
# ePrivacy Regulation: Has Europe Gone Mad?

**Compliance and Ethics**


Cookie Use
We use cookies to ensure that we give you the best experience on our website. If you continue, we assume that you consent to receive all cookies on our website.
OK
More Info


Cookie Use
We use cookies to ensure that we give you the best experience on our website. If you continue, we assume that you consent to receive all cookies on our website.
OK
More Info

## CHEAT SHEET

- ***The new age.*** The European Commission is becoming increasingly focused on ensuring stronger online privacy protection, simpler rules for cookies, and transparent marketing via phone, email, or text.
- ***In the process.*** The draft regulation intends to apply to three types of service categories: (1) internet access, (2) interpersonal communications, and (3) other services comprising wholly or mostly of signal conveyance.
- ***Level of consent.*** Recent changes to ePrivacy regulations in the European Union state that privacy will be guaranteed for both content and metadata. This means that all data must be deleted or anonymized unless otherwise provided with the end-users' consent.
- ***Back to market.*** Under the proposed ePrivacy regulations, end-users are to be provided with the ability to identify, block, and unsubscribe to marketing communications.

It seems that every time we turn around, a country, regulator, or legislator in Europe is issuing a new law, rule, directive, guidance, or legislation that changes (and strengthens) the way companies handle personal data. The newly proposed Regulation of Privacy and Electronic Communications (the ePrivacy Regulation) is no different. We saw a leaked draft back in December, shortly followed by an official draft in January 2017. The ePrivacy Regulation will replace the existing Directive 2002/58/EC (also known as the Cookie Laws). The update is intended to harmonize current ePrivacy laws and ensure that they align with the General Data Protection Regulation (GDPR), with an ambitious effective date of the May 25, 2018 — the same effective date as the GDPR.

Please note that the General Data Protection Regulation is a set of overarching laws for data protection, whereas the ePrivacy Regulation only addresses electronic communication and would thus align within the parameters of the GDPR.

This onslaught of data regulations is a direct response to our rapidly changing digital environment and its attendant societal evolution. Until recently, the European Union has approached data protection through directives, with great deference to individual member states. This is because a directive has to be implemented into each member state through its own national laws. As a result, companies operating in Europe currently have to navigate a tangled web of 28 different national laws and regulatory hurdles.

More guidance will be forthcoming from the data protection authorities. Law firms have already started issuing guidance.

In recent years, we have seen a variety of efforts toward harmonization, such as creating standard contractual clauses for cross-border data transfers out of Europe and implementing a mutual recognition process for binding corporate rules (another data transfer mechanism) that eliminate the need for individual review of the application by each member state.

The latest of these harmonization efforts is the ePrivacy Regulation. In short, this proposed regulation will broaden the scope of the current directive to capture new technologies, like the Internet of Things

and communication apps (referred to as “over the top” (OTT) content providers including Voice over IP, email, and short message services/texting), as well as strengthen the rules and protections that apply to electronic marketing, the use of cookies, and similar tracking technologies.

## Rationale of the ePrivacy Regulation

The European Commission has issued a fact sheet that states that the “objective is to reinforce trust and security in the Digital Single Market.” The goal of the larger Digital Single Market Strategy is to increase the public’s trust in digital service security. This strategy initiative identified the ePrivacy Directive as one element of the digital market that needed updates to provide adequate data protection for individual users. It also leveled the playing field within the electronic communications market, given the prevalence and market strength of some large and well-known companies.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final.

The European Commission states that:

> More and more Europeans use services such as Skype, WhatsApp, Facebook Messenger, Gmail, iMessage, or Viber to send messages. However, the current ePrivacy rules only cover traditional telecoms providers. To ensure that Europeans’ electronic communications are confidential, regardless of the technology used, the proposed rules will also apply to internet-based voice and internet-messaging services. Privacy is guaranteed for communication content, as well as metadata (e.g., time of a call and location), which have a high privacy component and needs to be anonymised or deleted if users do not give their consent, unless the data is needed for billing.

The European Commission is therefore clearly focused on ensuring stronger online privacy protection, simpler rules for cookies (the complexity around companies’ complying with “cookie rules” has made the rules nearly unenforceable), and transparent marketing via phone, text, or email.

## Scope and enforcement

The draft regulation applies to “the processing of *electronic communications data* carried out in connection with the provision and use of *electronic communications services* and to information related to the terminal equipment of end-users.” The key definitions here are electronic communications data and electronic communications services.

“Electronic communications data” means electronic communications content [the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound, include voice activated devices], and electronic communications metadata [data processed in an electronic communications network for the purposes of transmitting, distributing, or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration, and type of communication].

“Electronic communications services” include those services provided in the exchange for remuneration via electronic communications networks. However “remuneration” does not necessarily require financial payment, but can include any exchanged benefit, such as access to a contact list or a geolocation. Companies should note that this includes instances where providers automatically collect data, such as through cookies. Similar to the scope of GDPR, this provision essentially includes nearly all websites and applications.

Particularly, the draft regulation is clear that it is intended to apply to three types of service categories:

1. Internet access;
2. Interpersonal communications; and,
3. Other services comprising wholly or mostly of signal conveyance (i.e., machine-to-machine communications or broadcasting).

The proposed regulation therefore extends the scope of the current ePrivacy Directive to reach both traditional telecommunications firms and internet service providers, as well as those online services which are “functionally equivalent,” like the OTT providers mentioned earlier.

Recital 11 of Regulation.

OTT includes services like Skype, iMessage, Facebook messenger, and Viber. And the proposed regulation reaches even further to Internet of Things (IoT) and machine-to-machine communications — so your remote garage door opener, smart toaster, and pet-cam will be covered. Therefore, regulatory oversight and compliance obligations for ePrivacy communications, under the proposed ePrivacy Regulation, will apply not only to obvious electronic communications, but also to those not-so-obvious ones as well.

To align with the GDPR, the proposed fines for non-compliance can (for the more severe offences) reach to the higher end of four percent of a company’s gross global revenue or €20 million. Similarly, the enforcement arm stretches to entities who do business in the European Union — including those that provide electronic communication services or gather electronic communication data from European end-users’ devices. Interestingly, the end-users can be either natural persons or legal persons (i.e., companies).

It remains to be seen if the inclusion of legal persons carves a chance for entities to initiate complaints against their competitors, as well as consumers against corporations — as consumers/end-users will have the same remedies as the GDPR. These remedies include the right to lodge a complaint with the entity in question and with supervisory authorities, the right to request effective judicial remedies, and the right to seek compensation and damages.

**European General Data Protection Regulation**

The General Data Protection Regulation (GDPR) is a broad set of data protection requirements that were initially proposed by the European Parliament, the European Council, and the European Commission in 2012. It is intended to replace the current Directive 95/46/EC, which has resulted in a spider web of compliance requirements across the 28 member states. Proposed in January 2012, GDPR faced hundreds of amendments before finally being adopted in April 2016. It currently has an effective date of May 2018. It is anticipated that the new requirements under the GDPR will create

approximately 75,000 new jobs in privacy, because the GDPR will apply to all controllers and processors established in the European Union, as well as to those doing business involving personal data on natural persons in the European Union. This greatly expands the jurisdiction of the Data Protection Authorities in the European Union, as penalties are expected to rise to €20 million, or four percent of worldwide gross revenue. See here for more information on the GDPR.

## Key provisions

The European Commission presents the proposed regulation in three main sections: updates to current rules, simpler rules for cookies, and stronger rules on marketing calls.

### Updates to current rules

As discussed above, the updates mainly attempt to address the changes in both society's use of electronic communications and technological advances. The rules are also updated to reflect the different types of data that comprise electronic communications.

Given that electronic communications data (data) includes both content and metadata (such as the time, length, and location of the communication), the proposed regulation addresses the processing of data when necessary for the purposes of the intended communication and for keeping data secure by detecting errors, ensuring quality control, and maintaining functionality. However, there are distinct and separate rules for content and metadata.

The European Commission states that through this proposed regulation, privacy is "guaranteed" for both content and metadata — "which have a high privacy component and need to be anonymised or deleted if users did not give their consent, unless the data is needed for billing." In the current directive, the term "traffic data" is used instead of "metadata." Essentially, all data must be deleted or anonymized, unless end-users expressly consent to its continued use or it is being temporarily used for limited purposes and then deleted or anonymized. These limited purposes include transmission, security, and the detection of faults in either transmission or security.

As a result, intercepting data is allowed only with the consent of end-users and for specific, transparent purposes. The biggest change here is that for consent to be valid, it must now meet the high bar for consent set by the GDPR (i.e., it must be "unambiguous"). This more stringent prohibition against interception (with the heightened consent requirement) is yet another way the authorities are trying to control the growing technology capabilities, such as advertising technology, including targeted behavioral ads that monitor users' online behavior.

However, the proposed regulation does expand the permitted uses of content data by allowing for the use of consent both if the processing is necessary, or for other purposes if anonymity prohibits those purposes. In the latter scenario, the regulation will only expand the permitted uses if the provider has consulted with the data protection authorities before engaging in the processing. Metadata is similarly restricted to necessary processing (quality, billing, calculating payments, detecting/preventing fraud, or for the abuse of services) or for other purposes if anonymous information prohibits the use (no prior consultation with authorities is required). However, once the other purpose has been accomplished, the metadata must then be erased or anonymized.

## Simpler rules for cookies

Cookie consent requirements have been one of the most frustrating data protection requirements for companies to consistently follow and maintain across the European Union. An online search for “cookie consent” yields many, often conflicting, articles on what to do. This proposed regulation aims to simplify without reducing this requirement, while maintaining an expected standard of personal data protection.

See Recital 21 of Regulation.

# There is still a cookie consent requirement

In-house counsel should note that there is a new exemption for first party analytic cookies — not third party analytic cookies. First, the “party” specifically refers to the service provider and not to the domain from which the cookie is loaded, unless the provider and the domain are the same entity. This is yet another route that the proposed regulation aims to address regarding digital advertising technology. Keep this narrow exemption in mind when reviewing the information provided below on simplifying cookie rules. However, as is the case under the current rules, non-privacy intrusive cookies will not require consent, such as those strictly required to operate the website.

The proposed regulation also wants browser providers and similar software providers (vs. website owners) to provide cookie controls to end-users (along with other tracking technology controls). As part of the initial set-up and readily available for future changes, end-users should be given choices on cookie consents. This may mean the end for the seemingly endless parade of cookie banners that we now see — and may take the burden off of website owners and onto software and browser providers. Existing software will require updates to the new user-friendly cookie control. Implied consent, which has become the market standard for obtaining cookie consent in the absence of meaningful enforcement to the contrary, seems to be eliminated as an option.

Additionally, device information, such as IMSI (International Mobile Subscriber Identity), IMEI (International Mobile Equipment Identity), and MAC (media access control) is prohibited other than for establishing the connection unless a “clear and prominent” notice that meets the GDPR requirements is clearly visible and user-friendly. The proposed regulation provides for the possibility that such notices may be provided by means of standardized icons. This is eerily reminiscent of the “do not track” efforts that have been in place for several years and remain largely ineffective.

### Value of personal data online

Personal data is often referred to as the “oil of the 21st century.” Why? How much personal data is collected online and what is it worth? Data brokers, which are companies that collect and sell personal information, have been around for years. However, with digital data, “big data,” and the “Internet of Things,” the business model for data brokers is simply unimaginable to the average consumer. Data brokers, such as Acxiom (who reported a revenue of US$850 million for 2016) collect about 1,500 data points per person on 500 million consumers, through 23,000 servers. There are about 4,000 data brokers worldwide. Can you think of 1,500 things about yourself individually? And once data brokers collect data points about you, you are placed in categories, such as single parent with income over US$50,000, individual with enormous credit card debt, expectant mother, soon-to-be retiree whose kids live in another state, etc. These profiles give a company enormous

marketing opportunities. And these lists are updated weekly. The data comes from the online searches you make, the loyalty card programs you participate in (from about 1,400 companies), and social media. They even compile lists of people with medical problems, including those with allergies and cancer patients — none of which is protected because the data brokers do not obtain the information from entities that are regulated by the government (in the United States or many other countries). The US Federal Trade Commission has issued reports on data brokers and has called for regulatory control or at least more transparency. So how much is your information worth? A single email might be US$79. A marketing profile for one person to one company, bought in batches of 1,000, costs about US$5 per person. But the broker selling that data sells it to multiple companies, builds on it, sells it again, year after year — depending on your interests, lifestyle, income, buying patterns, and about 1,495 other data points. Your profile could be worth thousands of dollars over time and basically costs nothing to compile.

### Stronger rules for marketing calls

This area will be one of the more straightforward requirements of the proposed regulation. In general, the requirements remain the same for opt-in consent for electronic communications. The ability to rely on “soft opt-in” consent for marketing similar products or services in the context of a sale to existing customers remains. For marketing calls, the big change are those OTT services, robocalls (automated calls), etc. In particular, the proposed regulation seeks to control the wide range of communication channels now in use (and those that can be developed) given the technological advancements, such as instant messaging, in-app delivery, and SMS. End-users are to be provided with rights and the ability to identify marketing communications, block marketing communications, and easily unsubscribe to marketing communications.

## Next steps

If your company is addressing GDPR, build in this newly proposed regulation. You may wind up undoing some changes you’ve made in the past few years, but in most cases, you will be adding these new requirements into your action plan for European operations.

#### What can a company do to prepare for EU data protection regulations?

The ePrivacy Regulation is simply the latest in a series of steps that the European Union has taken to increase data protection on its citizens. Given the extraterritoriality of the GDPR and the other regulations either proposed or in scope, there are tens of thousands of companies impacted. What should these companies be doing to prepare?

First, pay attention. Does the GDPR or any other data protection regulation apply to your company? Many companies (in and out of Europe) are blithely unaware of the coming regulations.

Then, once you have determined (most likely) that you are subject to the regulations (and this does not mean just the GDPR), take deliberate steps to bring your privacy program and business processes into compliance. Unless you have a mature and well-defined privacy program, it will likely take you months, if not years, to come into compliance. Here are some common actions that will help

you comply with EU data protection regulations:

- Perform a data inventory and mapping — know what data you have and where it is (this includes cookies);
- Get rid of personal data that you do not need;
- Appoint a privacy officer — one that knows privacy laws;
- Give that privacy officer the authority and independence to take action;
- Assess/change business processes around personal data collection, use, and sharing (this means data on employees, general consumers, vendors, customers, and likely your customers' customers);
- Review and amend your privacy policies, including your online privacy policy;
- Protect personal data in motion and at rest; and,
- Implement and strengthen your vendor oversight program.

These will get you started on compliance with the ePrivacy Regulation, the GDPR, and other European data protection initiatives. Many companies need expert help with these processes, so ensure that your executives understand the importance of dedicating both funds and resources to these efforts. Most likely, it will cost less to properly fund a program than it will to pay the potential fines.

K Royal

Global Chief Privacy Officer

Crawford & Company

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.