ICO advice to government on online advertising exception(s) to regulation 6 consent requirements – Summary of responses to call for views

Introduction

In July 2025 we launched a call for views on our approach to the Privacy and Electronic Communications Regulations (PECR) regulation 6 consent requirements (hereafter 'regulation 6') for online advertising purposes. This call for views ran until 7 September 2025.

We received 76 responses: 59 through our Citizen Space platform and 17 by email. Thank you to everyone who provided a response for their time taken to comment and share their views.

This summary outlines the key themes from the responses we received. It sets out how we have considered these and used them to inform our advice to government on a viable approach to creating online advertising exception(s) to regulation 6.

We have included named quotes where respondents indicated that they were happy for us to publish their responses.

Our advice[1] has been developed in accordance with the ICO policy methodology.[2] The methodology draws closely from best practice

[1] ICO, 2026. ICO report for DSIT: Advice on a viable approach to creating online advertising exception(s) to regulation 6 PECR. Available at: https://ico.org.uk/media2/yefdqvk4/20260505-report-for-dsit-on-changes-to-regulation-6-pecr-for-online-advertising.pdf

[2] The ICO's policy methodology

principles and aligns with government guidance, including the HM Treasury Green Book.[3] The process has involved:

- understanding the project rationale and objectives;
- carrying out research and analysis, including running this public call for views; and
- developing and appraising a series of policy options.

We sought views on:

1. Our regulatory posture towards regulation 6 consent requirements.

2. What features are the minimum requirements for a commercially viable advertising model, looking at:

- targeting (ie how an advert is targeted towards a user or group of users);
- frequency capping;
- measurement and attribution;
- brand safety, brand suitability and brand compliance;
- ad fraud prevention and detection; and
- ad delivery and billing.

3. What impacts, positive and negative, would be anticipated if regulation 6 consent was not required for advertising capabilities deemed to be low risk. Respondents were also asked to identify challenges and risks around this proposed approach and any safeguards and innovations that could help to overcome these.

Advertising capabilities

Targeting

We have categorised respondent's views on targeting into four approaches:

- Contextual targeting – based on the content the user is accessing.
- Demographic and interest-based targeting – segmenting audiences by traits (eg their age or gender) or interests and activities.
- Geolocation targeting – based on IP address or GPS information.
- Behavioural targeting – including using browsing behaviour and purchase histories.

[3] The Green Book and accompanying guidance - GOV.UK

Some respondents have used different terminology to describe different targeting approaches. Respondents have different views on what information targeting approaches like 'contextual' and 'behavioural' include. For consistency and clarity, we've used our own definitions of these targeting methods, described in our guidance on the use of storage and access technologies,[4] to group points raised by respondents.

Contextual targeting

Contextual targeting was the most frequently referenced method by respondents commenting on this capability. Many respondents interpret contextual targeting to be about the content of the page, site or app the user is viewing. For this reason, it was commonly referenced as a more privacy-preserving technique. Other respondents referenced wider features as part of a contextual advertising method, such as putting audiences into cohorts. They highlighted that this approach would process personal data. We've considered those points in the next sub-section.

We heard that contextual information could be derived by:

- the page URL;
- Natural Language Processing (NLP); or
- semantic analysis of the page eg using keyword matching.

Some respondents, including those representing news media publishers, said that while contextual-only targeting is technically feasible, it is not commercially viable. During engagement, we also heard the view that it works for some online services better than others – for example, it can suit interest-based platforms focused on one topic better than broader, more diverse services like news sites.

"Our members report that they cannot effectively monetise consent-less data inventory because ad agencies will pay several times for personalised advertising what they would pay for contextual advertising and in some cases wouldn't bid any money to certain contextual ad campaigns at all."

Source: Professional Publishers Association

We also heard that contextual signals, combined with additional signals (eg geolocation data, demographic and interest data, device information

[4] How do the rules apply to online advertising? | ICO

and time-of-day) would enable contextual models to be commercially viable, even if this then blurs the boundary with behavioural advertising.

Respondents noted that they would need to implement safeguards to prevent these being misused, eg for tracking and profiling. For example, abstraction may be required to reduce the risk of this analysis gathering more information than required, potentially leading to processing personal data or inferring sensitive information. One example provided was to use the category "car accessories and parts" rather than "Ford Focus headlamp".

Demographic and interest-based targeting

Several responses discussed demographic and interest-based targeting. One described this as requiring "declared, inferred or third-party data (eg age, family status, life stage) to reach relevant audiences." First-party information could include sign-up information, such as age or gender, or other information based on site activity, eg products added to a shopping basket. Few respondents commented on the size of audience segments they felt would be necessary for commercial viability. One example provided to indicate the appropriate level of granularity was: "males between the ages of 40-49, who are interested in camping."

Browsing and behavioural data was also referenced as sources for demographic and interest-based targeting. It was not always clear where respondents drew the line between this approach and behavioural advertising.

Geolocation targeting

We heard that geolocation targeting (or 'geotargeting'), often based on the user's IP address or GPS data, is needed for targeting ads. Respondents described it as particularly useful in combination with contextual targeting approaches. Geotargeting can be done at various levels of granularity:

- Country-level location. Respondents generally considered this as a minimum requirement. This ensures the product being marketed is available in the country where the user sees the ad and served in the right language. It also ensures compliance with any local laws (ie restrictions around marketing certain products in specific jurisdictions).

- Region or city-level location. People suggested this as sufficient information to tailor campaigns and ensure commercial relevance while providing a balance with user privacy.
- Postcode-level location. A small number of respondents raised this as required information for geotargeting. They did not define whether full or partial postcodes were necessary. Rationale for more specific geotargeting included points about local businesses or organisations running events being able to promote themselves.

"Country information is an absolute minimum. If allowed, this could either be retrieved from IP addresses (the typical way of doing it) or from the time zone information stored in the device.

Next to that some indication of the type of device the ad will be watched on (eg a desktop or phone).

Finally contextual information, like the page URL the user was watching and the identifier of the ad position within the publisher, which allows targeting on contextual things."

Source: Opt Out Advertising

Behavioural targeting

Many respondents agreed with our opinion, explained in the call for views, that behavioural targeting should always require user consent.

While we heard clearly that behavioural advertising models are most valuable, these approaches are out of scope for this work.

ICO response

Our preferred approach, laid out in our advice to government, reflects the views we have received about the minimum information required to target ads towards users. Specifically:

- We note that there is no one definition of "contextual targeting" and that respondents will have different views of what it means. We suggest that content the user is immediately viewing, mapped to a broad taxonomy (eg 'sports' or 'cycling'), is sufficient to enable contextual targeting. This aligns with user expectations we heard in our citizens' juries where participants were generally accepting of ads

without consent when they are about the content they are viewing. Using more granular categories, particularly where these are broadcast across a large number of parties, could increase the risk of people being targeted and of special category data being inferred.

- We agree that basic temporal targeting based on time zones could be acceptable for targeting users who have not granted consent.
- We agree that geotargeting to the region or city level is sufficient. This aligns with user expectations from our citizens' juries.
- While some take the view that behavioural or ID-based targeting was required to access the greatest commercial value, we are clear that this should always require consent. Our view remains that, PECR aside, processing personal data for behavioural advertising purposes will require consent under the UK GDPR. In part, this is because these approaches without consent would also misalign with user expectations as understood through our user research.

We understand that contextual approaches are not always the most profitable solution for some organisations. Organisations may choose to use other approaches where they have obtained valid consent from the user.

Frequency capping

Frequency capping limits the number of times an ad is shown to a single user or device within a specified timeframe. We heard that frequency capping is needed to prevent excessive repetition of ads, which can worsen user experience, harm brand reputation and waste budgets. This is because organisations are spending money on ads that are unlikely to lead to sales.

Frequency capping usually involves device IDs to identify users. Respondents commenting on this generally prefer these IDs to be persistent or assigned to a user for a specific time period, eg a week or month.

We also heard an alternative view that frequency capping should not be permitted without consent, because it requires user recognition and comes with risks of this being misused for tracking and profiling.

Respondents made three suggestions to reduce this risk:

- Limiting frequency capping capabilities to one browser session, which could be a compromise between utility and privacy.
- On-device frequency tracking solutions, where the user's device decides if a specific ad can be shown again, based on a rule set by the advertiser.
- First-party frequency capping, where the online service (the publisher) can cap the number of times an ad is shown on their service only.

ICO response

We understand the value of frequency capping functionality for both publishers and advertisers. Typically, it involves identifying someone's device. Approaches for cross-site frequency capping involve persistent identifiers such as third-party cookies. We agree with the respondents who told us that this comes with a risk of an identifier for frequency capping being used for other purposes.

Based on what we have heard through the call for views, other engagement and through our user research, our proposed approach will include frequency capping within the first-party publisher domain – the online service the user is interacting with – only.

While this may be seen as lower value than cross-site practices, we think it better balances the value of frequency capping with the potential risks to users.

We have also advised that government could consider including privacy-enhancing technology (PET)-enabled, cross-site frequency capping within scope of an exception. We understand that these market solutions may not yet be available. However, if developed, they could add value for industry without increasing risk to users.

We think cross-device frequency capping will always need consent. This is because people should have choice and control over when their identity is tracked across devices for advertising purposes. We also note that the regulation 6 rules are intended to provide specific protection for the user's device.

Measurement and attribution

Respondents from the online advertising industry stated that measurement and attribution are critical for advertisers to justify their ad spend. In particular, these are needed to demonstrate a campaign's value, effectiveness and return on ad spend. The next three sub-sections will cover measurement and attribution, including affiliate marketing capabilities.

Measurement

We heard from different parts of the industry that collecting data on impressions, clicks and views is central to making online advertising commercially viable. This information gives advertisers the ability to make budget decisions and to understand the impact of their campaigns.

Some respondents acknowledged that common measurement and attribution techniques carry privacy risks to users, as they rely on user IDs. To address this, some respondents said that data does not need to be held by the publishers at a user level. They suggested safeguards such as:

- cleanroom integrations; and
- PETs, including trusted execution environments and multi-party computation, resulting in aggregated data.

It was suggested that these safeguards could help to balance privacy and utility where the user hasn't given consent.

Attribution

Some respondents also highlighted the importance of attributing a conversion (eg a sale or sign-up) to an interaction with an ad, to allocate credit. This usually involves following a user's journey from initial ad exposure through to a final action. It may involve tracking users across devices and over multiple sessions, where a conversion action isn't taken immediately or is taken on a different device. Some respondents specified they favour a multi-touch attribution model (where credit for a conversion is split between clicks or impressions the user has made on different services) over a last-touch attribution model (where credit is given to the most recent click or impression before conversion). This allows sharing credit for conversions across parties.

As with other capabilities, involving independent third parties was considered important to deliver measurement and attribution capabilities and ensure reliable and trustworthy information.

We heard that PET-enabled attribution reporting could be useful to avoid identifying individuals and reduce risks, eg using differential privacy techniques. However, it was also suggested that this would not eliminate the risks to individuals. Rather, risks would depend on decisions taken by those creating PET-enabled attribution tools, such as the epsilon value (sometimes referred to as the 'privacy budget') used for differential privacy.

Affiliate marketing

Affiliate and partner marketing is a performance-based strategy where businesses pay partners, publishers or third parties, (or 'affiliates') for driving traffic, leading to sales using unique tracking links. Respondents from the affiliate marketing industry told us that affiliate marketing is lower risk than programmatic online advertising approaches. This is because it does not involve complex user profiling, drawing of inferences about a consumer or retargeting or lengthy supply chains. As one respondent explained:

"To measure how an advertisement has performed, it is necessary to use cookies:

- to record the referral of the consumer from the publisher's website to the advertiser's, typically on the clicking of an advertisement or other content which links to the advertiser's website;
- on arrival at the advertiser's website, to attribute the referral to the correct publisher; and
- to recognise the completion of an e-commerce transaction (or the completion of another desired outcome, such as enrolling to test drive a car) at the advertiser's website ("transaction")."

Source: Awin Limited

For cashback platforms, we understand that transaction-level information is required to allocate credit to publishers and the correct cashback to consumers. The tracking period must be long enough to correct data in the case of consumer refunds. We heard that newer, privacy-focused

approaches to attribution, such as Apple's Private Click measurement,[5] are insufficient to deliver this capability.

ICO response

We understand that the ability to count aggregated impressions, clicks and views is important for a viable advertising model. We also recognise that independent third-party verification is an important factor to maintain advertiser trust. Our advice to government explains how an exception(s) to regulation 6 could include these functions. It takes these responses into account, as well as the findings from our user research and our understanding of the legal framework.

We understand the importance of attribution in online advertising. However, it inherently relies on tracking users across sites, to connect where a user has seen the ad with their later purchase. This would involve sharing personal data outside of the first-party domain and carries a tracking risk. Promising innovations using PETs are emerging that can enable cross-site attribution without identifying users across sites. Our advice recognises the potential of these solutions.

We have considered affiliate marketing within this capability. While we accept that there are differences between these practices and programmatic advertising, the technical underpinnings are the same. In our view, there are still risks to users of being tracked across sites and devices. Innovation from some parts of the affiliate marketing industry would be needed to make use of any exception(s) in line with our preferred approach if they were introduced. However, we think our attribution proposal offers an opportunity for this part of the market to innovate, without opening up unacceptable tracking risks to users.

Where cross-site attribution capabilities go beyond any future exception(s) (eg where they rely on third-party cookies), this capability can still be done with valid consent.

Separately, we have clarified the circumstances in which rewards and cashback services can make use of the 'strictly necessary' exception to the current regulation 6 rules. This is available in our final guidance on

[5] Now known as Web AdAttributionKit. See: UIEventAttributionView | Apple Developer Documentation

the use of storage and access technologies.[6]

Brand safety, suitability and compliance

Respondents told us that brand safety is an important function for brands to protect their identity and reputation, by ensuring that people see their ads in an appropriate place. Similarly, publishers also want to control what types of ads are appearing on their site. We understand that the level of importance of brand safety features depends on the type of campaign and potential risk for that brand. Some respondents highlighted that the risk to users is minimal because this capability is about analysing web content, not users.

We heard that brand safety can be done in a minimalist way. Specifically, by making the URL of where the ad would be served available to advertisers, along with a contextual classification of content (categorising pages by topic or sensitivity). Blocklists and allowlists can restrict delivery of ads solely to approved sites. Content classification is often done at scale, using natural language processing and semantic analysis. Respondents said that this classification was required before the ad appears on a page.

We heard that independent verification of brand safety is important to buyers for credibility and oversight. Respondents mentioned third-party tools that they use for brand safety and other purposes. They noted that they use scripts and tags and other storage and access technologies to classify and block content.

Several respondents stated a need for greater transparency between publishers and advertisers, with concerns raised over misrepresentation of the context in which ads will be shown.

ICO response

We agree with the view that stated contextual classification of the first-party site is sufficient for the purposes of brand safety. Using the full URL, while useful, creates a risk of organisations using this information for individual targeting purposes where it is combined with other information. We also understand that the sell-side sometimes truncates or blocks the

[6] https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-on-the-use-of-storage-and-access-technologies/

URL in the bid request, reducing the potential value of this information.

Instead, our proposed approach suggests that the publisher site (or a third party on their behalf) does page scanning for brand safety purposes. They can submit an abstracted signal in the bid request to convey information to buyers. This will mitigate risks of misuse of this information or of third parties collecting more information than is required. We have explained this further in our advice to government.

Ad fraud prevention and detection

We consistently heard that ad fraud prevention and detection is an important feature of a commercially viable advertising model. Without the ability to detect and prevent ad fraud, advertisers lose confidence that their ads are reaching real users, the publisher's credibility is affected and ad spend is wasted as it is diverted to illegitimate sources.

We have separated views into points about invalid traffic (IVT), domain spoofing and other types of ad fraud. Respondents noted that these services are often provided by third-party ad verification services.

Invalid traffic (IVT)

IVT detection or traffic validation was the most commonly referenced ad fraud prevention and detection feature. We understand IVT to be a broad term describing online activity that does not always come from a real user, meaning impressions do not represent legitimate advertising consumption. Participants cited different amounts of information required for IVT prevention and detection (eg to validate impressions).

IP addresses were raised as a minimum requirement to detect IVT. Knowing the IP address can help to identify bots, unknown browsers or known data centre traffic, for example by comparing against a list of known bots or data centres. One respondent stated that 'only short retention periods [of IP address] are required'. Some respondents said that user agent strings were also required alongside IP addresses. We understand this to be because bots can use specific browser and device combinations.

Some respondents said they needed more information to identify sophisticated IVT, eg incentivised browsing or rerouting techniques. This would include behavioural analysis, for example to monitor mouse movements, click behaviour or the duration of user engagement. We

understand that organisations require a log of event-level delivery data, which could be aggregated to detect statistical anomalies.

We heard that there is some privacy innovation in ad fraud detection, where cookies, identifiers or fingerprinting techniques were typically used for maintaining records of users across sessions. These more privacy-preserving approaches can involve 'session-level validation, aggregated reporting, and short-lived tokens.'

Like with brand safety, we recognise that third-party verification services usually provide ad fraud prevention and detection functionality.

Domain spoofing

Protection against domain spoofing (where bad actors pretend to be legitimate publishers and sell fake ad space) was another frequently referenced requirement for ad fraud.

Some respondents said they verified publisher authenticity via DNS and SSL certificate analysis.[7] Some also mentioned using the IAB Tech Lab solutions: Ads.txt/app-ads.text and sellers.json.

Other types of ad fraud

Respondents highlighted other types of ad fraud aiming to deliver false ad engagement metrics like impressions and clicks, including:

- "ad stacking" and "pixel stuffing" - where ads are invisibly layered or made too small to see; and
- click farms – a coordinated group of people or systems generating large volumes of fake clicks or other engagement to inflate metrics.

Respondents said that impression and click verification to detect these types of ad fraud is performed by tracking user engagement patterns, timestamps and device IDs.

ICO response

We understand that ad fraud is a significant issue in online advertising. However, ad fraud prevention and detection tools often involve accessing significant amounts of information from the user's device and sharing it

[7] While respondents mentioned SSL certificate analysis, we note that TLS is the successor to SSL and uses more modern cryptographic protocols. Our guidance on encryption clarifies our view on this: Encryption and data transfer | ICO

with third parties. Even if the purpose is valid, there are still high risks to users of being identified and for this information to be widely shared or misused.

We accept the need for pre-bid filtering, using device and browser information, by the publisher or publisher ad server. However, our preferred approach dictates that if this were to be exempt from consent requirements, organisations must not share information in the ecosystem. Instead, publishers could use a secure method (one example being the Private State Token API) to reassure buyers that the user is human.

We also understand the value industry places on commonly used tools including IAB Tech Lab solutions like ads.txt/app-ads.txt, sellers.json, ads.cert and buyers.json. These tools involve the use of information about the service providers and advertisers involved, rather than the subscriber or user – so, in principle, using these tools may carry a lower risk to users.

We think that restricted post-bid analysis on the first-party site without consent could be acceptable for verification purposes. Third-party analysis of user behaviour must have consent due to the inherent tracking and profiling risks.

Our advice document explains our views in more detail.[8]

Ad delivery and billing

Most respondents focused on billing rather than ad delivery requirements, and points were closely related to ad measurement. Some respondents considered conversion tracking within ad delivery and billing – we've incorporated that feedback within the measurement and attribution section above instead.

Where ad delivery was discussed, respondents raised that they needed storage and access technologies to technically deliver ads, including sending and responding to ad requests and delivering ad files. Here, they needed session management cookies to ensure consistent ad delivery during user browsing sessions.

[8] ICO, 2026. ICO report for DSIT: Advice on a viable approach to creating online advertising exception(s) to regulation 6 PECR. Available at: https://ico.org.uk/media2/yefdqvk4/20260505-report-for-dsit-on-changes-to-regulation-6-pecr-for-online-advertising.pdf

We heard that billing is required to ensure the right organisations get paid correctly. Impressions, clicks and views were commonly referenced metrics for billing. These were said to provide proof of ad delivery, ad interactions or views between advertisers and publishers. They are therefore fundamental to their commercial relationship.

Some respondents added other information required alongside impression, clicks or view logs, such as:

- the timestamp;
- ad slot ID;
- device or user agent information;
- IP address; and
- a campaign or creative ID.

Affiliate marketing respondents told us that they use attribution to determine advertising commissions. We have considered this under the measurement and attribution capability.

Some respondents commented on what they considered to be privacy-preserving features for ad delivery and billing, including truncating the IP address and limiting how long they can keep billing logs.

ICO response

We noted that few respondents focused on required capabilities for ad delivery in their response (for example, the use of a third-party ad server as a basic requirement). It might be that some respondents assumed this functionality would be permitted, or did not appreciate the use of storage and access technologies involved in ad delivery. Our advice highlights that ad delivery is required to serve ads and would need to be included in any future online advertising exception to regulation 6.

We understand the requirement to bill accurately. Our proposed approach aligns the functionality for billing with measurement by advising that any future exception permits billing based on aggregated impressions, clicks and views (including third-party verification). This is for consistency, because both functions often rely on the same information, based on similar uses of storage and access technologies.

Finally, we note that IP address truncation is insufficient to guarantee anonymisation.

Other key themes

The role of the ICO and project approach

Many respondents, particularly those from within the online advertising industry, welcomed this call for views and our proposed approach to change our regulatory posture. However, some raised questions and concerns about our role in proposed changes to regulation 6. This included comments highlighting that it is government's role to change the law.

"We note that this proposal is in relation to enforcement, and we encourage the development of secondary legislation in this area in order to provide more robust legal certainty to firms."

Source: UK Finance

Some also raised queries about whether all organisations would interpret a new regulatory posture in the same way. They suggested that clear ICO guidance, industry-standard definitions and defined technical and policy frameworks would be required.

ICO response

Changing legislation is a matter for government and parliament. We recognise that this government has plans to use its power under the new regulation 6A in PECR to amend the rules for online advertising. As an independent regulator, we are providing advice on how government could do that, following our commitments to support its economic growth ambitions and our duties under the Data Protection Act.

We originally planned to revise our regulatory posture in the interim period before any legislative change, but we have since changed our approach. This change recognises that clarity is essential for any new approach to regulation 6 to support economic growth and innovation. We heard from this call for views that our intention to change our regulatory posture was confusing. Some said that they would not make use of benefits stemming from a new enforcement approach without a change in the law itself.

We think that our new approach is a better way to support innovation in

low-risk online advertising whilst maintaining legal certainty for businesses. If government does decide to make changes to regulation 6, we will provide guidance to support organisations looking to make use of any new exception(s).

Wider industry context

We heard several different points about wider factors that will influence the impact of a new approach to regulation 6:

- Regulation 6 is only one challenge facing publishers. By itself, a new approach won't solve all the industry's problems. On the other hand, others suggested that this could provide an incentive to overcome inertia in the industry and accelerate its use of PETs.
- Impacts on the industry will depend on advertiser actions – if advertisers don't buy inventory made available by any relaxed regulation 6 rules, the new approach won't work. Similarly, advertisers and publishers still operate in a landscape influenced by platform policies, agency practices and legal risk assessments.
- There would be technical and operational complexity in implementing new models. This may require significant system updates across the adtech ecosystem. There may be additional costs and demands for engineering, compliance and project teams.
- Some advertisers and publishers operate across borders. If UK rules diverge, it could lead to fragmentation, higher compliance costs and unintended risks of non-compliance.
- Some organisations already break the regulation 6 rules because they do not foresee a threat of ICO enforcement action. Enforcement of non-compliance would be required for this new approach to have an impact.

ICO response

We understand the landscape the online advertising industry is operating in, beyond the legislation we regulate. For example, the evolution of large language models and agentic AI is changing the way users interact with online services, which may lead to decreasing search-directed traffic. We know that advertising formats are changing, eg with video advertising increasing. We understand that third-party cookie availability is an ongoing challenge. However, we think that reducing regulatory requirements in low-risk areas would be helpful for an industry facing

challenges.

We also recognise that if government adopted our preferred approach, it would require a change in approach for the industry to utilise it. We recognise the potential for innovation and we would support adoption, for example through our Regulatory Sandbox and Innovation Advice services and by providing clear guidance.

We agree that regulatory supervision is essential alongside any relaxation in the law to uphold people's rights. Our action under the online tracking strategy has led to 99% of the UK's top 1,000 websites meeting our compliance checks for advertising cookies.[9]

Risks for users

Views were split between respondents who felt that we could identify commercially viable solutions that could also safeguard people's privacy and improve user experience and those who did not (see Table 1 in section 3.5).

Of those who disagreed, some respondents raised concerns about ads being targeted at users without their consent, highlighting the risks of harm from people being targeted based on their personal data. For example, one respondent said:

"The ability to target individuals based on personal data is the main enabler of harms, discrimination and predatory practices that plague online advertising. Targeting based on personal data exposes women to unjust prosecutions for their attempt to exercise reproductive health rights; problem gamblers to being targeted with gambling ads that are meant to exploit their addiction; anyone to be excluded on the basis of their gender, sexual preferences, ethnicity or other sensitive characteristics; children and those in a more vulnerable status to be targeted and taken advantage of."

Source: Open Rights Group

Other concerns raised about a proposed change in our approach to regulating regulation 6 included:

[9] Online tracking strategy update – April 2026 | ICO

- current compliance issues in the ecosystem and the potential for these to be exacerbated by relaxed rules;
- the risk of multiple data points collected without consent being combined together to identify individuals; and
- a need to also reinforce regulation 6 rules to 'level the playing field' for the industry.

ICO response

We agree that targeting users based on their personal data can cause harm. Our preferred approach takes user concerns into account, including findings from our citizens' juries on new routes to viable online advertising.[10] If government adopted our preferred approach and it was written into law, targeting users with behavioural advertising would still require consent. As laid out in our advice to government, information that can be used for targeting will be limited to basic data points. Our advice also describes how organisations can use this data to minimise the risks of information being linked together and misused to identify and re-target individuals.

Our advice to government is based on our expertise as the data protection regulator, including the work undertaken as part of this project.

Safeguards

Respondents expressed wide-ranging views on technical safeguards, the current use of PETs and recent innovations that could be used in circumstances where online advertising may be delivered without consent. Suggestions included:

- Using PETs to mitigate data protection and privacy risks associated with using storage and access technologies for online advertising purposes. Specific PETs mentioned included:
    - differential privacy;
    - secure multi-party computation;
    - homomorphic encryption;
    - federated learning; and
    - trusted execution environments.

[10] ICO, 2026. Citizens' Juries on New Routes to Viable Online Advertising. Available at: https://ico.org.uk/media2/outapyon/citizens-jury-final-report.pdf

- On-device processing. This was identified to be a robust approach, as it can limit the transfer of information and reduce re-identification risks. For example, on-device solutions that use signals like content consumption to create 'anonymous cohorts'.
- Adoption of browser-level technical signals, such as Global Privacy Control.[11]
- Data labelling frameworks, designed to encode legal bases and processing restrictions directly into machine-readable signals.
- New browser-based APIs, such as those developed through the Google Privacy Sandbox.
- Data clean rooms, including those that process datasets in a secure environment.
- Contractual controls, for example to prohibit re-identification.

We also heard that technical safeguards alone are not enough to tackle the inherent risks in online advertising. Respondents suggested that the core problem is non-compliance with the current legislation, rather than a lack of available safeguards.

ICO response

Some of these responses helped to inform our advice to government, where the use of PETs and technical controls form a vital underpinning to our preferred approach. Responses helped identify where PETs can enable cross-site functionality (eg for attribution and frequency capping). We think adopting PETs is the only possible way to use cross-site functionality without consent, because otherwise the risks of users being identified and tracked across sites would be too high.

However, we agree with respondents who said that these safeguards alone aren't enough. Our approach recognises the role for such technical solutions, without just relying on them to address risks inherent to online advertising.

Expected impacts

Respondents were asked how far they 'agree that the approach outlined in our call for views can identify commercially viable solutions that can also safeguard people's privacy and improve user experience'. Table 1 provides an overview of the responses, illustrating that more than half

[11] Global Privacy Control — Take Control Of Your Privacy

(51% or 30 responses) agreed or strongly agreed, while 37% (22 responses) disagreed or strongly disagreed.

Table 1: Agreement with approach

Response	Count	%
Strongly agree	12	20%
Agree	18	31%
Unsure/Don't know	7	12%
Disagree	2	3%
Strongly disagree	20	34%
Total	**59**	**100%**

Source: ICO Citizen Space consultation n= 59

As illustrated in Table 2, 31% of respondents (18 responses) also noted that they felt there were challenges in delivering commercially viable advertising if we revised our regulatory posture towards regulation 6 for specific advertising purposes.

Table 2: Challenges

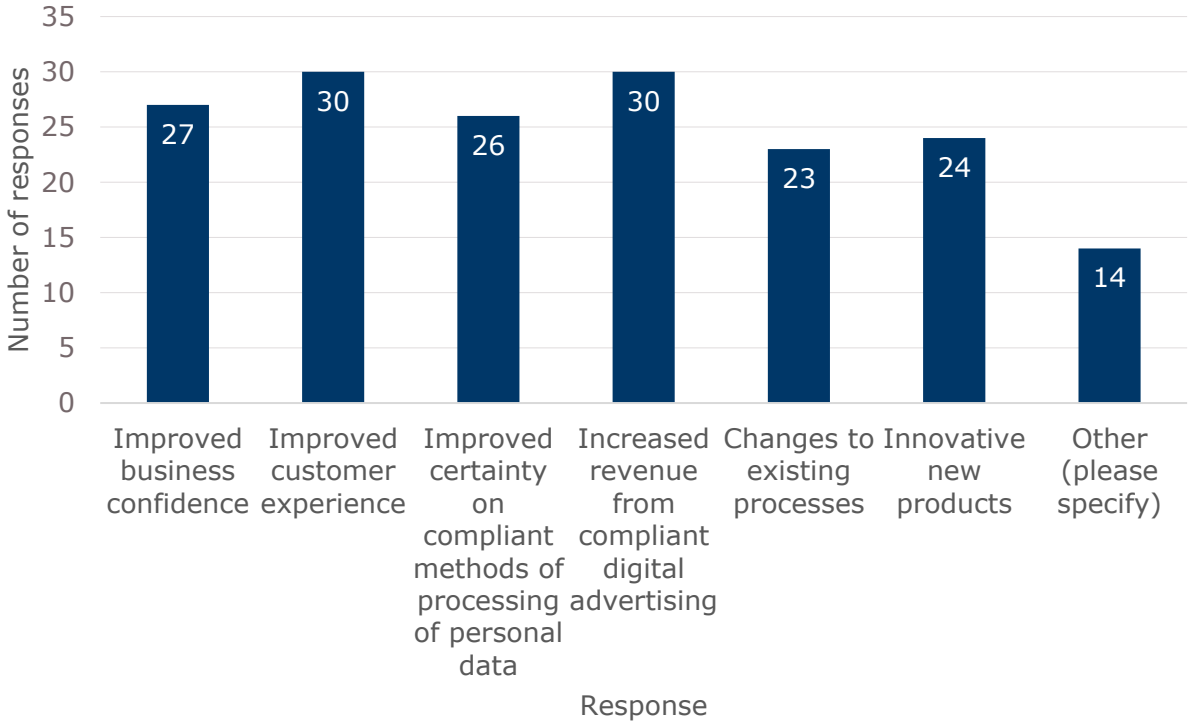
Response	Count	%
Yes	18	31%
Unsure / Don't know	25	42%
No	16	27%
Total	**59**	**100%**

Source: ICO Citizen Space consultation n= 59

Respondents were asked whether they would anticipate positive and negative impacts if any of the capabilities referenced were permitted without regulation 6 consent in low-risk circumstances.

Overall, the majority of respondents (55%) identified that the proposed regulatory approach would result in either 'benefits' (25%) or 'both benefits and costs' (30%), while just 5% of respondents identified only 'costs'. The remainder (40%) did not provide an answer. As illustrated in **Error! Reference source not found.**, the most popular positive impacts selected were 'improved customer experience' and 'increased revenue from compliant digital advertising'.

Figure 1: Positive impacts anticipated



Source: ICO Citizen Space consultation n= 59

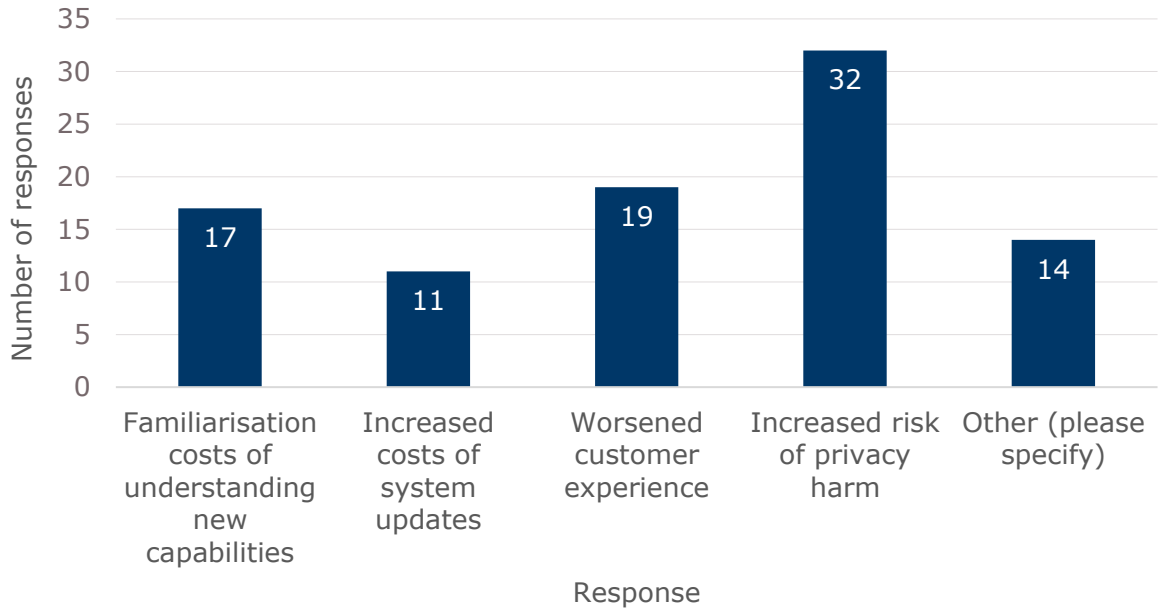
For those who responded 'other', additional positive impacts included 'economic growth', 'increased competitiveness' and 'innovation'. Respondents provided further opinions on the potential for positive impacts.

"The overreliance on consent has not created an improved level of trust from users, confronted throughout their online experience with consent banners. The new approach is likely to improve customer experience with a reduced number of consent requirements across their browsing activities, in line with the operational functioning of the internet. It will also ensure that users are more aware when a higher risk is present as they will be presented with a consent requirement."

Source: European Publishers Council

'Increased risk of privacy harm' was the most popular negative impact selected, as illustrated in **Error! Reference source not found.**.

Figure 2: Negative impacts anticipated



Source: ICO Citizen Space consultation n= 59

For those that stated 'other', additional negative impacts included 'governance complexity' and 'discriminatory targeting'. Opinions provided on the negative impacts are below.

"It is important to understand that users' interests and fundamental rights can be negatively affected by ad tech beyond privacy, and consideration of changes to PECR enforcement should not be limited to negative impacts on privacy. For example, ad targeting can be discriminatory with men and women being shown different ads based on profiling. Profiling of people can also enable targeting of vulnerable individuals for exploitation or harm, eg gambling companies targeting addicts or bad actors spreading extreme views or disinformation."

Source: People Vs Big Tech

"Clearly familiarisation with a new PECR regime will consume some executive time and effort. However, this would be more than offset by a reduction in the substantial sums currently spent on commissioning advice from lawyers and data protection consultants, as well as operational time and diligence to ensure our technology environment adheres with PECR. We would also expect our business overall to expand,

as a relaxation in regulatory constraints, reduction in ad fraud, and more certainty around ad delivery metrics will encourage advertisers to increase budgets."

Source: DMG Media

ICO response

The responses to the questions on anticipated impacts have informed our cost-benefit analysis, which we shared with DSIT and published alongside our advice. Comments concerning issues facing the industry and potential impacts have also been considered in decisions on our preferred approach and final advice to government.

Overview of responses

Breakdown of responses

This consultation received 59 responses via Citizen Space. 33 were responding on behalf of an organisation, 21 that were not responding on behalf of an organisation and 5 responding as 'other'. Table 3 shows the complete breakdown of respondents:

Table 3: Breakdown of respondents

Which of the following describes your organisation	Number	%
I'm not responding on behalf of an organisation	21	36%
A private sector organisation	21	36%
A charity or third sector organisation	11	19%
Other (please specify)	5	8%
A public sector organisation	1	2%
Total	**59**	**100%**

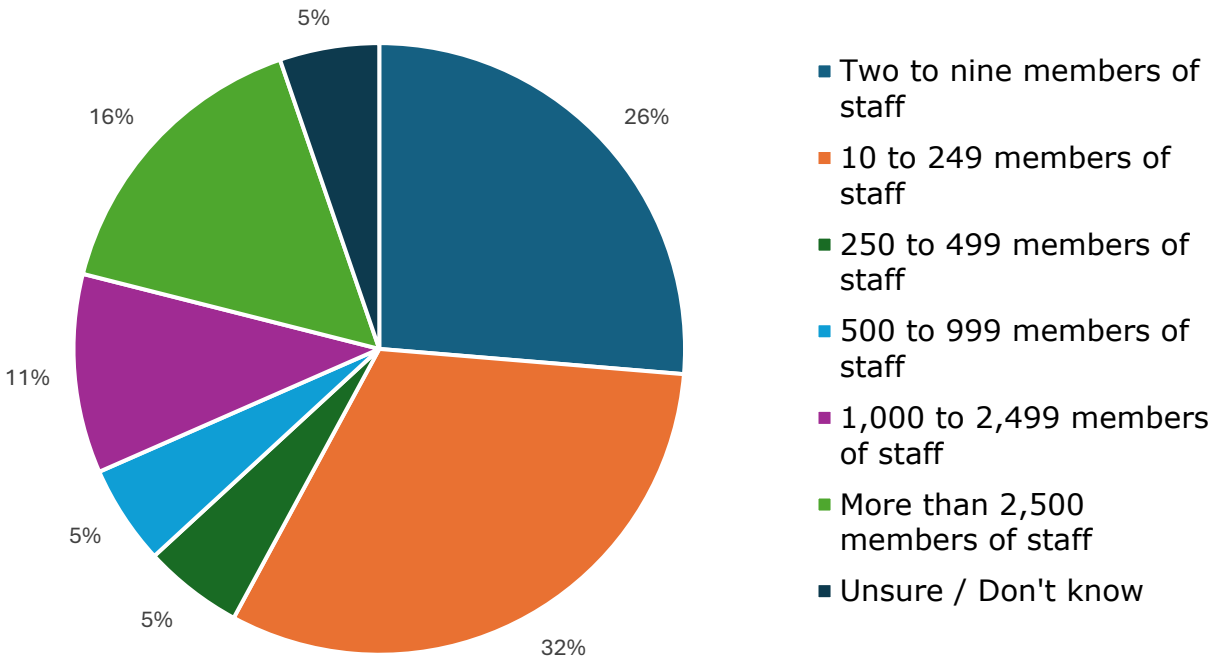
Source: ICO Citizen Space consultation n= 59

There were also 17 respondents by email. These responses did not answer the survey questions and so have been excluded from the analysis

in this section. However, the email responses provided have been considered in preceding parts of this summary.

Of the total 38 organisational responses received, the majority (58% or 22 responses) were SMEs (organisations with fewer than 250 members of staff), while 16% (six responses) were from organisations with over 2,500 members of staff. Figure 3 illustrates the organisation size stated by respondents.

Figure 3: Organisation size



Source: ICO Citizen Space consultation n=38