
UK ICO and Article 29 Working Party Weigh in on Proposed ePrivacy Regulation

APRIL 13, 2017

While companies prepare for the EU General Data Protection Regulation (GDPR) to take effect in May 2018, another highly significant item on the agenda is arguably the current review process of the [proposal for a Regulation on Privacy and Electronic Communications](#) (ePrivacy Regulation). Last week, the UK Information Commissioner's Office (ICO) and the Article 29 Working Party (Working Party) both released key information on the process and substantive issues that will ultimately shape the final version of the ePrivacy Regulation:

- On April 4, 2017, the Working Party issued an [opinion](#) on the proposed ePrivacy Regulation, stating that it “welcomes” the European Commission’s current proposal, which was unveiled on January 10, 2017, but that the Working Party is “highly concerned” about four key areas related to:
 - The tracking of the location of terminal equipment (such as via Wi-Fi or Bluetooth);
 - The conditions under which the analysis of content and metadata is allowed;
 - The default settings of terminal equipment and software; and
 - “Tracking walls.”
- On April 6, 2017, the ICO published a [blog post](#) highlighting the upcoming process for ePrivacy reform and the ICO’s role in drafting and providing guidance on the proposal.

As we have [previously noted](#), the ePrivacy Regulation—which would repeal and replace Directive 2002/58/EC (commonly known as the “ePrivacy Directive” or “Cookie Directive”)—will have far-reaching impacts on the electronic communication sector and other online companies, including: websites, mobile apps, and other online services; third-party service providers (e.g., advertising, analytics, and other online technology providers); web browser and other software providers; and telecommunications and electronic communications services. Accordingly, companies may want to think strategically about how such changes will affect their businesses and consider reaching out to local data protection authorities that may play an active role in shaping the final draft, such as the ICO.

UK ICO Blog Post on ePrivacy Reform Process

In its [blog post](#) describing the process for overhauling the ePrivacy Directive, the ICO notes that the ePrivacy Regulation is due to come into effect in May 2018 alongside the GDPR. Accordingly, the next step is for the European Parliament and European Council to review the draft and come together at the end of this year to negotiate the final text. The ICO also summarizes some of the ePrivacy Regulation's major changes from current law, including that:

- It removes separate security obligations, which will be covered under the GDPR, but introduces customer notification of specific security risks.
- In terms of cookies and other online tracking devices, the focus shifts from website cookie banners to users' browser settings, and seeks to address issues around ad-blocking and Wi-Fi location tracking.
- It tightens the rules on marketing, with the default position being that all marketing to individuals by phone, text or email must be opt-in.
- It incorporates the GDPR's two-tier system of fines of up to €20 million, or 4% of worldwide turnover, for breaches of some parts of the Regulation.
- It would apply to services providing so-called 'over-the-top' communication channels over the internet, such as Skype, Facebook Messenger, or WhatsApp. It would also apply to businesses providing customer Wi-Fi access, as well as the traditional telecoms and internet providers.
- It would apply to organizations based anywhere in the world if they provide services to people in the EU.

The ICO indicates that it will be responsible for enforcement in the UK and therefore has been playing an active role in shaping the proposal to date. The ICO plans to issue an initial guidance document later in the year, to highlight key issues under the proposed ePrivacy Regulation.

Article 29 Working Party Opinion on Proposed ePrivacy Regulation

The Working Party's [opinion](#) on the proposed ePrivacy Regulation states that it "welcomes" the current proposal, but it urges that the ePrivacy Regulation be strengthened in four key areas where the Working Party has "grave concerns":

1. **The tracking of the location of terminal equipment (such as via Wi-Fi or Bluetooth).** The opinion recommends that the final ePrivacy Regulation: (a) require companies to obtain consent to track individuals' physical movements; (b) impose clear limitations on the scope of collection and processing of personal data (including hashed MAC addresses); (c) require an opt-out if tracking occurs in certain circumstances where personal data will be anonymized at a later time; and (d) promote the development of technical standards for devices to automatically signal an objection to such tracking.
2. **The conditions under which the analysis of content and metadata is allowed.** The opinion states that metadata and content from electronic communications are both "highly sensitive" and that consent should be obtained from *all end users (i.e., sender and recipient)* prior to processing metadata and content, with limited exceptions where it is "strictly necessary" to carry out certain processing activities. Notably, however, the opinion states that it should be possible to process electronic communications data for the

purposes of providing services explicitly requested by an end-user—such as search or keyword indexing functionality, virtual assistants, text-to-speech engines, and translation services—if the end-user requesting the service provides consent and the processing is limited to such purposes.

3. **The default settings of terminal equipment and software.** The opinion states that, in the view of the Working Party, “terminal equipment and software must *by default* discourage, prevent, and prohibit unlawful interference with it and provide information about the options.” Importantly, the Working Party takes the view that requiring software providers to require end-users to consent to a setting upon installation is not enough—instead, the opinion states that “terminal equipment and software must *by default* offer privacy protective settings, and guide users through configuration menus to deviate from these default settings upon installation.”
4. **Tracking walls.** The opinion calls for the ePrivacy Regulation to explicitly prohibit “tracking walls” where access to a website or service is denied unless individuals agree to be tracked on other websites or services. The Working Party believes that such “take it or leave it” approaches are rarely legitimate and that “individuals’ ability to access content online should not be dependent on the acceptance of the tracking of activities across devices and websites/apps.”

The opinion also suggests that the scope of the ePrivacy Regulation should be clarified to ensure that it provides an **equal or higher level of protection than the GDPR**. Finally, in addition to the “grave” concerns listed above, the opinion raises several other concerns and clarifications with respect to the current draft, including concerns about the territorial and substantive scope, the protection of terminal equipment, and direct marketing.

Implications for Businesses

At this point, it is not clear whether—and to what extent—the Working Party’s concerns will be addressed in the final draft of the ePrivacy Regulation. However, it is likely that the final draft will address at least some of the “grave” concerns listed above. Accordingly, companies may want to think strategically about how such changes will affect their businesses and consider reaching out to local data protection authorities that may play an active role in shaping the final draft, such as the ICO.

Authors



**Dr. Martin
Braun**

PARTNER

✉ martin.braun@wilmerhale.com

☎ +49 69 27 10 78 207