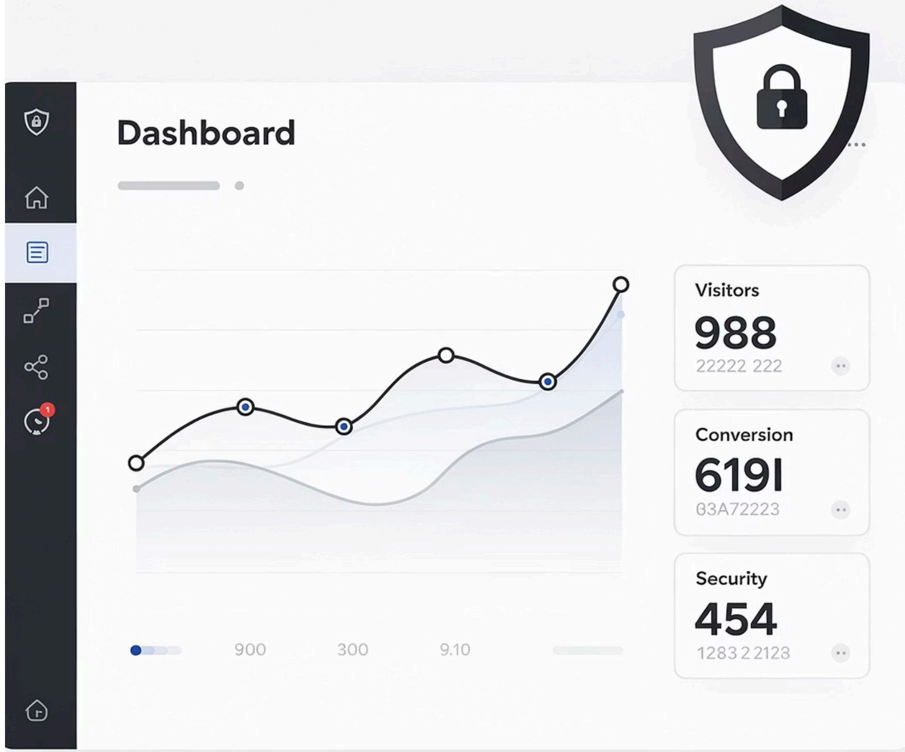
GDPR & GA4: A Comprehensive Compliance Guide

Everything website owners need to know about Google Analytics 4, UK GDPR, PECR, and consent requirements

Metric Owl™

BASED ON ICO GUIDANCE 2025-2026



⚠ URGENT

Why This Matters Now

134

Websites with compliance concerns out of the top 200 UK sites assessed

In January 2025, the ICO announced it had assessed the top 200 UK websites for cookie compliance and found significant concerns with 134 of them. It has now committed to reviewing the top 1,000 UK websites.

> The ICO's Executive Director of Regulatory Risk stated that uncontrolled tracking intrudes on the most private parts of people's lives and can lead to real harm — including vulnerable individuals being targeted based on their browsing history.

What Is GA4 and What Data Does It Collect?

Cookie Identifiers

_ga, _gid, _gat cookies that track users across sessions

IP Addresses

Used for geolocation before being processed

Device & Browser Info

Technical specifications and system details

User Behaviour

Page views, clicks, scroll depth, conversions

Demographics

Age, gender, and interest estimates

User ID

If enabled — requires explicit consent

Google's own terms confirm GA4 collects personal data including cookie IDs and IP addresses. This places it squarely within the scope of UK GDPR and PECR.

The Legal Framework

Three regulations you need to understand:

UK GDPR

Processing of personal data; requires a lawful basis for all processing

Applies to: All organisations processing personal data of UK residents

PECR

Use of cookies and tracking technologies; applies to personal AND anonymous data

Applies to: Anyone operating a website accessed by UK users

Data (Use and Access) Act 2025

Updates to PECR came into force June 2025; ICO guidance under review

Applies to: All UK website operators

PECR takes precedence over UK GDPR where both apply. If you need consent under PECR, consent is also required as your lawful basis under UK GDPR — you cannot substitute legitimate interests.

What Counts as Consent?

Under UK GDPR and PECR, valid consent must meet five requirements:

Freely given

Users must have genuine choice with no detriment for refusing

Specific

Separate consent for analytics, advertising, personalisation

Informed

Users must understand what they're agreeing to

Unambiguous

Requires clear positive action (tick, click)

Withdrawable

Users can change their mind as easily as they gave consent

What Doesn't Count

- Pre-ticked boxes
- Implied consent (e.g. "by continuing to browse...")
- Bundled consent with no granular options
- Cookie walls that block site access

CRITICAL TIMING

When Must Consent Be Obtained?

This is one of the most commonly misunderstood compliance issues. The timing is non-negotiable.

GA4 Must NOT Fire

- **Before** the user has interacted with the consent banner
- **While** the consent banner is being displayed
- **After** the user has rejected or declined consent
- **If** the user ignores the banner and navigates away

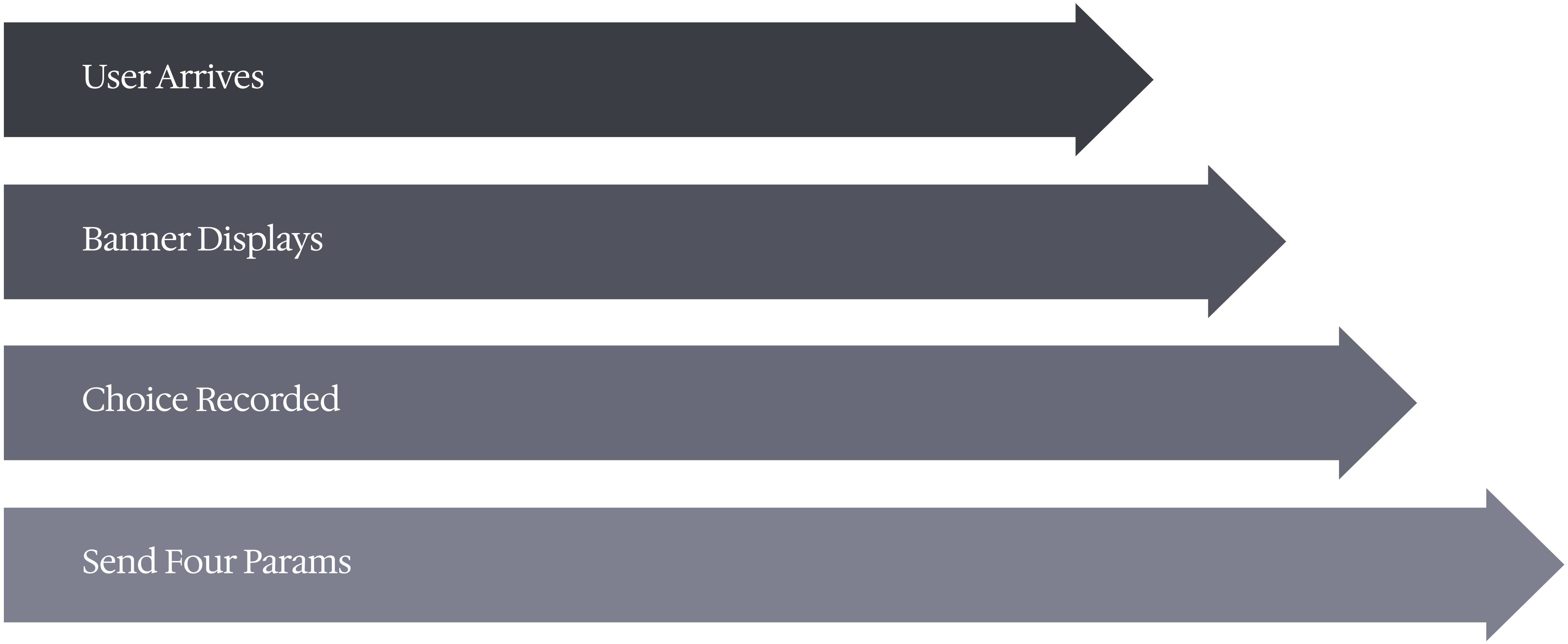
GA4 May Only Fire

After the user has **actively and clearly** indicated consent through a positive action

In September 2024, the ICO issued a formal reprimand to Sky Betting and Gaming for setting cookies before consent had been given. This is a real enforcement precedent — not theoretical risk.

Advanced Consent Mode v2 — What It Is

Google's 'answer' to the consent challenge became mandatory in March 2024 for websites using Google's services in the UK, EU, and EEA.



User Arrives

Banner Displays

Choice Recorded

Send Four Params

When users deny consent, ACM v2 sends minimal "cookieless pings" to Google — containing consent state signals, general region data, and basic session information.

Basic Mode

Tags only fire after consent is granted (fully compliant if properly configured)

Advanced Mode

Tags load but operate in a restricted state, still sending pings before/without consent

Advanced Consent Mode — The Compliance Problem

Direct guidance obtained from the ICO in April 2025 makes clear that Advanced Consent Mode does **not** provide a lawful basis for tracking users who have not consented.

Even without traditional cookies, **explicit consent is required** for any tracking or storage access technologies

PECR applies to tracking technologies processing both personal and anonymous data

Transmitting any signals — even cookieless pings — before or after rejection, without consent, is **not permitted**

Consent must be obtained **before** any such transmission begins

GA4 and the Data Controller Relationship

When you use GA4, you are the **data controller**. Google acts as a **data processor** on your behalf.

Under UK GDPR Article 28, you must have a Data Processing Agreement (DPA) in place with Google before using GA4.

How to Accept Google's DPA

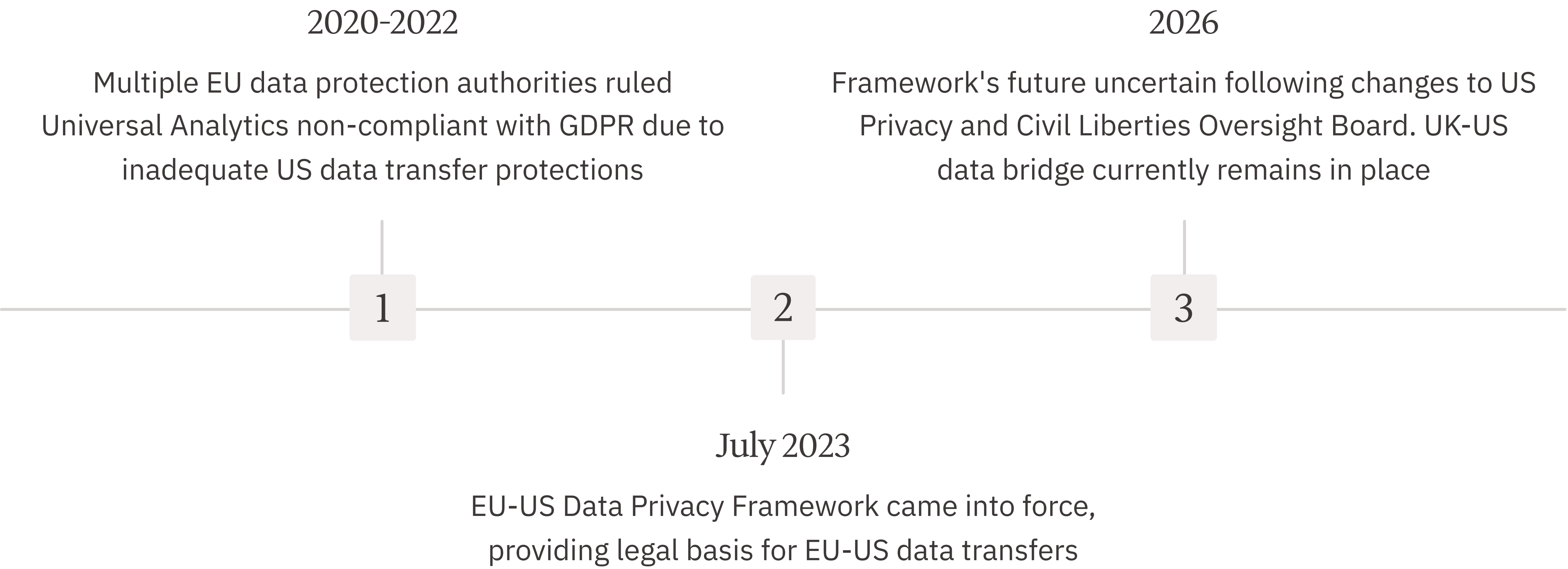
1. Log into your Google Analytics account
2. Go to Admin → Account Settings
3. Accept the Google Ads Data Processing Terms

Accepting the DPA does not make your implementation compliant — it is a necessary but not sufficient step.

INTERNATIONAL

International Data Transfers

GA4 transfers data to Google's servers, many of which are in the United States. This is a significant compliance consideration.



1

2020-2022

Multiple EU data protection authorities ruled Universal Analytics non-compliant with GDPR due to inadequate US data transfer protections

2

July 2023

EU-US Data Privacy Framework came into force, providing legal basis for EU-US data transfers

3

2026

Framework's future uncertain following changes to US Privacy and Civil Liberties Oversight Board. UK-US data bridge currently remains in place

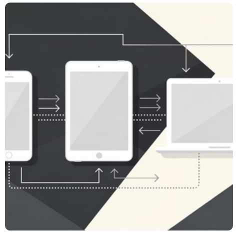
Practical steps: Accept Google's DPA, ensure your privacy policy discloses international data transfers, and monitor ICO guidance on adequacy decisions.

GA4 Privacy Settings You Must Configure

Correct GA4 configuration is essential. Key settings to review:

Data Retention

Set the minimum retention period necessary — default is 2 months, maximum 14 months. Under UK GDPR's data minimisation principle, do not retain longer than needed.



Google Signals

Disabled by default — keep it off unless you have explicit user consent. Google Signals enables cross-device tracking and demographic reporting.

User ID

Only enable if users are logged in and have given explicit consent. User ID can link data across sessions and devices.

Data Sharing Settings

Review and restrict data sharing with other Google products unless you have clear consent and business need.

Consent Management Platform (CMP) Requirements

A Consent Management Platform is essential for compliant GA4 use. A basic cookie banner is not sufficient.

Block Before Consent

Block GA4 and all non-essential scripts before any consent signal

Support GCM v2

Transmit the four consent parameters in real-time

Clear Reject Option

Provide "Reject All" as easy to use as "Accept All"

Granular Consent

Separate categories for analytics and advertising

Consent Log

Maintain audit trails for regulatory investigations

Google-Certified

IAB TCF v2.2 compliance for advertising services

Your Privacy Policy and Cookie Policy

You are legally required to inform users about your use of GA4 through clear documentation.

Privacy Policy Must Include

- That you use Google Analytics 4 and what data it collects
- The lawful basis for processing (consent)
- How long data is retained
- International data transfer details and destination countries
- Whether Google Signals or advertising features are enabled
- How users can withdraw consent
- How to exercise data subject rights (access, erasure, portability)

Cookie Policy Must Include

- All cookies GA4 places (_ga, _gid, _gat etc.)
- Purpose of each cookie
- Duration of each cookie
- Google identified as third party recipient

ICO guidance confirms you cannot rely on a privacy policy that is hard to find or difficult to understand as a valid means of obtaining consent.

Data Subject Rights and GA4

Under UK GDPR, users have rights over their data. As data controller, you are responsible for facilitating these rights even for data processed via GA4.

Right of Access (SAR)

Users can request what data you hold. Use GA4 User Explorer report to locate user data.

Right to Erasure

Users can request deletion. GA4 provides data deletion request tool in Admin → Data Deletion.

Right to Object

Users must be able to opt out at any time. Your CMP must make this simple.

Right to Data Portability

Users can request their data in machine-readable format.

Response timeframe: You have one calendar month to respond to data subject requests.

⚠ COMMON FAILURES

What the ICO Is Finding in Practice

Based on ICO enforcement activity and website reviews, the most common failures are:

- Firing GA4 during the pre-consent window before the banner has been interacted with
- Not including a "Reject All" button, or making it harder to find than "Accept All"
- Using pre-ticked boxes or sliders defaulted to "on"
- Relying on Advanced Consent Mode v2 without proper CMP configuration
- Treating analytics cookies as "strictly necessary" to avoid needing consent
- Not maintaining consent logs — leaving organisations unable to demonstrate compliance
- Misclassifying marketing or analytics cookies as functional cookies
- No Data Processing Agreement in place with Google
- Privacy policy does not mention GA4 or international data transfers

Compliant vs Non-Compliant Setup

Scenario	Compliant?
GA4 fires on page load before banner shown	❌ No
GA4 fires while banner is displayed	❌ No
GA4 fires after user clicks "Reject All"	❌ No
GA4 fires after user closes banner without choosing	❌ No
GA4 fires after user clicks "Accept Analytics"	✅ Yes
ACM v2 Advanced mode with no CMP — pings sent on rejection	❌ No
ACM v2 Basic mode — tags only load post-consent	✅ Yes (if properly configured)
Google Signals enabled without consent	❌ No
User ID enabled for logged-in users with explicit consent	✅ Yes
No DPA accepted with Google	❌ No

Step-by-Step Compliance Checklist

01

Legal & Documentation

- Accept Google's Data Processing Terms in GA4 Admin
- Update Privacy Policy to disclose GA4, data transfers, and lawful basis
- Create or update Cookie Policy listing all GA4 cookies
- Document your lawful basis as consent

02

Technical Configuration

- Implement compliant CMP supporting Google Consent Mode v2
- Set GA4 default consent state to DENIED in your CMP
- Ensure GA4 is fully blocked before any consent signal
- Configure granular consent categories
- Add clearly visible "Reject All" option
- Enable consent logging and audit trails
- Review and disable Google Signals unless consented
- Set data retention to minimum period required
- Disable User ID unless explicitly consented to

03

Testing

- Use browser developer tools to verify no GA4 requests fire pre-consent
- Test the reject flow — confirm GA4 is blocked after rejection
- Test the withdrawal flow — confirm GA4 stops if consent withdrawn

The Risk of Getting It Wrong

Enforcement is escalating across multiple fronts:

£17.5M

UK GDPR Maximum Fine

Or 4% of global annual turnover, whichever is higher

£500K

PECR Maximum Fine

Under review for increase

60%

Cookie Complaints

Of complaints to ICO in 2024 were about inability to reject tracking

Additional enforcement actions: ICO reprimands (publicly issued and reputationally damaging), enforcement notices requiring practice changes, and third-party collective redress actions approved in late 2024.

> The ICO is no longer taking a light-touch approach. In 2024, privacy rights group NOYB was approved to bring collective redress actions in the UK on behalf of data subjects.

☆ KEY TAKEAWAYS

Five Things to Remember

1 **GA4 is not automatically compliant**

Configuration, consent, and documentation are all your responsibility as data controller

2 **Consent must come first**

GA4 must not fire before, during, or after a user rejects the consent banner

3 **Advanced Consent Mode is not a compliance workaround**

It requires proper CMP integration and does not replace the need for consent

4 **PECR applies to all tracking technologies**

Including those processing anonymous data — and takes precedence over UK GDPR

5 **The ICO is actively enforcing**

The top 1,000 UK websites are under review; any organisation with a website could be next

This guide is for informational purposes only and does not constitute legal advice. Organisations should seek qualified legal counsel for advice specific to their circumstances.

REFERENCES

Sources & Further Reading

Official ICO Guidance

- ICO direct guidance obtained via formal enquiry, April 2025
- ICO Cookies and Similar Technologies guidance: **ico.org.uk/pecr/cookies**
- ICO Guidance on Storage and Access Technologies (updated post Data (Use and Access) Act 2025)
- ICO Consent or Pay guidance, 2025
- PECR overview: **ico.org.uk/pecr**
- UK GDPR Guide: **ico.org.uk/uk-gdpr**

Google & Industry Resources

- Google Consent Mode v2 documentation: **support.google.com**
- Google Ads Data Processing Terms: **support.google.com/analytics**
- Arnold & Porter: ICO Cookies Compliance Review announcement, January 2025

Disclaimer

This guide is for informational purposes only and does not constitute legal advice. Organisations should seek qualified legal counsel for advice specific to their circumstances.

Prepared incorporating direct ICO guidance, April 2025, and current regulatory practice as of early 2026.

REFERENCES

Sources & Further Reading

Official ICO Guidance

- ICO direct guidance obtained via formal enquiry, April 2025
- ICO Cookies and Similar Technologies guidance: **ico.org.uk/pecr/cookies**
- ICO Guidance on Storage and Access Technologies (updated post Data (Use and Access) Act 2025)
- ICO Consent or Pay guidance, 2025
- PECR overview: **ico.org.uk/pecr**
- UK GDPR Guide: **ico.org.uk/uk-gdpr**

Google & Industry Resources

- Google Consent Mode v2 documentation: **support.google.com**
- Google Ads Data Processing Terms: **support.google.com/analytics**
- Arnold & Porter: ICO Cookies Compliance Review announcement, January 2025

Disclaimer

This guide is for informational purposes only and does not constitute legal advice. Organisations should seek qualified legal counsel for advice specific to their circumstances.

Prepared incorporating direct ICO guidance, April 2025, and current regulatory practice as of early 2026.