PUBLICATION

Beyond GDPR: EU's ePrivacy Regulation to Add New Layer of Data Obligations

Authors: Andrew Jacob Droke
June 29, 2018

While many were focused on the May 25, 2018 enforcement date for the European Union's General Data Protection Regulation (GDPR), the Council of the European Union has continued its efforts to finalize the ePrivacy Regulation (ePR), which will replace the E.U.'s ePrivacy Directive and present certain new obligations when navigating the E.U.'s cybersecurity and privacy framework with respect to electronic communications.

On May 28, 2018, in response to the latest working draft of the ePR (available here) and the mid-May meetings of the Working Party on Telecommunications and Information Society and the Working Party on Information Exchange and Data Protection, the European Data Protection Board (EDPB) published a statement (available here) addressing the importance of the ePR and the need to finalize it "as soon as possible."

The EDPB explained that the confidentiality of electronic communications requires specific protections beyond those afforded by the GDPR and expressed its support of the ePR's broad prohibitions, narrow exceptions, and consent requirements. The EDPB also stated that the ePR must enforce the consent requirements for cookies and similar technologies and ensure that users' choices are considered, regardless of the technical means involved. The EDPB opined that privacy settings should facilitate expressing and withdrawing consent in an easy, binding, and enforceable manner.

On June 5, 2018, the Presidency of the Council of the European Union published a status report discussing those issues yet to be finalized, including the specific interplay between the protections afforded by the ePR and the GDPR as well as the processing of electronic communication metadata. Based on these issues, the ePR may not be finalized before Austria assumes the Presidency from Bulgaria on July 1, 2018. Nevertheless, in light of the EDPB's comments, U.S.-based companies must begin to understand how their compliance obligations under the ePR will intersect with their current operations and their obligations under the GDPR. Providers and users of electronic communications services not currently governed by the ePrivacy Directive will likely be included within the ePR's broad scope.

Who and What are Covered?

The ePR is intended to strengthen the protections afforded to electronic communications and to both clarify and enhance certain aspects of the GDPR. Importantly, the ePR will expand the E.U.'s current ePrivacy framework to include new and emerging messaging technologies (e.g., application and Internet-based messaging services that are functionally equivalent to traditional text and voice communication methods) in order to address aspects of the ePrivacy Directive that have "not fully kept pace with the evolution of technological and market reality." As noted by the EDPB, "extending protections to functionally equivalent services, including so called 'Over-the-Top' services is an essential element of the reform." The restrictions will also apply to text messages (SMS and MMS), telephone calls, VoIP calls, machine-to-machine communications (connected/smart devices), and email correspondence.

To that end, the ePR, in its current form, will primarily regulate the activities of two large groups: (1) those who *provide* electronic communications services (including certain public Wi-Fi networks, even when password protected), publically-available directories, and software that permits electronic communications; and (2) those who *use* electronic communications services to send direct marketing communications, to make use of the processing or storage capabilities of an end user's terminal equipment (including cookies), or to collect information from an end user's terminal equipment. The ePR will apply as soon as the data is collected, regardless of whether the user has created an account for the service.

Importantly, for U.S.-based companies, the ePR will apply if the affected, live human end user is located in the E.U. It does not matter where the processing occurs or where the provider/processer is located.

What is Required/Prohibited?

The current requirements and prohibitions imposed by the ePR fall into two primary categories: (1) those addressing the protection of end users' communications and the integrity of their terminal equipment; and (2) those addressing end users' rights to control their electronic communications. At a high level, the ePR addresses the following issues with respect to users' communications and equipment:

Confidentiality. The ePR generally prohibits any interference with the content and metadata of electronic communications. The prohibited conduct includes listening to, tapping, storing, monitoring (including observing website activities), scanning, surveilling, intercepting, and processing this information. As a result, without user consent, service providers are only permitted to process the data in limited ways (such as for security purposes). As noted by the EDPB, the consent requirements under the ePR correspond to those imposed by the GDPR and "access to services and functionalities must not be made conditional on the consent of a user." The EDPB has also taken the position that "there should be no possibility under the ePrivacy Regulation to process electronic communications content and metadata based on open-ended grounds, such as 'legitimate interests', that go beyond what is necessary for the provision of an electronic communications service." Further, even when consent is obtained, the ePR's introductory recitals suggest that any processing should be limited to the purposes and durations contemplated by the user.

Requirement to Delete/Anonymize. The ePR requires providers of electronic communication services to erase or anonymize electronic communications content after the message is received by the intended recipient and to erase or anonymize the associated metadata once it is no longer needed for transmission purposes (with a limited exception for billing purposes). The ePR acknowledges that the time of receipt will depend upon the technology employed and that, in turn, the confidentiality and deletion obligations will also depend on the specific nature of the messaging system.

Protection of Equipment. The ePR includes provisions designed to protect end users' terminal equipment, including a general prohibition on both (a) using the processing and storage capabilities of users' terminal equipment; and (b) collecting information from the equipment. Thus, although certain exceptions apply, the ePR will typically require user consent and a specific and transparent purpose to support the use of any cookies or trackers. As noted above, the ePR's consent requirements mirror those imposed by the GDPR.

Application Privacy Settings. The ePR mandates that software, including Internet browsers, include features designed to give users the option to prevent third parties from storing or processing information (including cookies) on their machines. The current draft would require the software to be user-friendly and to remind users of the privacy settings in certain instances. The EDPB further noted that the "settings should preserve the privacy of the users by default, and they should be guided to choose a setting, on receipt of relevant and transparent information." Although a browser-level control could make end users' selections more efficient, it would not obviate the requirements imposed for providers of covered services.

In addition to these provisions affecting users' communications and terminal equipment, the ePR includes the following protections with respect to end users' right to their control of electronic communications:

Number-based Interpersonal Communications. The ePR incorporates certain protections with respect to number-based communication systems. In particular, service providers must offer users, free of charge, the ability to block Caller ID information and certain calls (with limited exceptions for emergency communications). The ePR also specifically requires providers of these services to "deploy state of the art measures to limit the reception of unwanted, malicious or nuisance calls by end users." Providers of number-based services would also be required to obtain user consent before listing an individual's personal data in a publically available directory.

Direct Marketing Communications. Perhaps more importantly to most U.S.-based companies, the ePR generally prohibits the sending of direct marketing communications via electronic communications services without user consent. Direct marketing communications include any form of advertising communicated by voice-to-voice calls (live calls not using automated systems), communications made via automated calling/communication systems (with or without human interaction), emails, text messages, and messages via functionally-equivalent apps or other techniques. It does not, however, include advertisements displayed to the general public on websites that are not directed to a specific end user.

Despite prohibiting the sending of direct marketing communications without consent, the current draft of the ePR would permit those who receive contact information in connection with a sale of goods or services to use that contact information to send marketing communications so long as the user is given an opportunity to object at the time the contact information is provided and in each future marketing communication. The future correspondence must, however, be limited to the sender's own similar products or services, and E.U. member states may adopt time limits addressing how long the seller can use the information.

Further, even with permitted communications, senders will be obligated to state their identity, to use effective return addresses and numbers, to inform users of the marketing nature of the communication, to state the name of the individual or entity on whose behalf the communication is being made, and to give end users the opportunity to object to receiving future marketing communications. The method for objecting or withdrawing consent must be easy to use, free, available at any time, and effective. Additional restrictions apply to direct marketing calls.

Enforcement and Penalties

Similar to the GDPR, the current draft of the ePR includes a bifurcated penalty structure in which violations are subject to either (a) a maximum penalty equal to the greater of €10M or two percent of global revenue or (b) a maximum penalty equal to the greater of €20M or four percent of global revenue. Violations of the provisions addressing confidentiality of communications, permitted processing of data, and the time limits for erasure are subject to the larger cap. Member states' supervisory authorities are vested with enforcement authority, and the ePR grants a private right of action to end users.

Next Steps for U.S.-Based Companies

Because the ePR remains in draft form and may be revised prior to implementation, U.S.-based companies must continue to monitor the ongoing efforts to finalize the ePR. Additionally, organizations should begin to determine the scope and nature of their communications with end users in the E.U., review the controls currently in place, and develop strategies for adjusting those processes. Taking these steps now will enable companies to more efficiently implement the required controls upon finalization of the ePR. Please contact Andrew Droke or a member of Baker Donelson's GDPR Team for additional information or assistance.