Confused by EU cookie rules? The ICO and CNIL are here to help (sort of)

John O'Brien, Senior Associate at Reed Smith LLP, examines recent guidance on cookies from the ICO and CNIL, highlighting how they diverge, and what organisations should do whilst the uncertainty continues

No privacy issue confuses EU organisations more than the rules governing the use of cookies on websites. Companies consistently struggle with this area of law, which is unsurprising, as EU Member States continue to have different regulatory approaches and laws for cookies. For those that have become used to the (relative) harmonisation of the GDPR, grappling with disparate national cookies laws can seem utterly bewildering.

Many are also keeping a wary eye on the future. The long heralded e-Privacy Regulation continues to grind its way through the EU's opaque legislative process. At the time of writing, we have no fixed date for when the finalised text of the new Regulation will be published. This means that, for now, organisations must continue with the EU's patchwork cookies governance regime under the increasingly outdated e-Privacy Directive (2002/58/EC).

In this article, we examine some recent guidance on cookies from the UK and French data protection regulators. We also set out some basic rules for organisations using cookies in the EU. These rules are not a panacea for your company's cookie compliance ills. However, they will ensure that you have a defensible case, should a regulator ever come knocking.

Britain versus France

July 2019 saw both the British and French regulators ('ICO' and 'CNIL' respectively) issue detailed cookies guidance. As always with guidance from different national regulators, there are some overlaps and some divergences.

It is clear from the guidelines that both regulators take the view that where consent is required to drop a cookie, user consent must meet the GDPR's standard. This means that consent is specific, free, informed and unambiguous. It also means that consent is given before cookies are dropped.

For consent to be informed, users must be able to identify all parties who place cookies on their device. This means that an organisation's cookies policy needs to clearly explain if its websites drop cookies on behalf of third parties.

Both the ICO and the CNIL are consistent that merely continuing to browse websites does not constitute valid consent from users for cookies to be dropped. Nor can organisations rely on users' browsers settings to obtain consent for cookies: although both regulators believe that browser settings may be adapted in the future in a way that allows them to collect valid consent, for now, companies cannot direct customers to amend their browser settings if they want to opt out of cookies being dropped.

Neither regulator is a fan of consent for cookies being bundled into website terms and conditions. Users should provide consent for each purpose that companies use cookies. Both regulators accept that organisations can offer 'global' consent for all cookies for which consent is required. However, the CNIL requires a second layer of consent that allows users to give specific consent for each purpose separately.

The CNIL envisages offering companies a grace period of six months to get their houses in order. This period will only start once the CNIL issues its final opinion, currently expected in the first quarter of 2020. The ICO does not envisage any similar grace period.

Other divergences between the ICO's and CNIL's guidance include:

Cookie walls: This approach sees companies block access to their websites unless users agree to cookies being dropped. The CNIL believes that cookie walls are never compliant. The ICO is much less black-and-white in its analysis, stating that consent gathered through cookie walls is 'unlikely to be valid'. However, it also notes that the GDPR must be balanced against other rights, including freedom to conduct business.

Consent for analytics cookies: The ICO believes that analytics cookies always require user consent, without exception. The CNIL, on the other hand, states that certain analytic cookies do not require consent if they meet a list of specific CNIL requirements. The ICO stated that it is unlikely to commence enforcement proceedings against companies using analytics cookies without user consent if 'there is a low level of intrusiveness and low risk of harm to individuals'.

Copies of the guidelines:

ICO: www.pdpjournals.com/docs/888002

CNIL: www.pdpjournals.com/docs/888003

Lifespan and retention period: Analytics cookies that benefit from the CNIL exemption set out above can be set for 13 months. The CNIL does not set a specific retention period for other cookies. The ICO states that cookies' lifespans must be proportionate in the context of their intended purpose.

Rules of thumb

If your company uses cookies, do:

- make sure the consents you collect meet the GDPR standard;
- provide users with clear information about the cookies being dropped before they consent;
- clearly and specifically name any third party companies that drop cookies on your websites, and explain what they will do with the information they collect;
- give users control over the dropping of any non-essential cookies;
- allow users to continue accessing your website even where they do not consent to the dropping of non-essential cookies;
- ensure that information about how you use cookies and how users can make decisions about the cookies you use are as easily accessible as possible to users;
- strike a balance between a thorough description of the cookies you use and your users' ability to understand how you use cookies; and
- provide more detailed information about your cookies in a separate cookies policy that can be accessed by users from your cookies consent mechanism, cookies banner, or through a prominent position on your website.

Conversely, when using cookies, make sure you do not:

- drop non-essential cookies before users give their consent;
- use pre-ticked boxes or sliders defaulted to 'on' to obtain consent;
- bundle consent for cookies into website terms and conditions or other contractual language;
- rely solely on users' browser settings to obtain consent; or
- include long tables or detailed lists of all cookies operating on your website when there are dozens of them. Instead, it is more transparent and accessible if you provide a more general overview of the type of cookies you use.

Plus ça change?

The guidance issued by the ICO and the CNIL does not contain any startling new requirements or information. However, they clearly demonstrate the piecemeal nature of regulation in this area.

Companies may read each set of guidance and wonder if it is worth their time updating their cookies strategies now. The temptation exists to wait for the introduction of the new e-Privacy Regulation. Why undertake a big compliance project now, if the rules are likely to change in the near future?

Unfortunately, we simply do not know when the e-Privacy Regulation will finally make it to the statute books. This means that delay is not the most pragmatic approach for companies weighing up their cookies compliance strategies. Now that GDPR has bedded down, regulators are starting to turn their attention to e-Privacy matters like cookies and electronic marketing. We can expect more active regulatory enforcement in this area over the next year.

In practical terms, this means that organisations must now tailor their strategies to align with regulators' cookies guidance. This could mean defaulting to the strictest requirements across the EU, or picking and choosing approaches from country to country. As with practically all areas of privacy and data protection law, there is no 'one size fits all' approach. The correct approach for your organisation will depend on its scale, resources, reliance on cookies, risk appetite, and locations throughout the EU.

It is clear that by issuing guidance, both the CNIL and the ICO intended to support companies that use cookies. However, the publication of both sets of guidance almost contemporaneously serves to highlight the different approaches of two of the EU's biggest regulators. When it comes to cookies regulation in the EU, it seems that the more things change, the more they stay the same.

John O'Brien is leading a Workshop on 'Breach Notifications — What's Required in Practice' at the 18th Annual Data Protection Compliance Conference taking place in London on 10th and 11th October 2019. See www.pdpconferences.com for further details.

John O'Brien
Reed Smith LLP
jobrien@reedsmith.com