Upholding information rights

Wycliffe House, Water Lane, Wilmslow, SK9 5AF
T. 0303 123 1113 E. icocasework@ico.org.uk
www.ico.org.uk

Sent by email to:

15 November 2023

Dear DPO,

Compliance of your organisation's cookie banner with the requirements of PECR and UK GDPR

The ICO is the UK's independent public authority responsible for overseeing and enforcing the provisions of the Privacy and Electronic Communications Regulations 2003 (as amended) (PECR), the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation 2018 (UK GDPR).

We have recently carried out an assessment of the cookie banners of the top 100 UK websites in May based on active time spent by UK users to monitor compliance with PECR and GDPR.

For the reasons set out in this letter, we are concerned that your website may infringe PECR and UK GDPR. As set out further below, the ICO may decide to take action in respect of these suspected infringements unless you take steps to address our concerns within one month of this letter.

On 23 October 2023 we assessed the cookie banner on your website to see whether:

- non-essential advertising cookies are placed before the user has the opportunity to provide consent;
- users can reject non-essential advertising cookies as easily as they can accept them; and
- non-essential advertising cookies are placed even if the user did not consent to such cookies.

Please note that our assessment is limited to the points outlined above; other areas of compliance with data protection and e-privacy legislation have not been assessed.
We ask that you address our concerns by taking steps within one month of this letter to bring your organisation's cookie banner into compliance with the requirements of PECR and UK GDPR. As part of this ongoing work, we are planning to publish the names of organisations that fail to take appropriate steps to address our concerns. Further information regarding publication is provided in section 2 of this letter.

The legal obligations relating to the use of non-essential advertising cookies and the related processing of personal data are set out in PECR and UK GDPR. We attach at Annex 1 a summary of these obligations.

We explain in more detail below:

1. why we are concerned that your website may not be compliant with PECR and UK GDPR; and

2. the action we recommend you take to address our concerns and our next steps.

1. Our concerns about the compliance of your cookie banner with PECR and UK GDPR

Non-essential advertising cookies were placed without obtaining consent from users

Our assessment identified that your website places non-essential advertising cookies, for which consent is required, without obtaining consent from users. Your website has no cookies banner at all and as such consent cannot be sought from users. We have included screenshots from our assessment demonstrating this in Annex 2 to this letter.

We are concerned that the placing of non-essential advertising cookies and processing of personal data is therefore unlikely to comply with PECR and UK GDPR.

Non-essential advertising cookies were placed before the user had the opportunity to provide consent

Our assessment identified that your website places non-essential advertising cookies, for which consent is required, without first obtaining consent from users. We have included screenshots from our assessment demonstrating this in Annex 2 to this letter.

Even if consent is later obtained using a cookie banner, we do not consider such consent to be valid, given that that placement of non-essential advertising cookies and processing of personal data occurred before consent was sought. This is regardless of whether a user subsequently provides consent or not.

We are concerned that this placing of non-essential advertising cookies and processing of personal data is therefore unlikely to comply with PECR and UK GDPR.

Users cannot reject non-essential advertising cookies as easily as they can accept them

Our assessment identified that your website informs people that non-essential advertising cookies are used and asks for their consent. However, while the cookie banner contains a button allowing immediate consent to cookies, it does not give similar means to refuse the storage of these cookies as easily or in one click. We have included screenshots from our assessment demonstrating this in Annex 2 to this letter.

As such, we are concerned that any consent purportedly obtained by a user clicking "Accept all" on the first layer of the cookie banner cannot be regarded as having been

freely given, specific or informed in relation to each processing activity. This is because your cookie banner fails to provide an equally prominent "Reject All" or other equivalent and non-ambiguous option not to accept non-essential advertising cookies.

We are concerned that this failure to obtain meaningful consent for placing non-essential marketing cookies or processing personal data means that the way you operate your website is unlikely to comply with PECR and UK GDPR.

Non-essential advertising cookies were placed despite the user opting to reject them

Our assessment identified that your website offered a consent mechanism, but failed to respect the choices that individuals expressed by placing non-essential advertising cookies despite the users opting to "reject all" cookies. We have included screenshots from our assessment demonstrating this in Annex 2 to this letter.

We are concerned that your processing of personal data after the placement of non-essential advertising cookies that have previously been refused by the user is likely to lack a valid lawful basis under Article 6 UK GDPR, and is therefore also likely to infringe Article 5(1)(a) UK GDPR. You are also likely to have infringed PECR Regulation 6 because the placing of non-essential advertising cookies requires valid consent from the user. These cookies should not be placed without such consent.

2. Next Steps

We ask that you address our concerns by taking steps within one month of this letter to bring your organisation's cookie banner into compliance with the requirements of PECR and UK GDPR. In summary:

- You must not place non-essential advertising cookies, nor process personal data using such cookies, without first obtaining valid consent from individuals accessing your website.

- You must provide data subjects with a way of refusing non-essential advertising cookies at the same point you seek consent. For example, by providing a button to 'reject all' or another equivalent and non-ambiguous solution that is equally prominent as the option to accept cookies.

- You must respect individuals' choices in respect of the placement of non-essential advertising cookies. Where a user does not accept placement of these cookies, such cookies should not be placed and personal data should not be processed using this technology.

In a month's time the ICO will conduct another assessment of the cookie banner on your website to identify whether your organisation has taken steps to improve compliance with PECR and UK GDPR. Depending on the outcome of the further assessment, we will decide on what further action (if any) to take in relation to your organisation on the basis set out below.

Over the past few months we have sought to raise public awareness of the need for organisations to comply with cookie banners. For example, on 9 August 2023 we published a joint paper with the Competition and Markets Authority calling for businesses to stop using harmful website designs, including in relation to cookie banners.
As part of this ongoing work, we are planning to publish the names of organisations that fail to take appropriate steps to address specific concerns raised by the ICO about their cookie banners. We consider this is an appropriate step to ensure that people are protected from the unlawful use of cookies and unlawful processing of their personal data.

If we identify that your organisation has failed to address the ICO's concerns, we may publish the fact that the ICO has written to you about our concerns. We will inform you if we decide to make our concerns about your organisation public in this way and give you a reasonable opportunity to make representations about our decision. We may also consider taking other action using our enforcement powers, including by way of enforcement notice or penalty notice.

The ICO will not publish your organisation's name if you take action to ensure compliance by addressing our concerns. Alternatively, if you agree, we may publish your organisation's name as a positive example of how cookie banners can comply with PECR and UK GDPR.

If you take action to address our concerns about your cookie banner within one month of this letter we do not require or expect a response. However, if you plan to address our concerns but are unable to rectify your cookie banner by 15/12/23 please explain in writing the following:

- what steps you plan to take to address the concerns set out in this letter;
- why you are unable to take those steps within one month; and
- the expected timescale for the implementation of your planned steps.

If you have any questions or would otherwise like to comment on any of the points raised in this letter, please contact: cookiecompliance@ico.org.uk.

Yours sincerely,

[Personal data redacted]

Stephen Almond
Executive Director, Regulatory Risk

The Information Commissioner's Office

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice.

Annex 1 –
Data protection and e-privacy obligations

Privacy and Electronic Communications Regulations 2003 (PECR)
Regulation 6 PECR applies to any technology that stores or accesses information on a user's device. Regulation 6 of PECR therefore applies to the use of cookies and similar technologies.

Where cookies are used, an organisation must:

- say what cookies will be placed;
- explain what the cookies will do; and
- obtain consent to store cookies on devices

There is no definition of consent in PECR. Instead, the UK GDPR definition of consent applies (see the section on UK GDPR below). In that regard, the ICO's guidance on cookies and similar technologies explains that "a consent mechanism that emphasises 'agree' or 'allow' over 'reject' or 'block' represents a non-compliant approach, as the online service is influencing users towards the 'accept' option".[1]

Further, although PECR includes an exemption from the requirement to obtain consent for "strictly necessary" cookies, as explained in the ICO's guidance on cookies, advertising cookies are not regarded as "strictly necessary".

This means that in relation to non-essential cookies for advertising:

- "the user must take a clear and positive action to give their consent to non-essential cookies – continuing to use your website does not constitute valid consent;
- you must clearly inform users about what your cookies are and what they do before they consent to them being set;
- if you use any third party cookies, you must clearly and specifically name who the third parties are and explain what they will do with the information;
- you cannot use any pre-ticked boxes (or equivalents such as 'on' sliders) for non-essential cookies;
- you must provide users with controls over any non-essential cookies, and still allow users access to your website if they don't consent to these cookies; and

[1] Cookies and similar technologies | ICO

- you must ensure that any non-essential cookies are not placed on your landing page (and similarly that any non-essential scripts or other technologies do not run until the user has given their consent)".

UK General Data Protection Regulation (UK GDPR)
The UK GDPR sets out the requirements for consent that applies both to processing under UK GDPR and to the use of cookies or similar technologies under Regulation 6 of PECR. We have summarised the key provisions relating to consent below.

- Article 4(11) of the UK GDPR states:

  "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

- Article 7 of the UK GDPR provides further specific requirements about consent, requiring that:

  - you must be able to demonstrate that you have valid consent;

  - your requests for consent must be 'clearly distinguishable from other matters' – ie, they must not be bundled as part of the terms and conditions for using the service;

  - your request for consent must be in an intelligible and easily accessible form, using clear and plain language; and

  - your mechanism for obtaining consent must allow the individual to withdraw their consent at any time (in a way that is as easy as it was for the individual to give consent).

The recitals to the UK GDPR provide further indication about the meaning of consent in this context. For example:

- recital 32 of the UK GDPR makes it clear that using pre-ticked boxes, or silence or inactivity on the part of the individual, does not constitute consent;

- recital 42 states that "consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment"; and

- recital 43 clarifies that consent is presumed not to be freely given if the performance of a contract is dependent on the consent, despite such consent not being necessary for the performance of the contract.

Finally, the ICO's guidance on consent clearly sets out what is expected by the ICO in terms of ensuring people are able to give meaningful consent:

> "You must clearly explain to people what they are consenting to in a way they can easily understand. The request for consent needs to be prominent, concise, separate from other terms and conditions, and in plain language.
> […]
> The key issue is that there must still be a positive action that makes it clear someone is agreeing to the use of their information for a specific and obvious purpose.
> […]
> Consent means giving people genuine choice and control over how you use their data. If the individual has no real choice, consent is not freely given and it will be invalid".[2]

For processing of personal data to be lawful under the UK GDPR, an Article 6 lawful basis must be identified. Where consent has been obtained for the placement of cookies, consent will be your lawful basis for the subsequent processing of the personal data under Article 6 the UK GDPR.

Where consent is relied upon as a lawful basis under UK GDPR, you must ensure that you tell individuals, at the time consent is sought, about your processing in a way that is easily accessible and easy to understand. Where there is a lack of transparency, the consent obtained will not be valid.

If you do not have a lawful basis for processing personal data, or are not doing so in a transparent way, then you will infringe Article 5(1)(a) of UK GDPR. Article 5(1)(a) of UK GDPR requires personal data to be processed lawfully, fairly and in a transparent manner in relation to the data subject" ('lawfulness, fairness, transparency'). The ICO has published extensive guidance about the application of this principle.[3]

We have also published other detailed guidance on PECR and UK GDPR.

[2] What is valid consent? | ICO
[3] Principle (a): Lawfulness, fairness and transparency | ICO

Annex 2 –
Assessment screenshots

Screenshot showing non-essential advertising cookies placed before the user had the opportunity to provide consent:

Screenshot showing users cannot reject non-essential advertising cookies as easily as accept them:

Screenshot showing non-essential advertising cookies placed after the user had rejected consent:

Screenshot showing that no consent was obtained despite non-essential advertising cookies being placed: