HOW TO ACHIEVE COOKIE COMPLIANCE

Prepared by Alan Mac Kenna, Data Protection & Cyber Risk Team
UNDERSTANDING COOKIES, CONSENT & COMPLIANCE

WHAT ARE COOKIES?

Internet cookies are small text files that are used to save information related to a user’s activity on a website or app. As well as being used to provide users with a more personalised experience, they can also be used to track a user’s activity across the various online services that they use.

WHAT IS COOKIE CONSENT?

Legal requirements for cookie processing have been in place for some time now. However, in recent years, court rulings and guidance from data protection authorities have further clarified these requirements, particularly in relation to when website operators must ask for consent to process cookies.

- Consent must be obtained for any storage of or access to information on users’ devices, unless the processing falls within a narrow exemption.
- Consent should be gained for each processing purpose
- Consent needs to be freely given, specific, informed and unambiguous
IS IT JUST **COOKIES** THAT ARE IN SCOPE OF THESE REQUIREMENTS?

No – the legal requirements apply to cookies and *similar technologies*. ‘Similar technologies’ that would come within scope include pixel trackers, browser fingerprinting, and the use of local storage, among others. Requirements are also not limited to the context of website processing – mobile device applications also need to be considered.

IS CONSENT **REQUIRED** FOR ALL TYPES OF COOKIES?

Website operators use cookies for varying purposes.

**Strictly necessary:** Necessary cookies enable core website functionality such as security network management and accessibility. They are required for the website provider to provide the intended service to the website user.

For example, a cookie that enables a website to provide shopping cart functionality is a strictly necessary cookie. This is because it would not be possible to provide the user with the online shopping service they are requesting, without such processing.

Strictly necessary cookies do not require consent.
Other purposes (such as Analytics, Social features, Marketing): Analytics cookies are an example of a type of cookie that enables website operators to collect information about how people use their website – for example, the number of users on a website, how long they stay on the site for, and what parts of the site they visit. These services are often provided by third parties (e.g. Google), embedded into the website. Analytics cookies require consent.

WHAT IS COOKIE COMPLIANCE?

Cookie compliance is measured by whether or not website operators are in line with cookie processing requirements set out by ePrivacy Regulation, and meet the standard of GDPR transparency and consent. Compliant websites satisfy regulatory requirements and data protection authority guidance, giving users adequate information and control over how their data is collected and processed using cookies and similar technologies. Conversely, non-compliant websites are those that do not give their users sufficient information and control over cookie processing.
WHY IS COOKIE COMPLIANCE IMPORTANT?

The goal of implementing these requirements is to protect the fundamental rights and freedoms of individuals who access information services. Users must be able express their informed consent, indicate which cookies they allow website operators to use, and which they do not. Failure to comply can result in enforcement action being taken, including monetary fines.

PROCESSING SPECIAL CATEGORY DATA (E.G. HEALTH DATA, RELIGIOUS AFFILIATION)

Depending on the context of your service offering (e.g., healthcare), or the third-party services that you have integrated into your website, you may be processing special category data. Explicit consent is required for the processing of special categories of personal data, which is unlikely to be met by means of a cookie banner alone. Website operators should take account of the context in which they are operating when assessing what compliance means for them.
CONSENT MANAGEMENT PLATFORMS

Cookie Consent Management Platforms (CMP) can be used to provide website users with information and control over the reasons that a website processes cookies and similar technologies.

For a CMP to achieve compliance it must:

- **Explain** each purpose for processing
- Only process non-strictly necessary cookies **after** the user has affirmed their consent
- Allow users to alter their consent after setting their preferences
- **Facilitate expiring** the users consent after a defined period
- Allow users to read the privacy and cookie policy, **without** first setting cookies
- **Avoid pre-checked boxes** and sliders that default to enabled
WHAT DOES COMPLIANCE LOOK LIKE?

Cookie Banner: Do’s

- Inform users about the purposes for which cookies are used
- Give users clear and equal options to accept or reject cookies
- Allow users to either affirm their acceptance or further manage their cookies
- Make sure cookie banners do not obscure access to privacy or cookie policies
Cookie Banner: Don’ts

The banner only presents users with a single option, such as “Accept”, without the ability to express their preference. This does not give users the opportunity to provide freely given, specific, informed and unanimous consent.

- Use nudging techniques to encourage the user to accept cookies
- Only give users a single option such as “Accept”, "OK" or “Got it”
WHAT DOES COMPLIANCE LOOK LIKE?

Cookie Management: **Do’s**

- Give users control over each processing purpose (e.g. Marketing, Analytics)
- Enable “strictly necessary” cookies by default
- Set reasonable expiry dates on cookie consents (DPC recommends 6 months)

The banner presents as a tool showing all the cookie processing purposes, enabling the user to toggle them on or off as preferred.

“Strictly Necessary” cookies are enabled by default. The user cannot turn these off.

Should the user wish to find out more details, or manage their preferences regarding individual cookies, they can do so by clicking “DETAILS” and expanding the relevant section.

Manage Cookies

We use cookies to improve your experience on our site, understand how visitors use our site and show you personalised advertising. To find out more, you can read our privacy policy and cookie policy. You can manage and learn more about your cookie preferences below.

- **Strictly Necessary**
  - These are necessary to provide you with our services.

- **Functional**
  - These provide functionality on our site such as remembering your preferences or embedding external videos.

- **Analytics**
  - These provide us with statistical information to better understand how visitors use the website.

- **Marketing**
  - These cookies are used to track visitors across websites. The intention is to display ads that are relevant and engaging for the individual user and therefore more valuable for publishers and third party advertisers.
Cookie Management: Don’ts

- Include pre-checked boxes and sliders
- Enable cookies that are not strictly necessary by default

The banner presents as a tool showing all the cookie processing purposes. However, this banner enables all cookies by default, even those that are not strictly necessary. This does not give users sufficient opportunity to provide freely given, specific, informed and unanimous consent.
WHAT DOES COMPLIANCE LOOK LIKE?

Just-in-time consent: Do’s

✔ If a user has not previously given consent for a particular cookie (e.g. viewing a video embedded via a third-party service), it is recommended to seek the user’s consent at a point that makes it easier for the user to put into context why you are asking for it. In the case above, this is at the point the user can view an embedded video.

✔ The user may decide to enable the cookie, learn more about its processing or further manage their cookie preferences.
ADDITIONAL CONSIDERATIONS

USING A LAYERED APPROACH

Website operators are required to provide clear and comprehensive information about the cookies they are using, and the purposes for which they are being used.

A layered approach (see below) presents cookie options, allows users to consent by purpose, and provides an ability to drill down for more information and control over individual cookies.
COMMON CHALLENGES

Website operators face common challenges in implementing compliant cookie processing.

- **Bridging the gap** between legal requirements and technical implementation
- **Validating compliance** – having assurance that what the CMP tool is reporting as being configured is actually reflected in the processing that is occurring
- **Multiple digital partners / web properties** – An organisation may have more than one website in their portfolio and use multiple digital agencies to manage those properties. Difficulties achieving compliant cookie processing can arise due to differences in the technologies used to deliver those web properties and the tools available to provide consent management. Consistent engagement with the various stakeholders is key.
- **Ongoing compliance** – once cookie compliance is achieved, it takes effective policies and procedures to ensure that compliance is maintained going forward, as those web properties evolve.
RECOMMENDATIONS:

- Involve all relevant stakeholders that have an interest in the organisation’s website when addressing cookie compliance;
- Ensure you have access to expertise that understands how the legal requirements need to be translated into technical implementation;
- Validate that a user’s choices are being respected, not solely relying on what the Consent Management Platform tool is reporting;
- Develop a consistent policy for the organisation’s digital agency partners to follow, to ensure effective governance over cookie processing going forward.

CONCLUSION

Data protection authorities are poised to take action on website controllers who are not compliant with cookie processing. Controllers are advised to take stock of their processing in this area and review policies, procedures and measures taken to ensure adequate compliance.

We can help you

If you require assistance navigating compliance with processing related to cookies and similar technologies, Trilateral offers a range of data governance services that can help your organisation meet these requirements and maintain ongoing compliance.

Our support services will help your business to protect individuals’ fundamental rights, building trust among your users and ultimately, your customers.

To learn more, please contact: dcs@trilateralresearch.com