Contents

[5] New e-Privacy Regulation (expected Autumn 2020)

What's different?

It's clear though that the issue of access to online content being conditional on the user's consent to cookies, and who's responsible for obtaining such consent are key issues discussed by Member States and issues that European Commission has pushed.

The latest version of the e-Privacy Regulation[1] (dated 28/8/18) includes various small changes throughout, especially on the Recitals.

Notable exceptions are the Arts.6, 8 and 10, E-PR that the Bulgarian Presidency of the European Commission has decided to ask for more guidance and asked Member States to choose among

[1] E-PR

several options. There haven't been any changes in the wording of Art.8 and 10, E-PR since they are the subjects of proposed options.

Recital 20, E-PR is important to Marketeers, as it explains that the responsibility to obtain consent lies on the entity that makes use of processing and storage capabilities of the device or collects the information. However, the entity can request another party to collect consent on their behalf (i.e. a publisher).

Direct marketing (Art.16, E-PR)

There's some tidying-up of this Article in its drafting, confirming that Member States understood that advertising presented to an individual, such as display advertising shouldn't be considered as direct marketing.

This is further clarified by Recital 32, E-PR that says that displaying advertising to the general public shouldn't be considered as direct marketing.

However, the Recital still makes the distinction between display ad to the general public and display ad that's directed to any specific identified or identifiable end-user.

An identified or identifiable end-user is the user that has logged in with a private account or personal log-in. Thus, any targeted ad presented in a log-in environment would be considered as direct marketing and the provisions of Art. 16, E-PR would apply.

Art.16 (2), E-PR, for the soft opt-in, the text now allows the use electronic contact details obtained in the context of a purchase (as opposed to in the context of a sale).

On the time limit for the use of the soft opt-in exemption, the new wording reads:

"Member States may provide by law a set period, after the sale of the product."

This doesn't change anything significantly and it will create again a patchwork around Europe that publisher would have to comply/respect different time limits across the EU. There are no proposed changes to the language regarding the common prefix to telemarketing. Similarly, the definition of both direct marketing communication and automated calling and communication systems hasn't changed, maybe because there were no further discussions on the issue.

Relationship with the GDPR?

It's important that brand owners understand the different ways in which the GDPR and E-PR will affect their business.

The current PECR provides a specific set of privacy rules to regulate the processing of personal data by the telecoms sector. Until it's is amended, PECR will co-exist with the GDPR (which applies to all sectors including the telecoms sector). There remains some uncertainty in the relationship between the E-PR and the GDPR, which will require clarification.

The E-PR is a proposal for a Regulation on Privacy and Electronic Communications that repeals PECR. It's designed to complement the GDPR with regard to electronic communications data that qualify as personal data and will significantly strengthen the online and direct marketing legal landscape.

Initially, the aim was to replace the PECR so that the E-PR would come into force on the same day as the GDPR. However, due to ongoing discussions and various legislative hurdles still to cross, E-PR is more likely to come into force in Autumn next year.

While the GDPR regulates the processing and sharing of personal information, the E-PR addresses the rules companies and organizations must follow when sending electronic direct marketing and using track technologies such as cookies. If it's adopted, it's proposed that it will be *lex specialis* to the GDPR meaning that its terms can override those of the GDPR in case of a conflict.

Summary of main changes:

- it extends the scope of PECR to cover telecoms providers, text and email providers and 'over the top' providers (Apps)
- it applies rules to new tracking and e-marketing technologies
- it aligns privacy concepts with the GDPR (consent, data breaches, territorial scope, fines)

The E-PR aims to modernise the law, meaning that not only traditional telecoms providers will be caught but also text and email providers, internet-based voice and internet-messaging services - "over-the-top" content providers such as Skype, Whatsapp, Facebook Messenger and iMessage.

E-PR will apply to any brand owner that provides any form of online communication service that utilises online tracking technologies or that engages in electronic direct marketing including non-EU providers that provide electronic services (free and/or paid) to EU nationals.

It also changes the way that electronic communications data is currently regulated by creating separate rules for the use of content and metadata, about how each is used, when consent is required. The proposal also includes new rules for the storage and erasure of electronic communications content.

Consent and E-PR

E-PR will be in alignment with the GDPR's approach to valid consent. This means that for consent to be valid it must be freely given, specific, informed and unambiguous. As with the GDPR, this means that, if relying on consent, anything other than clear opt-in consent to electronic direct marketing won't be valid consent.

Direct marketing and E-PR

The definitions of direct marketing and electronic communications are broader than those in PECR. The proposal distinguishes between B2C and B2B communications. For B2C communications, the proposal requires the sender of the communication to obtain the consent of individuals for direct e-marketing purposes.

In contrast, for B2B communications, the proposal leaves it to the Member States to ensure that the legitimate interest of corporate end-users is sufficiently protected from unsolicited communications.

Cookies and E-PR

The new Regulation will change the rules surrounding use of cookies, including marketing cookies, with privacy rights being prioritised.

Cookies and tracking for online advertisement will remain lawful but will be governed by clearer rules, giving choices to users from the outset when initially choosing their settings. This will be mean a significant change for internet browser providers like Microsoft and Google. They will require a clear, affirmative action from the end-user of terminal equipment to signify his or her freely given, specific, informed and unambiguous agreement to the storage and access of third party tracking cookies in and from the terminal equipment.

Telephone marketing calls and E-PR

Companies and organizations making direct marketing telephone calls would be required to display calling line identification or present a specific code/prefix indicating that the call is a marketing call.

Relationship between UKGDPR and E-PR

As previously discussed, if the E-PR is adopted as it stands, it will be *lex specialis* to the GDPR meaning that its terms can override those of the UKGDPR in case of a conflict.

Many aspects have been drafted in line with the UKGDPR so as to avoid such conflict: the penalties for non-compliance will reflect those in the UKGDPR; end users are granted many of the same remedies as provided by the UKGDPR – the right to lodge a complaint with the ICO, the right to an effective judicial remedy against the ICO, and the right to an effective judicial remedy against a data controller or data processor; a right to compensation and damage is also envisaged and; individuals will also have the right to sue for compensation for 'material or non-material damage' caused by an infringement of the E-PR.

Soft opt-in under E-PR

The current draft of the E-PR retains the soft opt-in exemption but limits it to commercial marketing about the sale of goods or services where the brand owner has obtained the individual's personal details in the course of such a sale.

However, the reference to negotiations has been removed, so this is more restrictive in its scope than its predecessor.

Any electronic direct marketing under the soft opt-in must be limited to marketing similar products or services of the specific entity using the soft opt-in (i.e. not another group company).

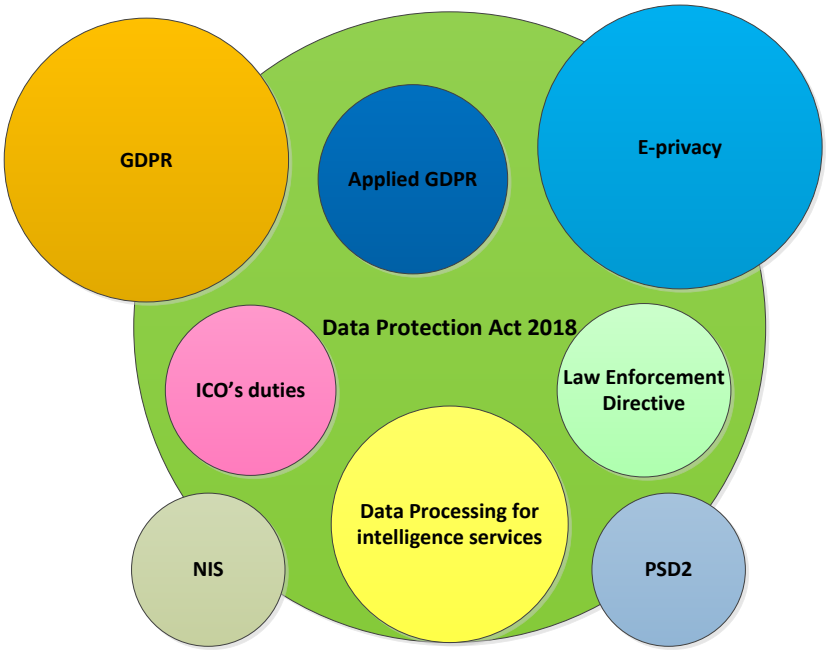
Also, like the PECR, the marketing materials must be closely related to the products/services originally purchased. And the requirement of providing an individual a simple and clear option to opt-out in every correspondence from receiving such B2B marketing remains.

E-PR is one element of the legal data protection eco-system

As you can see from this diagram, E-PR (e-Privacy) is one element of the legal data protection eco-system within EU Member States as well as the UK on exiting the EU in March 2020.

In the UK, the legal eco-system includes new powers of the ICO under the Data Protection Act 2018, Applied GDPR, PECR (e-Privacy), Law Enforcement Directive (LED), the Directive on Security of Networks and Information Systems (NIS), PSD2 and regulations for data processing for the Intelligence Services.

Diagram 1: Data protection eco-system in the UK



Confidentiality of electronic communications

Art. 5, E-PR specifically identifies that electronic communications data shall be confidential. Any interference with electronic communications data, including listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by anyone other than the end-users concerned, will be under the latest revision prohibited, except when permitted by the proposed revision.

Consent is now required to process communications content and metadata

The application of the risk-based approach in relation to the processing of personal data under the GDPR to metadata appears to be an effective safeguard against privacy challenges.

The processing of any metadata – irrespective of its source technology or whether it originates from an electronic communications service – can create privacy challenges and therefore may require a data protection impact assessment (DPIA) in line with the GDPR's risk-based approach and accountability principle.[2]

This ensures the nature, scope, context and purposes of the processing of the metadata are taken into consideration, risks and impacts are identified; safeguards and mechanisms for mitigating that risk are implemented, including a justification for which the data controller can be held accountable.

M2M

E-PR also refers to mobile to mobile (M2M) communication in the context of underlying conveyance.

The proposed definition of an electronic communications service explicitly refers to M2M communication, when dealing with the (technical) transmission service.

Services offering the (technical) transmission of M2M communication should adhere to the confidentiality of communications, even though the message carried may have been composed without direct human intervention.

New business opportunities

The processing of electronic communications data can be useful for businesses, consumers and society.

E-PR broadens the possibilities for providers of electronic communications services to process electronic communications metadata, based on end-user's consent. This is an opportunity for brand owners as GDPR and E-PR both require brand owners to review what personal data they hold and what personal data they don't require to hold, thus enabling a 'data cleanse' of their data systems.

One of the key principles of both the GDPR and E-PR is that the company or organization should implement an opt-in policy and have a data subject's consent to process their personal data.

[2] The accountability principle is the seventh data protection principle (Art.5, GDPR) and one of the most important sentences in the GDPR

Combined with purging redundant, obsolete or trivial personal data that hinders rather than helps brand owners, marketers will be left with a fine-tuned database of highly relevant leads and customers that genuinely want to hear from them.

Revised rules on cookies

The responsibility for obtaining consent for the storage of a cookie or similar identifier within the new E-PR lies on the entity that makes use of processing and storage capabilities of terminal equipment or collects of information from end-users' terminal equipment, such as an information society service provider or ad network provider.

Companies and organizations may request another party to obtain consent on their behalf. The end user's consent to storage of a cookie or similar identifier may also entail consent for the subsequent readings of the cookie in the context of a revisit to the same website domain initially visited by the end-user.

Not all cookies are needed in relation to the purpose of the provision of the website service. For example, some are used to provide for additional benefits for the website operator.

Making access to the website content provided without direct monetary payment conditional to the consent of the end-user to the storage and reading of cookies for additional purposes would normally not be considered disproportionate in particular if the end-user is able to choose between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes on the other hand.

Such a trade off, provided that it complies with the higher standards of data protection, privacy and security is acceptable.

Conversely, in some cases, making access to website content conditional to consent to the use of such cookies may be considered to be disproportionate and not in accordance with the higher standards of data protection, privacy and security expected by the user.

Consent shouldn't be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security vulnerabilities and other security bugs, provided that such updates don't in any way change the functionality of the hardware or software or the privacy

settings chosen by the end-user and the end-user has the possibility to postpone or turn off the automatic installation of such updates.

Protection against spam

Spam emails may affect the availability of bona fide email services and could potentially impact the performance of networks and e-mail services, which justifies the processing of electronic communications data to mitigate this risk.

Providers of electronic communications services are encouraged to offer end-users the possibility to check emails deemed as spam to ascertain whether they were indeed spam and at the same time this mustn't prohibit the processing of metadata to quantify a level of quality of service requirements.