Implementer Guide to Privacy & Electronic Communications Regulations (PECRs) for public sector websites

This document sets out guidance from the Government Digital Service (GDS) to government departments and other public sector bodies which are required to comply with the new Privacy & Electronic Communication Regulations (PECR) which came into effect in May 2011.

This guidance builds on existing guidance provided by COI in May 2011 and updated guidance from the Information Commissioner's Office (ICO) issued in December 2011. This guidance focuses on ensuring that the main objective of the new regulation, the protection of website users' online privacy, is satisfied by public sector websites.

This guidance is for information only. Website owners are responsible for ensuring their own compliance with the updated PECRs.

Background

Following changes to PECRs in May 2011 all website owners with a UK presence, are now required to obtain informed consent from website users and subscribers in order to store information on their devices. The primary impact of these changes for websites is that only cookies (and related technology such as HTML5 local storage) that are deemed 'strictly necessary' for a service requested by the user are exempted from this requirement.

The ICO guidance material considers some methods for obtaining user consent such as pop-ups. However, these can be quite disruptive to the user experience and are likely to make the sites less usable. Website owners should consider how opportunities for users to provide consent can be maximised without undermining usability.

The preferred method of compliance with the new regulations i.e. least disruptive to the user experience, would be one based on users' "implied consent". In this context "implied consent" can be taken to mean that a user is aware of the implications of taking a certain action and that by choosing to take such action are implicitly giving their consent to the related outcomes. However, the ICO does not believe it is possible to take such an approach at present because "evidence demonstrates that general awareness of the functions and uses of cookies is simply not high enough for websites to look to rely entirely in the first instance on implied consent ".

This emphasises the need to raise the awareness levels amongst users of government websites about the uses and functions of cookies. Consistency in the presentation of cookies-related information will help towards achieving the aim of educating users, so this document sets out a recommended template for departments' 'Use of Cookies' policy

Transparency about which cookies websites set and why remains central to the ICO

requirements and consequently to this guidance.

Recommendations for Website Owners

The initial measures public sector websites should undertake in order to protect users' online privacy (which is the main objective of the new guidelines) and raise awareness levels are set out below.

1. **Undertake a comprehensive audit of cookies**
   All government departments, their agencies and relevant NDPBs must complete a comprehensive audit of the cookies and related technologies used by their sites and their usage. Where it is not possible for a department's web team to definitively list all the cookies (both first- and third-party), an external organisation can be commissioned to carry out an audit.

   This audit should determine the intrusiveness (in privacy terms) of each cookie. A table to help you do this is attached (*ANNEX 1*).

   You should publish the results of this audit on your website as part of your 'Cookies Policy'. Some examples of best practice are included to help you do this (*ANNEX 2*). Links to this policy should be made prominent. You should consider options for publicising this policy e.g. through news articles or on-site promotion.

2. **Look to reduce unnecessary and redundant cookies**
   Website owners should look to remove unnecessary or redundant cookies based on their level of intrusiveness. Removal of the more intrusive cookies in this category should be prioritised.

3. **Establish effective management of cookies**
   Website owners should ensure ongoing, effective management of cookies across their websites. This should include a procedure to prevent the creation and use of new cookies without an assessment of their value (in terms of user experience / analytics etc) weighed against their intrusiveness.

   Regular checks of cookies should be undertaken and the published list of cookies updated to ensure that a user will never find a cookie in their device that is not listed.

   Data-sharing and benchmarking options (offered by some analytics packages) should be switched off despite the fact that no personal data is collected.

Please note that the PECRs cover any technology that store or retrieves information from the users' computer. This includes cookies, HTML5 local storage and locally stored objects (Flash cookies).

Other steps towards compliance

The wide and varied uses of cookies means that many different stakeholders must be involved in finding the best routes to compliance, including considering in the longer term alternatives to cookies in website management. The ICO has been supportive of this type of multi-stakeholder engagement. In recognition of this GDS will seek to work with DCMS to:

- Engage in discussion with various vendors of Analytics packages in order to monitor industry developments which may facilitate compliance with the new privacy regulations.

- Continue to monitor and promote the efforts of major Internet browser vendors to develop products which help users indicate their consent to the setting of cookies by a website.

ANNEX 1: Cookie Intrusiveness Guide

Intrusiveness	**Functionality Types**
Moderately intrusive	- Embedded third-party content and social media-plugins - Advertising campaign optimisation
Minimally intrusive	- Web analytics / metrics - Personalised content / interface
Exempt from changes to privacy regulations	- Stop multiple form submissions - Load balancing - Transaction specific

Website owners should focus their efforts when reviewing, and where necessary revising the use of cookies, on the most intrusive types. This approach reflects the balance between valuable use cookies (e.g. for analytics and improving the user experience which enable continual improvement of digital services) and the need to protect users' privacy.

Rationale - 'Moderately Intrusive'

Limited control over used of information: Website owners have no direct control over how the information stored within third-party cookies is used. While all attempts should be made by web managers of government sites to provide information about relevant third-parties' cookie policies, it is probable that users will have a more convoluted journey in attempting to access this information. This might result in users not accessing the information thereby reducing their understanding of how cookies work and reducing the opportunity of providing informed consent.

User expectations when visiting the first-party site: A visitor to any first-party site has a relationship primarily with the site they have visited. Consequently, it is unlikely that visitors have an expectation that other parties might also be able to store information on their terminals. The setting of third-party cookies might be considered particularly intrusive when, in theory at least, they enable third-party websites e.g. Facebook, to track user behaviour across several sites. The fact that the visitor does not have to click on the plug-in or be a member of the social media networking site for the cookie to be set on their device, increases the perception that they are particularly intrusive.

Rationale - 'Minimally Intrusive'

Their usage *tends* to be controlled by the first-party and as such departments are able to be fully clear and transparent about how the cookies and the information stored in them are set and

used respectively

The scope of their use and information they store are limited to the first-party websites i.e. they are not used in relation to a user's activities on other sites.

Use of web-analytics/metrics: The use of metrics are integral are to departments' being able to provide the best possible user experience in order to encourage citizens to use more cost-effective channels for accessing government services. They also allow departments to assess and demonstrate whether the digital services they offer provide "value-for-money" as demonstrated by the recent National Audit Office (NAO) report.

Consequently, collecting these metrics are essential to the effective operation of government websites, at present the setting of cookies is the most effective way of doing this.

The ICO guidance supports this view as it states "...it is highly unlikely that priority for any formal action would be given to focusing on uses of cookies where there is a low level of intrusiveness and risk of harm to individuals. ***Provided clear information is given about their activities we are unlikely to prioritise first-party cookies used only for analytical purposes in any consideration of regulatory action***"

Personalised content/interface: Consistently presenting users with the version of the site (or features within the site) which they find most convenient increases their enjoyment of the site and thus, the likelihood that they'll use the service/website in the future.

ANNEX 2: Examples of Good Cookie Policy Pages

The following are examples of existing good cookie policy pages:

- https://www.gov.uk/help/cookies
- http://www.culture.gov.uk/4902.aspx
- http://www.consumerfocus.org.uk/cookies