McKinsey & Company

Risk Practice

What will Europe's e-privacy regulation mean for your business?

The ePrivacy Regulation, an elaboration of the GDPR, has been moving closer to adoption; beyond preparing for compliance, smart companies can find business advantages

by Daniel Mikkelsen, Henning Soller, and Malin Strandell-Jansson

September 2019

As companies continue to scramble to implement the requirements of the European Union's 2018 General Data Protection Regulation (GDPR), another set of data-protection obligations has appeared on the horizon. Europe's ePrivacy Regulation is in an advanced stage of preparation and is expected to replace the 2002 Privacy and Electronic Communications Directive (known as the ePrivacy Directive) by late 2019 or early 2020. Its focus is on privacy protection for data when they are transmitted electronically, and its status as a regulation (rather than a directive) means that it can be uniformly enforced across EU member states.

Many executives have not paid much attention to the new regulation, whether because it has yet to be enacted or they believe it will not apply to their businesses. In our view, the inattention is ill advised. In broad terms, the regulation specifies how the general data-protection framework outlined in the GDPR[1] will be applied to electronic-communication services provided over telecom networks and the internet. The regulation will apply to direct marketing sent over electronic-communication networks, an activity most companies engage in. It will also apply to the providers of electronic-communication services—such as the presentation and retrieval of information on the internet—and to the providers of the software and directories that support these services.

In the making, the new regulation has been highly contentious and one of the most lobbied proposals in the history of the European Union. One concern is that the introduction of a regulation targeting a specific set of companies could put these companies at an unfair disadvantage to those not subject to this regulation. Another concern is that the provisions of the new regulation could come into conflict with those of the GDPR. EU member states have also expressed fears that the regulation could limit innovation.

Despite the controversy, most market analysts believe the regulation will be enacted, and any company using electronic communications will have to monitor developments and prepare to meet the requirements. Penalties for infringement will be steep, with a top fine of 4 percent of worldwide revenues or €20 million, whichever is greater. In response, smart leaders will take a strategic view. They will work to help shape the new regulation and develop policies and practices to support compliance along the entire customer journey, especially in direct-marketing activities.

The key elements of the new regulation

The new ePrivacy Regulation will repeal and replace the EU's current e-privacy directive (exhibit). The new provisions will cover electronic-communication networks; data stored in or sent from end-user equipment such as phones, tablets, and computers (including cookies, device IDs, and other identification software); and methods employed to approach customers over electronic-communication networks for direct-marketing purposes.

The most important aspects of the new provisions are summarized as follows:

Data processing

The GDPR set out a list of general lawful purposes for data processing, namely vital interest, legal obligation, contractual necessity, legitimate business interest, public interest, and other purposes with the data subject's consent. While some of these purposes, such as the protection of vital and public interests (including statistical use and scientific research), are being considered for inclusion in the ePrivacy Regulation, the new regulation mainly takes a different approach. It will define specific requirements for different forms of usage.

For example, the use of cookies will require consent except when the cookies are necessary for transmitting data, providing a requested service, or measuring a web audience. This means that all marketing-related cookies will require consent. Consent will also be required for metadata

[1] For more detail on the General Data Protection Regulation (GDPR), see Daniel Mikkelsen, Henning Soller, Malin Strandell-Jansson, and Marie Wahlers, "GDPR compliance since May 2018: A continuing challenge," July 2019, McKinsey.com.

Exhibit

The European Union's uniformly enforceable ePrivacy Regulation will replace an older directive and augment the GDPR in protecting the privacy of data sent electronically.

Change	Current ePrivacy Directive	New ePrivacy Regulation
Automatically applies	**Member states must adopt into law** the 2002 directive for it to become applicable	**New regulation is directly applicable and enforceable** without being adopted into member-state law
Covers internet companies	Personal data are processed in connection with the provision of **publicly available electronic-communication services**	**Broader in scope,** including providers of electronic-communication networks or services
Covers metadata	**Covers communications data (including traffic data) but not metadata**	**Covers both content and metadata,** including cookies, online identifiers, search engines, directories, and direct marketing
Stricter cookie rules	**Customers must opt in** for information stored in the electronic-communication network or in terminal equipment (eg, cookies), except for transmitting or facilitating transmission, or if strictly necessary to provide a service explicitly requested by the user	**Consent is required throughout,** except for the provision of requested services, antifraud measures, security, software updates, or statistical purposes (eg, web-audience measuring) Cookie settings should be allowed in the browser settings
Stricter rules on marketing calls	**Users have control** over line identifications, call blocking, and call forwarding **Direct marketing is not allowed without consent** (B2C, B2B for member states to decide), except to existing customers; must **opt out from directories**	**Marketing calls must be clearly identifiable** as such, from the phone number or otherwise **Consent is required for inclusion in directories,** barring a national exception
More efficient enforcement	**Enforcement at the national level;** fines vary and are often rather low	**GDPR-specified uniform enforcement across member states;** fines of up to 4% of worldwide revenue

used in digital marketing, unless it is being used for purposes related to service quality, billing, interconnection, or fraud prevention. In addition, the ePrivacy Regulation has stricter consent requirements than the GDPR. Under current plans, it will require companies to contact customers twice a year to remind them of their right to opt out or withdraw their consent, whereas the GDPR does not specify an opt-in/opt-out schedule.

If the new regulation is approved in its current state, its impact is likely to be significant. All major companies use cookies—whether their own or from a third party—to improve their marketing. Cookies allow companies to target advertising to specific groups and analyze visitor traffic and behavior on their websites. According to a joint report from the Reuters Institute for the Study of Journalism and the University of Oxford, based on an analysis of 500 popular sites conducted in early 2018, more than 60 percent of websites had at least one third-party cookie per page; news sites had an average of 81 per page.[2] A subsequent study by the same team noted that the number of advertising and marketing cookies on news sites fell by 14 percent between April 2018 (before the GDPR was implemented) and July 2018 (shortly after implementation).[3]

[2] Timothy Libert and Rasmus Kleis Nielsen, *Third-party web content on EU news sites: Potential challenges and paths to privacy improvement*, a joint report from the Reuters Institute for the Study of Journalism and the University of Oxford, May 2018, reutersinstitute.politics.ox.ac.uk.
[3] Timothy Libert and Lucas Graves, *Changes in third-party content on European news websites after GDPR*, a joint report from the Reuters Institute for the Study of Journalism and the University of Oxford, August 2018, reutersinstitute.politics.ox.ac.uk.

Direct marketing
Direct marketing via email and telephone also requires consent unless contact takes place within an existing client relationship for a similar type of product. As before, companies need to offer customers an easy way to opt out of direct marketing every time they are approached. The regulation recommends that individual countries introduce "do not call" registers that companies must check before approaching individuals. It also requires that marketing calls use a specific prefix or code that makes them identifiable as such. Those making marketing calls must also identify the legal entity or individual on whose behalf they are calling.

Control and confidentiality of communications
The ePrivacy Regulation strives to maintain individuals' control over communications through provisions that are broadly similar to those in the directive it is intended to replace. Individuals have the right to block certain numbers and be excluded from public directories. They can also decide on privacy settings for telephone, computer, and internet communications. Electronic communications in the form of data, metadata, and voice recordings need to be treated as confidential and cannot be disclosed without consent or the presence of a legal obligation. This also applies to machine-to-machine or Internet of Things communications over electronic networks, and to public Wi-Fi communications.

Integrating data privacy into corporate strategy

All signs indicate that the new regulation will deepen the impact of the GDPR on most companies. The GDPR is already having a dramatic effect: our research indicates that marketing activities in Europe have declined by 10 percent since it was introduced. Some companies are struggling to address their existing customer base, with opt-in ratios of only 20 percent or lower. The ePrivacy Regulation will put even stricter rules in place.

Faced with such a challenging situation, companies need to address the new regulation with urgency while maintaining a strong focus on their business. To prepare for success under the new regulation, companies can consider taking the following actions:

Set up a cross-functional team that involves marketing. Marketing should be a key stakeholder in the implementation program. When programs are run by the legal or compliance function alone, they tend to focus purely on compliance. Cross-functional teams deliver the best results by looking for solutions that fit the company's overall business strategy as well as meeting customers' needs.

Take an active role in developing the regulation. Companies should engage in industry dialogue to assess the real-world impact of the provisions and propose best-practice solutions to safeguard

Cross-functional teams deliver the best results by looking for solutions that fit the company's overall business strategy as well as meeting customers' needs.

end-user privacy while also fostering innovation and market development. Online companies have already managed to secure the removal of a provision on preinstalled cookie settings in browsers that could have adversely affected business models based on online advertising. Leaders need to analyze the impact of the proposed regulation on their business and treat measures to safeguard data privacy as an opportunity to strengthen their branding and turn compliance investments into a form of strategic marketing. At the same time, they need to avoid taking steps that might incur unnecessary costs or hinder business development.

Optimize customer journeys to obtain consent to future contact. Our experience suggests that low-involvement marketing methods such as direct mail and untargeted email campaigns rarely achieve opt-in rates above 20 percent. Such low levels of consent make it difficult for companies to engage with potential new customers or cross-sell to existing customers. However, opt-in rates can reach much higher levels with the right choice of consent strategy and formulation of consent notices. We have seen companies achieve rates as high as 80 to 90 percent by offering customers easy and convenient ways to opt in at every touchpoint along the customer journey and by making them feel they have something to gain from future contact.

Make privacy a competitive differentiator. Privacy is a relative newcomer to top management's strategic agenda, so companies should seize the chance to evaluate what business opportunities the new requirements may create. For example, the right of portability, established under the GDPR, and the stricter control over direct marketing and directories could open up markets to competition and allow the development of new offerings in areas such as open banking, privacy and security solutions, comparison platforms, and intermediary services that help customers find a trusted provider or switch to a new provider. Marketing and legal departments can also work together to make privacy notices and consent requests stand out, not only to improve opt-in ratios but also to enhance customer perceptions and support business building.

The e-privacy regulation about to come into force in Europe is part of a broader trend that is spreading to Latin America, Asia, and the United States. Successful companies will not only take timely steps to comply with the regulation but will also treat data privacy as an integral part of corporate strategy. By assessing the possible impact of the regulation, developing a clear and comprehensive road map for addressing it, and managing business implications carefully, companies can turn the regulation from a burden to an opportunity.

Daniel Mikkelsen is a partner in McKinsey's London office, **Henning Soller** is a partner in the Frankfurt office, and **Malin Strandell-Jansson** is a senior expert in the Stockholm office.