Important Notice:

This Cookies Guidance Summary is made available on an 'as is' basis. L2 Cyber Security Solutions cannot take any responsibility for the consequences of errors or omissions. Any reliance you place on this document will be at your own risk. The documentation that is linked to, in this document, to the Data Protection Commission's website, should be considered the full official guidance.

Neither L2 Cyber Security Solutions, nor its employees are liable for any losses or damages arising from your use of this document. These individuals and organisations exclude all warranties and representations, express or implied, in respect of your use of this document.

COOKIES GUIDANCE SUMMARY:

Why are cookies a data protection concern?

A couple of recent court rulings in the EU have brought a new focus on how cookies are used and abused by websites. Effectively these rulings have determined that cookies may not be placed onto a website user's computer/device without getting their explicit, informed consent beforehand.

The Irish Data Protection Commission (DPC) carried out an analysis of 39 different websites and made the findings available here:

https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Data%20Protection%20Commission%20cookies%20sweep%20REVISED%2015%20April%202020%20v.01.pdf

As a result of that report, the DPC issued guidance for website owners. They gave a grace period of 6 months from the issue date, before they would start enforcement action against websites that did not adhere to that guidance. This enforcement will commence from October 2020.

This document summarises that guidance, with the full article available here:

https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf

I've got a cookie banner on my site, so I'm OK – right?

The cookie banner needs to be very clear about the type of cookies your website uses and for certain types, it must ask for consent before those cookies can be placed on the computer/device.

The cookie banner should also have a link to much more detailed, granular information about the cookies, so the website user can be more informed about them.

You can have different types of cookies:

- Strictly necessary

  These would be for things like language preference, or for remembering a shopping basket. These are permissible without getting consent, but full details need to be provided about these cookies.

- Analytics

  These are for measuring people's visits to the site, where they came from, where they are located, etc. These would require consent.

- Advertising/Marketing/Tracking

  Anything that targets or tracks a user, including "pixels" from social media and other advertising sites, will require consent.

- Chatbot

  If your website has a Chatbot feature, no cookie should be set until the user explicitly requests the chatbot function.

As a default, the cookie banner should have no cookies pre-ticked (strictly necessary are considered OK).

The cookie banner should also have a link to the Data Protection Statement (AKA Privacy Statement).

You can show the current consent setting for each of the different types on a cookie banner, but the user must have the ability to go in and consent or reject individual cookies within each type.

First party cookies are set by the website domain. These are generally less likely to cause data protection concerns, but if they are to be used for things like analytics, then consent should still be obtained before they are set.

Third party cookies are used where there are various other companies with whom information might be shared, these must be listed individually and the user allowed to consent or reject consent to each one individually. There should also be an accept all or reject all option available. These include social media like buttons.

There should be no attempt to "nudge" the user towards giving consent to all cookies by way of conflicting language or use of prominent coloured button that might appear to be the correct one to click to proceed. This is known as using a "dark pattern".

The use of colours to indicate consent on the cookie banner and cookie consent page needs to be considerate of people who suffer colour blindness. Use text rather than colour to indicate the consent.

The button that should be available to click in the cookie banner will be to accept the cookies as currently set by the user.

Any consent given by the user will have a lifespan of 6 months, after which the user must be prompted to give their consent again.

Cookie lifespans should be proportionate for what they are needed for. You shouldn't set "forever" cookies.

The user must be able to access the cookie settings at any time to be able to vary their consent.

I've told website visitors to use browser settings to control cookies.

This is not an appropriate way to enable a user to accept cookies or not.