

## The regulators have made it clear: you need to update your website cookies pop-ups and policies

12 SEPTEMBER 2019

CATEGORY:  
[ARTICLE](#)



As [previously discussed](#), after admitting the unlawful use of cookies on its own website, on 3 July 2019 the UK Information Commissioner's Office ('ICO') changed its cookies consent mechanism ([see graph](#)) and issued [a new guidance on the use of cookies](#), also applicable to any other tracking technologies.

The guidance confirms what we already know about 'consent' under the GDPR. Whilst none of its contents are surprising, it is nevertheless controversial. According to this guidance, the majority of operating websites today serve cookies unlawfully. For example, the legality of all of the following has been explicitly rejected:

- 'By continuing to browse our website you agree to our use of cookies.' – according to the guidance, statements such as this one cannot justify the use of cookies. As user consent cannot be implied such statements are insufficient to obtain valid consent. Yet, according to SimilarWeb, over 80% of the top 15 websites worldwide in the world use precisely this type of language.
- 'Everyone is using cookies for analytics so we can't possibly need consent for that.' Whilst the guidance appreciates the beneficial information analytics providers give to website operators, it nevertheless finds such information 'non-essential' for the delivery of the website. Thus, placing this type of cookies requires 'informed' consent provided by 'affirmative action'. According to various estimates, over 30 000 000 websites around the world use Google analytics.
- 'Fine – we will provide users with choice, but the default choice will be 'cookies on.' According to the guidance, the default cookies settings need to be put to 'off', meaning that if a user ignores a cookie banner or accepts its default settings, website operators will lose the benefit of online advertising revenue and analytics insights, the opportunity to deploy social media and cross-device tracking and the ability to embed third party videos and social media plug-ins.

The ICO dismisses any allegation that it wants online services to stop using cookies as simply 'a myth'.

The guidance goes into great level of detail in explaining how to comply with the requirements in practice. Whilst this is indeed helpful, some of the practical examples are arguably draconian. For example, the ICO suggests that even where a website provides users the opportunity to reject cookies, if that 'reject' button is smaller than the 'accept' button, then this is a non-compliant approach as the website is allegedly influencing users towards the 'accept' option. Apparently the same holds true even for larger 'reject' buttons when hidden behind a 'more information' button. On the other hand, the ICO suggests that website operators need to ensure their cookies banners are 'responsive' and adaptable. Message boxes designed for desktop view are allegedly unsuitable for use in mobile view and incapable of providing the required transparency information, meaning consent obtained by non-responsive cookies banner on mobile is invalid.

Of course none of the above makes sense if the law is not going to be enforced by the 700-strong team in Wilmslow. However, the ICO's press release suggests enforcement in the area will be an 'increasing regulatory priority'. The authority advises businesses to start working towards compliance 'now'. We too recommend clients start preparing for compliance with the ICO's advice, particularly in light of the trends picking up speed across the Continent.

The French data protection authority, the CNIL, also repealed its former cookies guidance and issued a new one. According to the authority's [23 July 2019 press release](#), the main novelties that echo the ICO's findings are twofold:

- scrolling down or swiping through a website or application can no longer be viewed as a valid expression of consent to the implementation of cookies.

- stakeholders who operate tracking technologies must be able to prove that they have obtained the consent.

The CNIL has also been clear about enforcement. The authority is now entering into consultations with stakeholders on the practical aspects of implementing the guidance and after these are completed, and a further recommendation is issued, businesses will be given six more months to comply. The French regulator looks determined to start enforcing the law in the summer of 2020.

The French and British regulators were not the only authorities to issue statements or guidance on cookies. Their guidance was preceded by cookies-related announcements from Slovenia, Germany and the Netherlands issued earlier in the year. The Slovenian data protection authority intends to abolish implied consent for cookies. A German regional data protection authority categorised a mere notification that a website uses cookies to improve browsing experience, or for web analytics and advertising as 'insufficient and misleading'. The Dutch authority confirmed that making access to a website conditional on accepting cookies cannot constitute valid consent.

The Italian data protection authority, on the other hand, has not yet revised its 8 May 2014 guidelines on cookies (supported by brief online FAQs) which, in essence, reflect the formerly acceptable implied consent standard for marketing and profiling that can be satisfied by a cookies banner and the statement that the continuation in browsing by the user is taken as a valid consent.

This being said, the operators practically adapted to implementing a system of consent granting based on the "accept" or "ok" button.

However, given the abovementioned trends in cookies set by the other European authorities we expect that the Italian data protection authority will too tackle the issue and revise its outdated guidance in the immediate future.

## Conclusion

All across Europe regulators seem to be in agreement on the issue of cookies. The authorities appear to be discharging their duty of clarifying the requirements of the GDPR and pointing to practical steps for compliance. Whether or not the industry agrees with the suggested steps to achieve compliance may prove irrelevant, given the regulators' determination to start enforcing the law the way they see fit.

Withers tech regularly helps clients comply with their regulatory requirements and gives advice that works for business. Our clients range from start-ups to large multinationals and in addition to the full spectrum of data protection advice we can give, we can offer the full service for all your legal needs. For more information, please contact [Richard Penfold](#), [Ashley Williams](#), [Yancho Yanchev](#), [Jacopo Ronchi](#), [Jacopo Liguori](#) or any other member of the firm's [data protection team](#).

# Authors

## Ashley Williams

SENIOR ASSOCIATE | LONDON

Intellectual property and technology

 +44 20 7597 6843

 [ashley.williams@withersworldwide.com](mailto:ashley.williams@withersworldwide.com)

## Jacopo Liguori

SPECIAL COUNSEL | MILAN

Intellectual Property and Technology

 +39 02 8821 4204

 [jacopo.liguori@withersworldwide.com](mailto:jacopo.liguori@withersworldwide.com)

## Jacopo Ronchi

ASSOCIATE | MILAN

Intellectual Property and Technology

 +39 02 8821 4284

 [jacopo.ronchi@withersworldwide.com](mailto:jacopo.ronchi@withersworldwide.com)

## Yancho Yanchev

DATA PROTECTION SPECIALIST | LONDON

Intellectual Property and Technology

 +44 20 7597 6673

 [yancho.yanchev@withersworldwide.com](mailto:yancho.yanchev@withersworldwide.com)