online advertising?](#)

## How do the rules apply to online advertising?

Search

[Guidance on the use of storage and access technologies](#)

What's new

[About this guidance](#)

[What are storage and access technologies?](#)

[What are the rules?](#)

[How do the PECR rules relate to the UK GDPR?](#)

[How do we comply with the rules?](#)

[How do we manage consent in practice?](#)

[How do the rules apply to online advertising?](#)

### At a glance

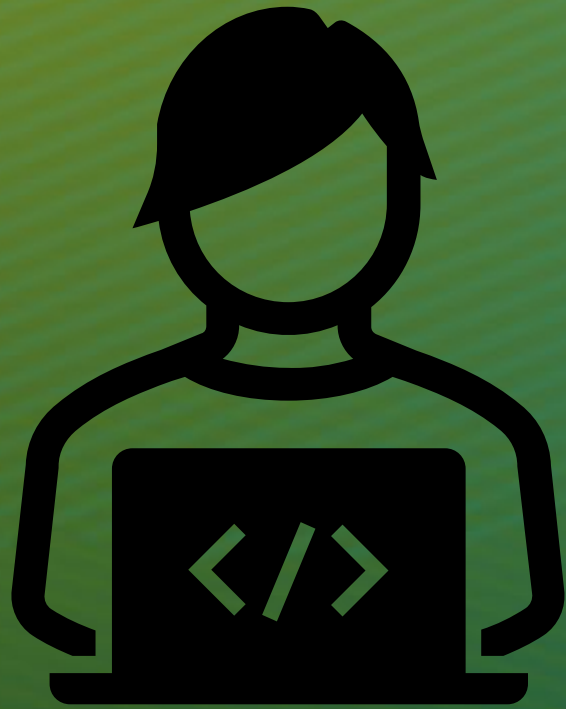
- The use of storage and access technologies for online advertising purposes requires consent. This applies both in the context of the technical processes involved in ad selection and delivery, as well as any associated tracking and profiling.
- Ad measurement does not require a **separate** consent, as the collection of information for measuring the effectiveness of campaigns is intrinsically linked to the purpose of online advertising.
- In principle, contextual advertising more readily enables you to comply both with the PECR requirements as well as your UK GDPR obligations than other types of targeted advertising.

### In detail

- [Do we need consent for online advertising?](#)
- [Does ad measurement require consent?](#)
- [What types of online advertising can we use?](#)
- [Can we use 'cookie walls' or 'consent or pay' models?](#)



# Examples of storage and access technologies - pixels



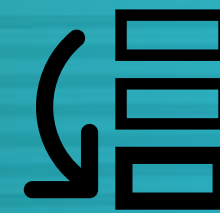
User visits site x with a pixel installed



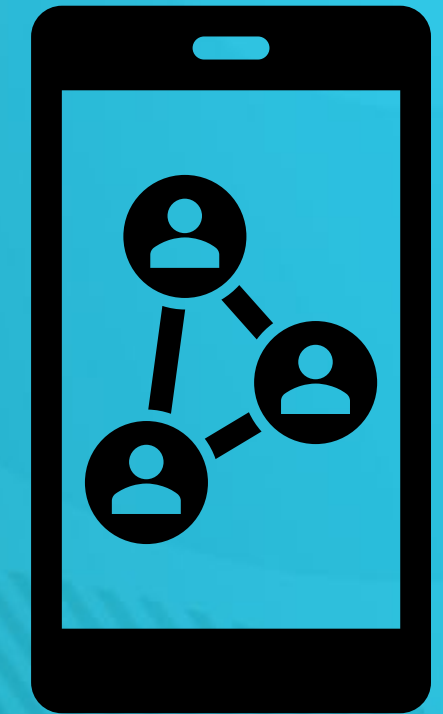
Pixel loads and collects data (IP address, geolocation, URL info etc) about user's activity.



Pixel transmits data to a social media platform



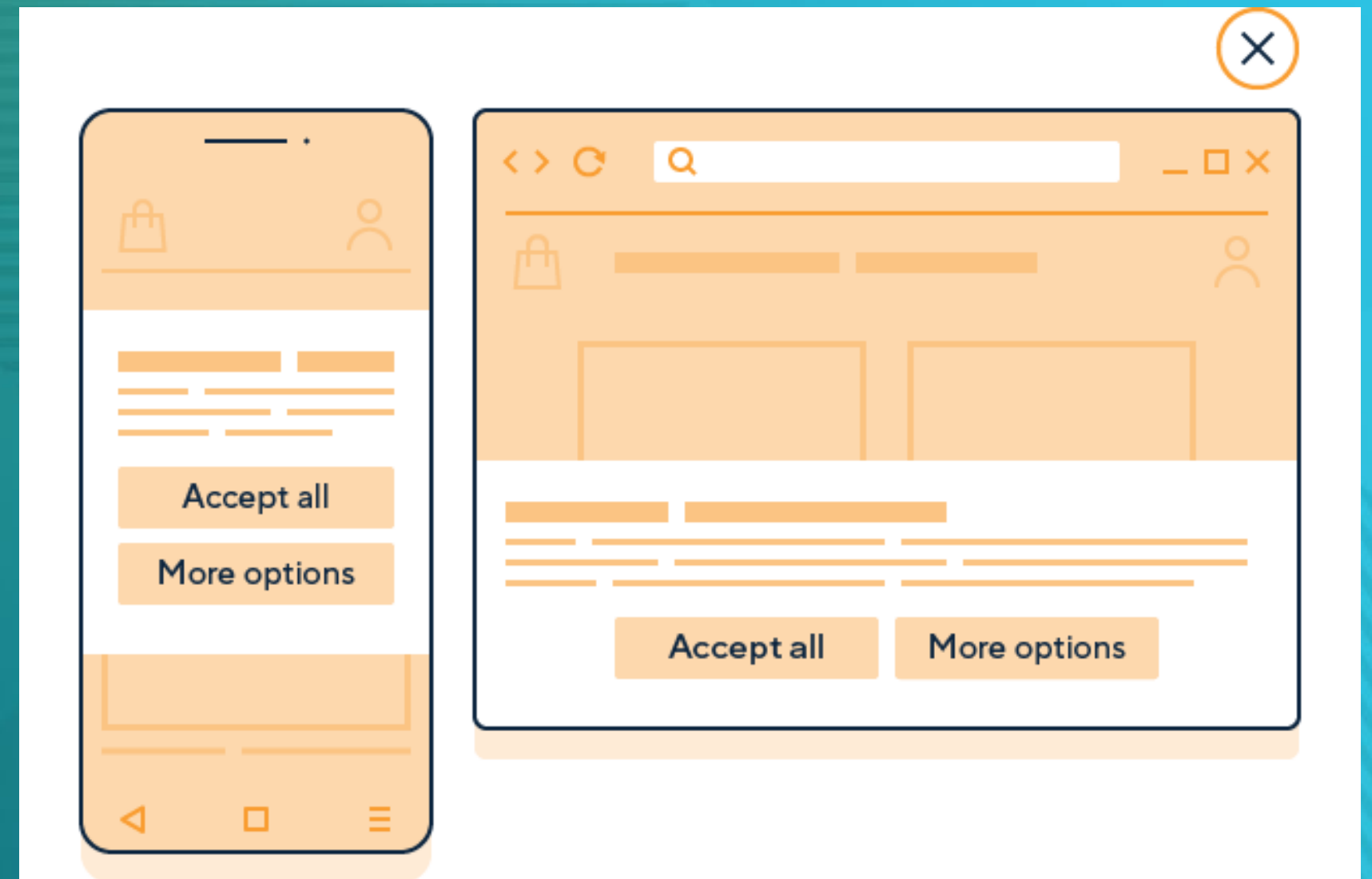
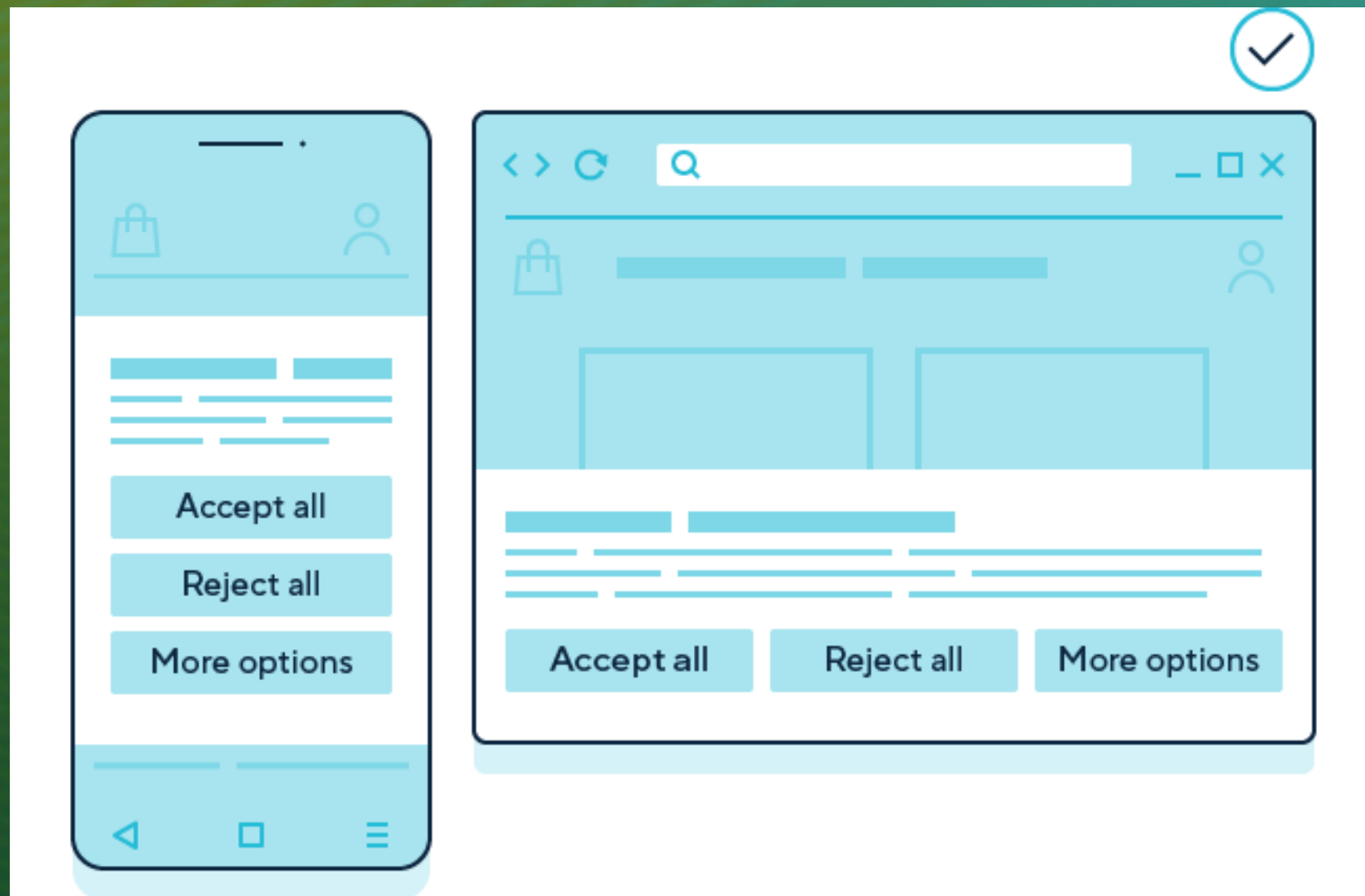
The social media platform matches pixel with data about existing users on the platform.



User leaves the site and visits their social media platform.  
They receive targeted ads from site x on their social media platform.

# Our expectations for consent mechanisms

It **must** be as easy for people to withdraw consent as it is for them to give it.

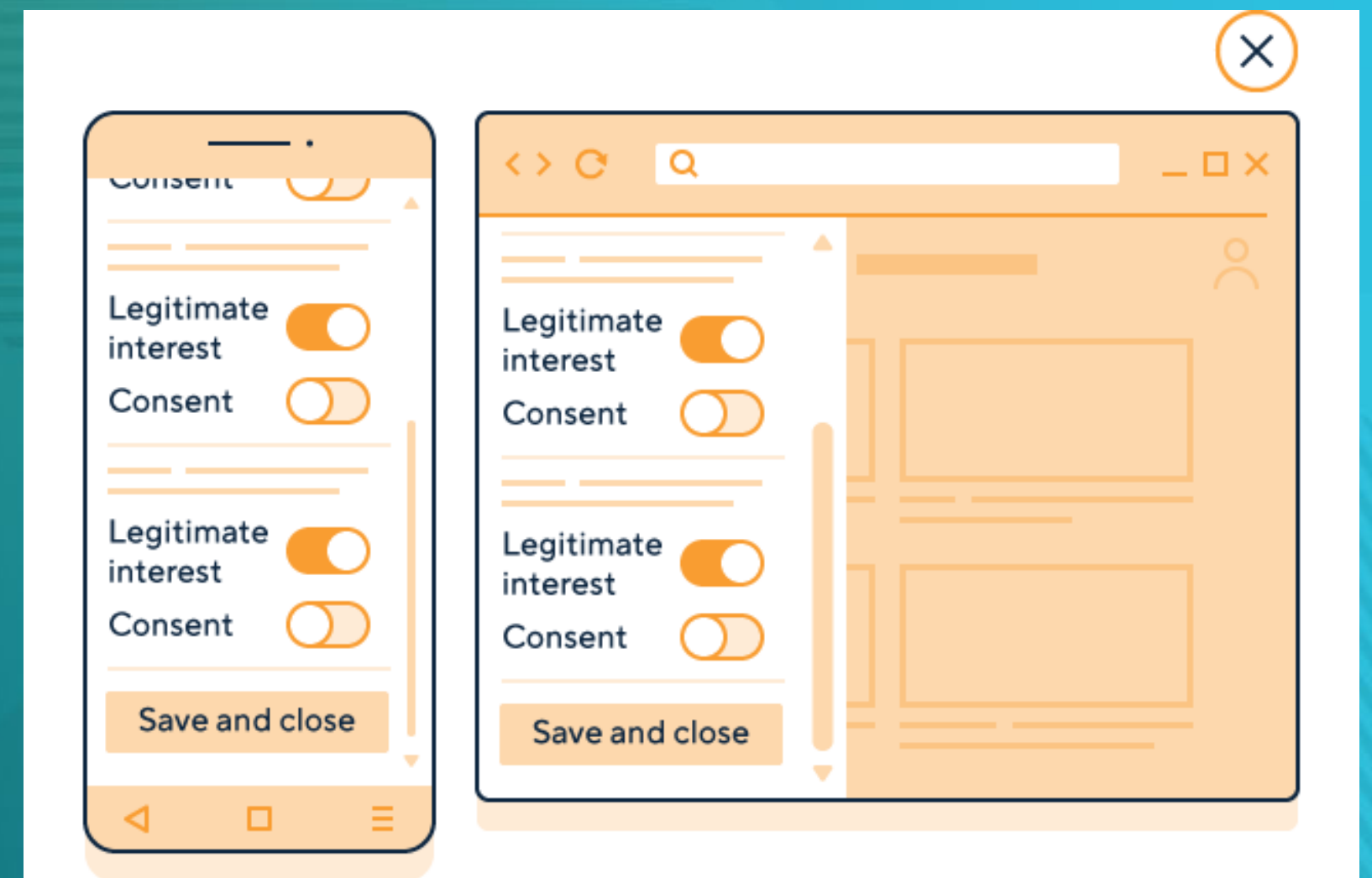




# Our expectations for consent mechanisms 2

“Our consent mechanism informs users about how they can revisit their preferences”

“Our consent mechanism does not incorrectly use legitimate interests as a lawful basis”





# Our expectations for consent

---

## **Settings-based consent?**

- Some storage and access technologies (like preference cookies or 'user interface' cookies) are deployed when a user makes a choice over a site's settings. For example, sites might remember which language to display the page in or the font size.
- It is likely the use of these technologies would fall under the appearance exception.

## **Feature-led consent?**

- A user may interact with a feature on your site, such as an embedded feature or a chatbot.
- If the user is well informed that this might happen, it can be considered strictly necessary to provide the service
- However, if a feature (like an embedded video) is using storage and access technologies for purposes that go beyond those that are necessary, this would not be covered by the exception.



# Data (Use and Access) Act 2025



## Data (Use and Access) Act 2025

CHAPTER 18

---

Explanatory Notes have been produced to assist in the understanding of this Act and are available separately

---



# Data (Use and Access) Act 2025 changes

---

- The DUAA made changes that relax consent rules to make it easier for organisations to use storage and access technologies for:
  - statistical purposes;
  - adapting the appearance or function of the website to the user's preferences or device; or
  - emergency assistance.
- We updated our draft updated guidance again earlier this month to reflect changes to how regulation 6 is now written following the DUAA. It covers the new enforcement regime for PECR.



# Statistical purposes exception

---

The statistical purposes exception means you don't have to get consent for storing or accessing information on a device if:

*“the sole purpose of the storage or access is to enable the person –*

- (i) to collect information for statistical purposes about how the service is used with a view to making improvements to the service, or*
- (ii) to collect information for statistical purposes about how a website by means of which the service is provided is used with a view to making improvements to the website.”*



# Statistical purposes exception 2

---

- This exception is about creating aggregate statistical information about visitors to your service and how you use this information for the purpose of improving it.
- It is essentially for analytics purposes. However, it's not a broad exception that covers all types of analytics technologies or ways you can use them.
- It is about how your service is used, not about who uses it.
- To use the exception, you **must** ensure your analytics involve statistical information. For example, things like:
  - How many people access your service;
  - What they access; and
  - How long they access it for.



# Examples: Statistical purposes exception

Activity – when using aggregate statistical information	Likely to meet exception?
Total visits to your website	✓
User interactions with pages on your website	✓
Information to understand how your users access your service (eg device types and browser or operating system versions)	✓
How your users reached your service. (eg via an email campaign, search results)	✓
Geolocation information of website users (eg at city or region level) that does not allow people to be identified	✓
Using web analytics tools to monitor or track people eg: logs of individual visitors to your website and the actions they took (if not obtained for the purposes of security)	✗
Online advertising purposes	✗

# Website appearance exception

---

The 'appearance' exception applies when the sole purpose of the storage and access is so you can either:

- adapt the way your service appears or functions in line with the subscriber's or user's preference; or
- otherwise enhance the appearance or functionality of the website when displayed on, or accessed by, the subscriber's or user's device.

This exception is **not** about adapting the content to display to a user on your service based on known or inferred interests or behaviours about them. For example, using their profile or previous browsing history to decide what content to promote at the top of the webpage, or to choose which advert to serve.



# Examples: appearance exception

Activity	Likely to meet the exception?
Remembering the language the subscriber or user selects (eg on a multilingual website).	✓
The use of an external font library to display your chosen font on the service.	✓
Detecting preferences indicated on the subscriber's or user's operating system, such as themes and colour schemes, and displaying the service using a similar theme, if available. For example, a user might turn on 'dark mode' in their mobile device settings.	✓
Changing the content you display to a user on your service based on known or inferred interests or behaviours about them.	x
Online advertising purposes	x

# Any questions?







# Keep in touch

Subscribe to our e-newsletter at  
[ico.org.uk](https://ico.org.uk) or find us on...



#DPPC25

[ico.org.uk/DPPC](https://ico.org.uk/DPPC)