fyi...

Scottish Information Commissioner: Observations on cookies consent

Document control	
Title:	Scottish Information Commissioner – Observations on cookies consent
Client owner:	Lorraine Currie, lcurrie@itspublicknowledge.info
FYI owner:	Frank Rankin
Author:	Frank Rankin, [redacted]
Date:	January 2021
Version:	0.2
Version history:	0.2 Amended version submitted to client 0.1 Initial draft for QA Dec 2020

Introduction

Following a conversation between Frank Rankin and Lorraine Curry on 11 December discussing the approach to cookies for the Scottish Information Commissioner's website, the following note was compiled.

On the table starting on page 3 we offer a view on where consent is necessary or not for the type of cookies currently used.

We also offer an observation on two specific issues as follows.

"Strictly necessary" exemption and public authorities

It has been noted by SIC that the "strictly necessary" exemption set out in PECR states that it applies to the delivery of "information society services" and that the definition of the term as set out in article 2(a) of the *E-Commerce Directive* and article 1(2) of the Technical Standards and Regulations Directive (98/34/EC), relates to commercially-based services and therefore may not apply to SIC activity. Or that by applying the exemption SIC may incur the liabilities associated with such services, for example around parental consent.

We are not aware of any other public authorities applying the narrow definition of ISS in this context and certainly, in its own practice and guidance, ICO makes no distinction between commercially based online services (which would fall within the definition of ISS) and public-sector online services (which would not). There is no evidence in policy or case law that it was the intention of the drafters of PECR to make it more burdensome for public authorities than for business. Nor are we aware of any criticism of or enforcement activity against public authorities anywhere else in the EU for applying the strictly necessary exemption.

While we agree a strict interpretation of the exemption would mean that it may not be applicable to public authorities, we note that no-one applies such an interpretation. SIC, by taking a broader interpretation (that the exemption would also apply to public authorities although they do not provide ISS) would be in the mainstream and that any risk of adopting such a position would be negligible.

"Settings led consent"

The question of what constitutes settings-led consent was raised. This term is not clearly defined by the ICO but arises in situations where the site "remembers" a preference selected by the user through deploying a cookie. ICO advise: "You can explain to them that by allowing their choice to be remembered they are giving consent to set the cookie. Agreement for the cookie could therefore be seamlessly integrated with the choice the user is already making."

https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply8

From this description it appears that a settings dialogue which clearly explains the use of cookies before the user selects a setting would be sufficient. This appears to meet the definition of consent in GDOR article 4 (freely given, specific, informed and unambiguous) although it is questionable whether this fully meets the EDPB emphasis on consent being unbundled and granular.

Cookie-free analytics

Some organisations are reducing cookie risk by opting for cookie-free analytics solutions. This may be worth exploring for OSIC. (See for example https://github.com/milesmcc/shynet https://privacystats.com/)

As a wider point, in order to meet the GDPR requirements of data minimisation and demonstrable compliance, as well as capturing the technical purpose of each cookie, it would be good to document the business requirement that each cookie meets.

ePrivacy Directive

The most recent (Nov 2020) draft of the proposed EU Privacy Regulation takes a position similar to that followed at the moment with regard to necessary cookies and, in fact, removes the word strictly: "...consent should not be requested for authorizing the technical storage or access which is necessary and proportionate for the purpose of providing a specific service requested by the end-user." (para 21, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9931_2020_INIT&from=EN)

While the UK will no longer be bound directly by the Regulation once enacted, it may well influence the UK position and updated ICO guidance or UK regulation may follow.

Current website cookies

Cookie name	Description of what cookie does	Suggested approach
__utm*	All cookies beginning with "__utm*" are Google Analytics cookies, used to track a user's visits to the website (pages visited, files downloaded etc). These are created and controlled by Google Analytics.	All analytics cookies require express consent on entering site
Personalization_id	This is a cookie put in place by Twitter to allow personalisation of twitter feeds.	"Features-led consent" would probably suffice although the term is not defined by the ICO. In this instance, the site could make clear wherever the option to Tweet a page appears that Twitter will deploy cookies if users access this feature. While this does not fully meet the requirements of consent in the GDPR definition, it is the approach ICO take with their Vimeo feeds and therefore seems a proportionate response. However it would be more robust to seek consent, possibly through adding social media cookies to the options provided in the main cookie consent form. An alternative risk avoidance approach would be to simply remove "Tweet this page"/Twitter button functionality. A similar approach would be appropriate for third party cookies deployed by Vimeo, as used by ICO here: https://ico.org.uk/for-organisations/training-videos/
Style	This is created by the design templates and is used to keep a consistent text size for users who have selected a smaller or larger text size using the "AAA - Text Size up | Down" links.	The ICO states in their guidance that such cookies are likely to be able to rely on the necessity exemption: "**User preference - Likely to meet an exemption? - Yes, depending on purpose limitation.** Session cookies used to store a user's preference can rely on the strictly necessary exemption, provided they are not linked to a persistent identifier... The exemption may in some cases also apply to persistent cookies but the user must be given sufficient information in a prominent location - for example, cookies used as part of a cookie consent mechanism, which remember the user's cookie preferences over a period

		of time (eg 90 days), can be exempt." https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply13 We would therefore suggest that no consent is required, particularly if the cookie is for the session only. If OSIC is not comfortable with that position, this may be seen as n example of "settings-led" consent as set out above.
Content	This is created when the cookie banner at the top of the page is read and closed, and is used to stop this message from appearing on other pages after the message has been closed.	Necessary to the function and to ensure (in compliance with GDPR recital 32) to ensure that consent requests are not unnecessarily disruptive. No consent required.
SIC	This is a user session cookie, used for keeping a user logged in as they navigate around the website. NOTE: this is only created when a user logs in to the website. If the site does not have a private area that users need to log in to, then this will only be created for SIC staff who are website administrators	Not deployed to external users. No consent required
Editor_PinTBActive	Added for SIC staff website editors only, used to indicate if the page editor is pinned in place or not. This will not be written out to any non-CMS users.	Not deployed to external users. No consent required
ASP.NET_SessionID	Used to identify the user's session on the server. The session being an area on the server which can be used to store data in between http requests. Used to maintain an anonymised user session by the server	Necessary to the functionality. No consent required.