

Your World First

C/M/S/

Law.Tax

The new ePrivacy Regulation

How will it impact your business?

January 2017



The new ePrivacy Regulation: how will it impact your business?

With the GDPR on the horizon, the EU is now overhauling and expanding the reach of the more specific privacy rules which relate to direct marketing, cookies and other forms of online monitoring. The ability of social media and messaging services to track users is one of many areas touched on in the European Commission's newly proposed ePrivacy [Regulation](#), which was officially [unveiled](#) last week. We highlight some key impacts for the tech and media sectors, provided the proposed draft passes through the legislative process without dramatic changes. Businesses should incorporate these new requirements into their GDPR readiness planning.

Why are the rules being updated?

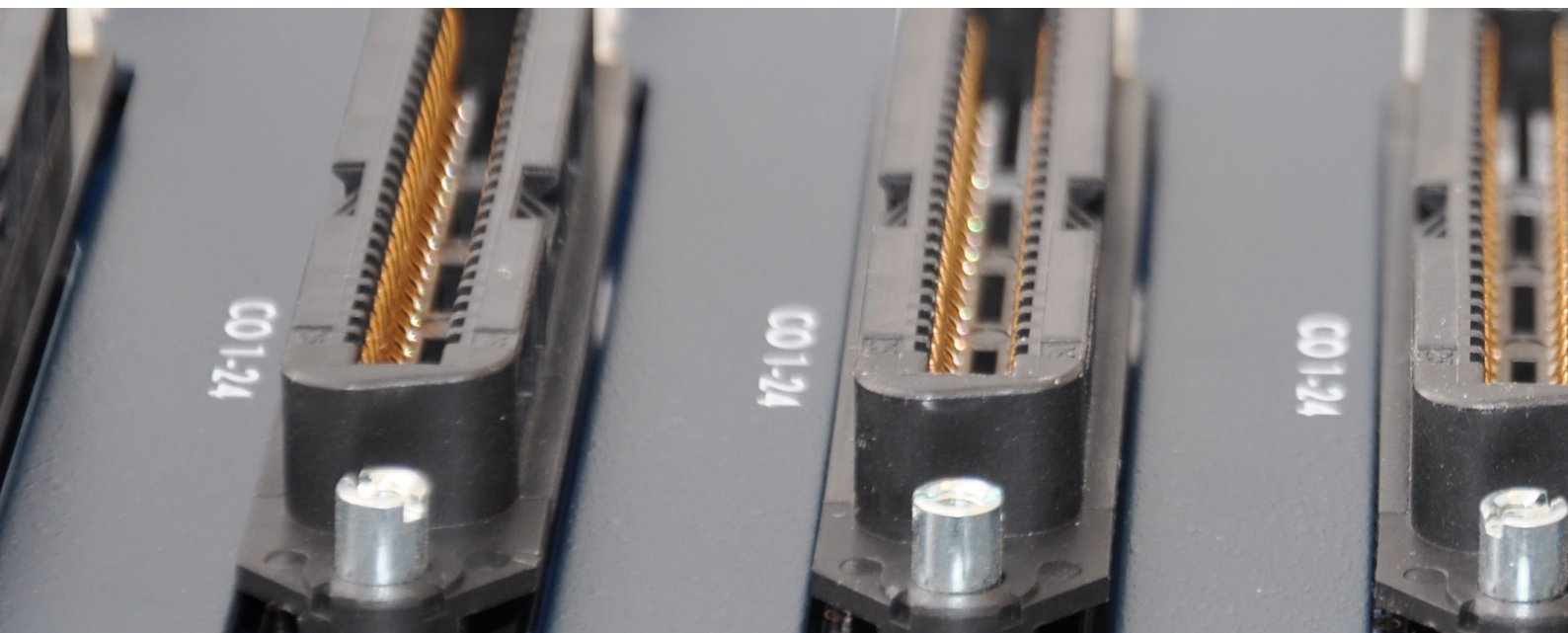
The regime for electronic communications, based on the EU's Privacy and E-communications Directive ([PECD](#)), which dates back to 2002, is being overhauled as part of the Commission's [Digital Single Market](#) package.

- Since the last review of the PECD in 2009, a new typology of players has emerged offering communication services that many end-users perceive as comparable to traditional electronic communications services such as telephone calls and SMS messaging.
- These new players, so-called Over-the-Top communications services ("OTTs") (e.g. Skype, Gmail, WhatsApp), are generally not subject to the current EU electronic communications rules (although often voluntarily comply); the Regulation is proposing to change this.
- The proposed new rules are designed to align with the stricter new general privacy rules under the GDPR (drawing on certain definitions and concepts used in

that Regulation), which will come into force in 2018. Like the GDPR, the proposed new e-communications rules would take the form of a directly effective Regulation, to help iron out differences in different EU Member States.

When will the new e-privacy rules come into force?

The Commission's aim is for the Regulation to apply from 25 May 2018; purposely the same date as the GDPR comes into force. However, as the proposal is at the start of the Brussels legislative process this may be overly ambitious. Being narrower in scope, it is unlikely to take as long to adopt as the GDPR, but there may be some areas of contention. In particular, representatives from the European Parliament have already mentioned disappointment that the consent requirements are not stricter and could look to push back on this. We will be tracking the Regulation's progress.



Which current EU and UK rules will the Regulation replace?

- In terms of EU law, the Regulation will repeal the PECD - its current relationship with the regulatory framework of electronic communications (likely to soon be replaced by the European Electronic Communications Code) will be maintained by the new Regulation.
- In the UK, the Regulation will repeal the 2003 Privacy and Electronic Communications (EC Directive) [Regulations](#). This assumes that the rules take effect before Brexit and, in the same way as the GDPR, that post-Brexit, the UK continues to adhere to EU style rules.

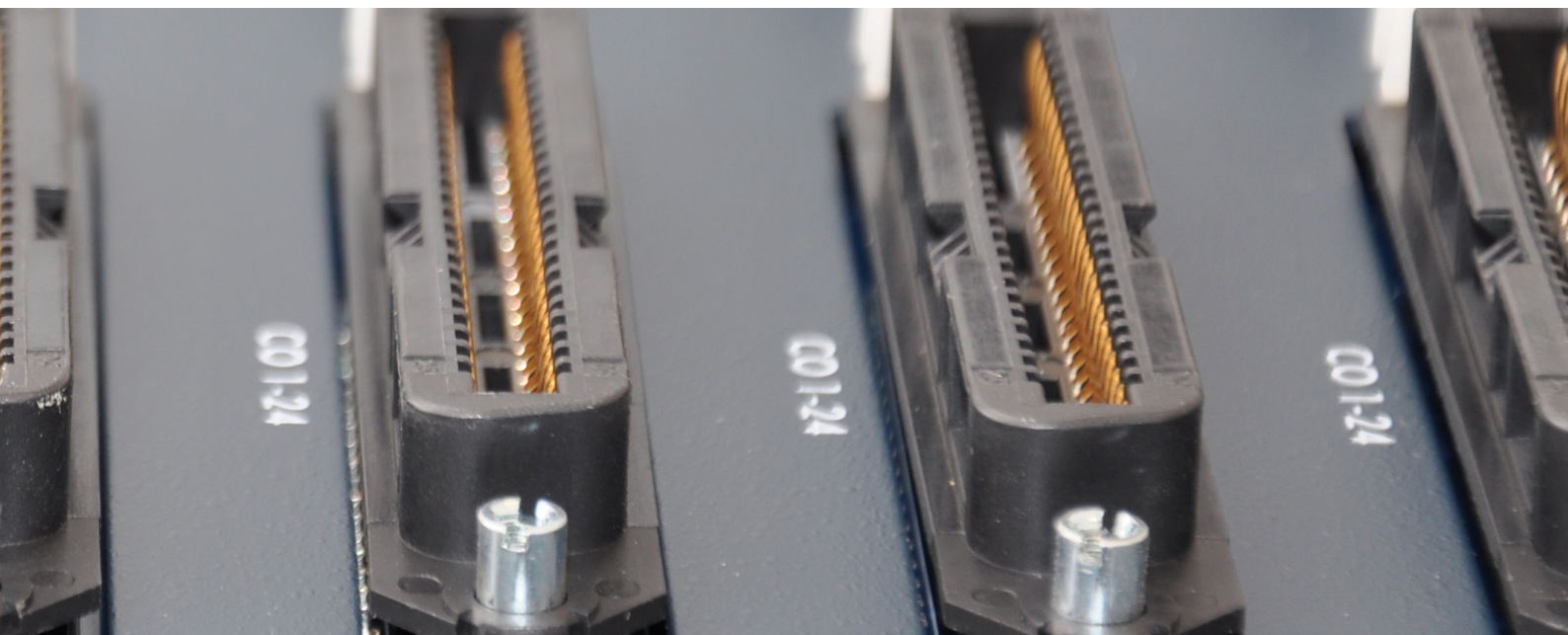
What is the risk factor? What are the increased sanctions for noncompliance?

The fines are in line with GDPR levels and are as follows.

- Infringements of the following rules could result in administrative fines of, the higher of 10,000,000 EUR, or up to 2% of the total worldwide annual turnover:
 - "cookie" information and consent rules,
 - privacy by design obligations,
 - rules on unsolicited communications (i.e. failure to respect opt-in rules), and
 - provisions on publicly available directories.
- Infringements of the following would be subject to administrative fines of, the higher of 20,000,000 EUR, or up to 4% of the total worldwide annual turnover:
 - the principle of confidentiality of communications,
 - unlawful processing of electronic communications data, and
 - time limits for erasure.

Is the scope of the regime changing?

- The new Regulation, like the GDPR, will have extra-territorial effect. It applies to the processing of electronic communications data carried out in connection with the provision and use of electronic communications services in the Union, regardless of whether or not the processing takes place in the Union.
- In addition to traditional voice, text and e-mail services, the provisions on confidentiality, the processing of electronic communications data, and storage and erasure of such data would apply to:
 - Over-the-top service providers ("OTT") such as unmanaged VoIP, instant messaging, web mail and social media messaging, and
 - Machine-to-machine communication (i.e. IoT technology), should the information or metadata exchanged between two devices be deemed to contain personal data.
 - The proposal's broad definition of "electronic communications services" is likely apply to all services that have a communications element - meaning dating apps, video game services, travel and e-commerce sites, even if they are just "ancillary" to another service.
 - As now, the rules on direct marketing and use of cookies and other tracking technologies would apply to all marketers and websites, regardless of whether they fall within the definition of electronic communications services.
 - Software providers and potentially retailers will also be impacted, as e-communications software placed on the market will be required to offer privacy settings which enable the blocking of third party cookies, and on installation, the software must inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.



What are the proposed changes to the rules for cookies?

The current rules on cookie consent, introduced by the 2009 amendments to the PECD, have attracted much controversy and resulted in an overload of consent requirements for internet users. There are some important changes to the rules.

- The new Regulation applies to cookies, spyware, web bugs, hidden identifiers and device fingerprinting. It prohibits the use of “processing and storage capabilities of terminal equipment and the collection of information from users’ terminal equipment, including about its software and hardware”, unless consent – or some other narrow conditions – are met.
- “Consent” has the same meaning as under the GDPR, i.e. freely given, specific, informed, active and unambiguous consent expressed by a statement or clear affirmative action.
- However, in the context of cookies, such consent may be expressed by browser settings and the Regulation places specific obligations on browser providers to ensure that appropriate consent settings and options are given to individuals.
- There are some new exceptions to the cookie consent rules, meaning those awkward banners and pop-ups won’t be needed where cookies are only used for:
 - web audience measuring – but this applies only to first party cookies,
- Alongside the familiar exceptions i.e.:
 - if it is necessary for the sole purpose of carrying out the transmission; or
 - it is necessary for providing an information society service, e.g. to add items to a shopping cart.
- Websites wanting to rely on cookies for marketing, tracking and behavioural purposes will therefore need to consider the browser consent users have given. In practice, we expect that websites will continue to want to get opt-in consent to override this and therefore pop-up consent boxes will remain a regular sight despite the European Commission’s intentions.
- The collection of device information e.g. for Wi-Fi log-ins is prohibited, other than for the purposes of establishing the connection, unless a “clear and prominent” notice is displayed “on the edge of the area of coverage” informing the user of:
 - how the data will be collected,
 - the purposes for which it will be used, and
 - the person responsible for collecting it and any other information required under the transparency requirement of the GDPR to make such processing fair.
- Such notices may be provided by means of standardised icons – to be developed under the “delegated acts” provisions of the Regulation – to make this information user-friendly.
- The Regulation proposes web browsers, and other applications that permit the retrieval and presentation of information on the internet, should provide users, at the moment of installation, with a clear and accessible choice on their privacy settings, which will be binding on third parties.
- The ‘choice’ should be as user-friendly as possible, whereby users are offered a set of privacy setting options, ranging from higher (e.g. never accept cookies) to lower (e.g. always accept cookies).
- Further, the information provided, should not dissuade users from selecting these higher privacy settings.

- Software installed before 25 May 2018 (assuming the Commission's implementation target is met) would need to offer the option to block third party cookies on the first update of the software, and at the latest by 25 August 2018.

Can users still use ad blockers?

The proposal does not regulate the use of ad blockers specifically, but instead gives website providers the ability to check if an end-user's device is able to receive their content, without obtaining the end-user's consent – this is a useful clarification.

Should the end-user's device be unable to receive the content requested, due to the user's own configuration, it is then up to the website provider to respond appropriately, for example by asking the user if they would be willing to switch off their ad blocker for the relevant website.

How would the rules on direct marketing differ?

The rules for opt-in and opt-out marketing consents are similar to the current position under the PECD (and there will have been a collective sigh of relief that 'soft opt-in' appears to have been retained), but there are some important changes to note.

- The restrictions on unsolicited marketing communications apply to all direct marketing communications sent via the broadly defined "electronic communications services" (in contrast to the PECD). The recitals indicate that this is intended to cover instant messaging applications, MMS and Bluetooth.
- The rules protect business recipients as well as individuals.
- There is no change in that organisations would be required to obtain end-users' prior consent, before sending commercial electronic communications for direct marketing purposes.
- Once given, the end-user's consent can then be withdrawn at any time.
- A soft opt-in remains for the use of e-mail contact details within the context of an existing customer relationship for the offering of the marketer's own similar products or services. Note that the draft Regulation, like the PECD, restricts the use of the soft opt-in to the context of "a sale of a product or a service" whereas the current UK Regulations extend this to the "sale or negotiations for the sale".

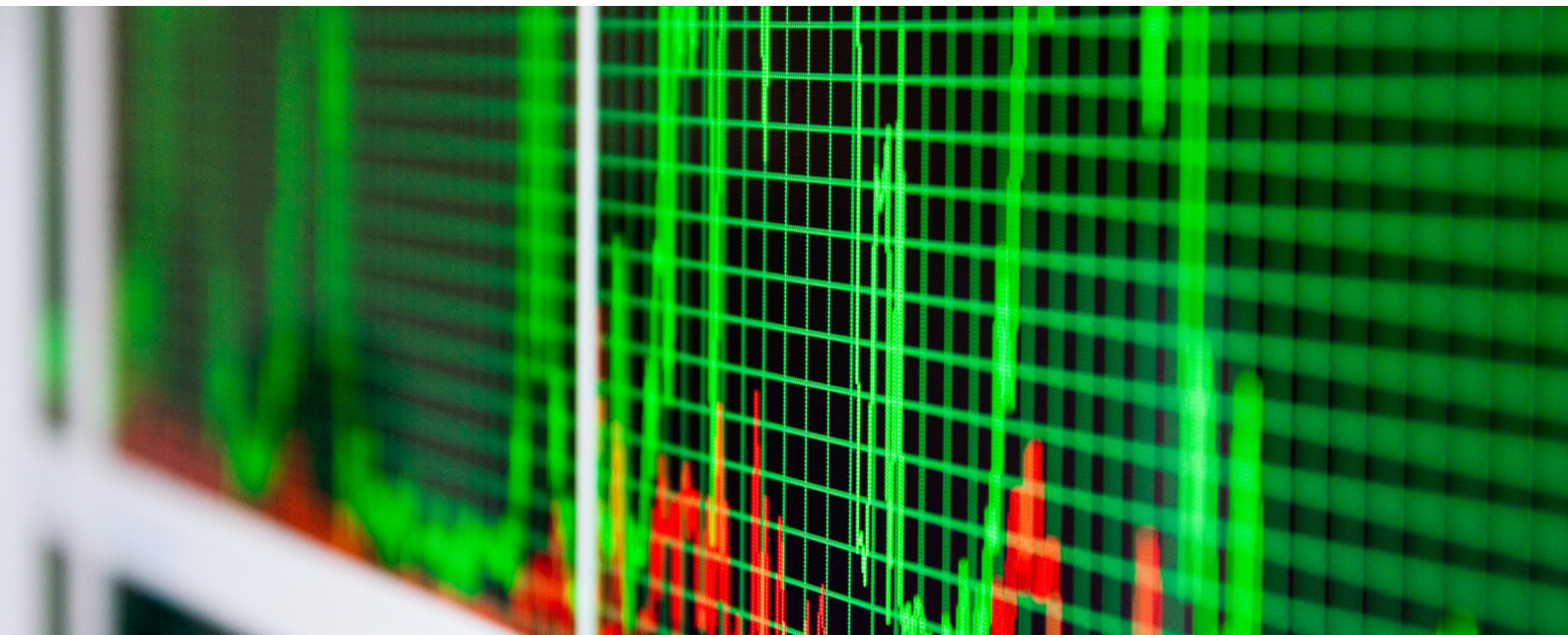
- Member States still have discretion to make live telemarketing calls opt-out (the current position in the UK).
- There are similar requirements for marketers to be transparent, i.e. make it clear that communications are marketing, the identity of the marketer and to facilitate opt-outs.

What does it say about metadata vs content of communications?

- Metadata is specifically mentioned in the Regulation. The basic rule is that both the content and metadata of ecommunications are confidential and that all is prohibited.
- Service providers will need users' consent to in order to use the metadata, such as location data, to provide services.
- There are a few exceptions to this, such as transmission and / or security.
- Certain high-risk processing of communications metadata may also require a Privacy Impact Assessment under the GDPR. In practice this is unlikely to mean much change.
- For the use of communications content in order to provide services, the rules are stricter. Providers of electronic communications services may process electronic communications content only:
 - when providing a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of their electronic communications content and the provision of that service cannot be fulfilled without the processing of such content, unless
 - all end-users concerned have given their consent to the processing of their electronic communications content for a purpose that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority.
- Consent for the use of both communication content and metadata for the provision of services can be withdrawn at any time, but in addition, service providers must remind end-users every six months that they have the right to opt-out.

What else does the new Regulation cover?

The new Regulation would also update the rules on calling line identification and call blocking, to combat nuisance calls, and the rules on public directories.



Comment and next steps

Given how far communications media and advertising techniques have evolved since 2002, or even 2009 when the PECD was last updated, the overhaul of the rules is overdue.

The current cookies rules in particular have been widely (and rightly) ridiculed, so reconsideration is welcome. However, it is not clear in practice that the proposals will actually mean an end to, or substantial decrease in, pop-up consent and banners unfortunately, and the high consent threshold (to align with GDPR) is likely to be unpopular in many circles. Whether or not the rules will achieve a truly “future-proof” state also remains to be seen.

The Commission’s aim is for the new rules to come into force at the same time as the GDPR. Whether this is realistic or not depends on how much lobbying it attracts from the wider domain of digital businesses now in scope and the scrutiny of the other European institutions. We will be tracking the progress of the proposal through its next legislative stages – consideration by the European Parliament, initially through a Rapporteur and lead committee – and by the

Member States in the form of the Council. Depending on the degree of consensus on the draft proposal, this process could take between months and years.

We will provide regular progress updates on our Datonomy blog at www.datonomy.eu

For more information please contact CMS’ Head of Digital and Data, Elle Todd, and Alex Dixie, the firm’s Head of Adtech.

For more information please contact:



Elle Todd
Partner
T +44 20 7067 3105
E elle.todd@cms-cmno.com



Alex Dixie
Associate
T +44 20 7067 3313
E alex.dixie@cms-cmno.com



Law . Tax

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.

cms-lawnow.com



Law . Tax

Your expert legal publications online.

In-depth international legal research
and insights that can be personalised.

eguides.cmslegal.com

CMS Legal Services EEIG (CMS EEIG) is a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices.

CMS locations:

Aberdeen, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luxembourg, Lyon, Madrid, Medellín, Mexico City, Milan, Moscow, Munich, Muscat, Paris, Podgorica, Prague, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Seville, Shanghai, Sofia, Strasbourg, Stuttgart, Tehran, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

cms.law