EUROPEAN ASSOCIATION OF COMMUNICATIONS AGENCIES

EACA position on the ePrivacy Regulation proposal

The European Association of Communications Agencies (EACA) represents more than 2 500 communications agencies and agency associations from 30 European countries that directly employ more than 120 000 people. EACA members include advertising, media, digital, branding and PR agencies. They create and place adverts and develop brand-building campaigns.

EACA welcomes the proposal for the ePrivacy Regulation (the Proposal) of the European Commission. EACA and its member agencies and national associations are keen to engage with legislators so that the final text meets the needs of European society: appropriate protection of consumers' private lives and the ability of European data-driven companies to compete on an equal footing within Europe and beyond.

This document first presents the main points of concern for European advertising agencies about the Proposal, before going into a more detailed article-by-article analysis and proposing solutions.

Value of advertising

According to the study, conducted and written by Deloitte, advertising contributes to the European economy in many ways:

- On average, 1 Euro of advertising spend generates 7 Euros for the economy
- Advertising provides almost 6 million jobs in the EU, equivalent to 2.6% of all EU employment
- Advertising provides personal and social benefits by funding or partly funding media services, meaning people can enjoy them for free or at a reduced rate
- Advertising contributes to wider economic growth through its ability to support competitiveness. It provides consumers with information on products and services, and helps to increase their choice of goods and services. This, in turn, drives innovation by incentivising businesses to create differentiated products and services, allowing them to out-compete their competitors not just in the EU but around the world.

Why does the ePrivacy Regulation matter to agencies?

Agencies manage and buy media space on behalf of their clients (brands). For example, Brand A may authorise Agency Z to reach men between 25-35, beer drinkers and football fans. The agency would create a media mix strategy and part of the strategy would be to reach and engage with these consumers online, via digital media. Advertising is increasingly data-driven. Advertisers and agencies rely on high-quality data to deliver targeted ads to the right people. Data of this quality can be sourced via 3rd party data providers or big online tech platforms.

Agencies rely on their own 3rd party cookies placed on terminal equipment and on 3rd party identifiers placed by other entities to deliver relevant ads to consumers. Without being able to communicate lawfully with end-users, the business model of agencies and other data-driven businesses would be seriously disrupted and a free and competitive data market in Europe would be endangered.

152 Boulevard Brand Whitlock
1200 Brussels, BELGIUM
+32 2 740 07 10
+32 2 740 07 17
info@eaca.eu
www.eaca.eu

EUROPEAN ASSOCIATION OF COMMUNICATIONS AGENCIES

What kind of ePrivacy Regulation does the European Union need?

EACA believes that the Regulation should achieve two intertwining objectives: more transparency and control for end-users and allow innovative online businesses to thrive.

The Regulation should build on the requirements of the General Data Protection Regulation (GDPR) and allow end-users to be properly informed about their data choices and the purposes of data processing. This will be only possible if the Regulation does not introduce new gatekeepers (such as browsers), but instead encourages the development of different privacy tools, including self-regulatory ones, which would also incite businesses to be more transparent and accountable.

The Regulation cannot rely only on consent requirements, which do not even match those in the GDPR, and a couple of narrow exceptions. Apart from causing obvious consumer fatigue, it would allow some global online companies to expand their data dominance further, while stifling European data-driven businesses.

EACA's main concerns about the Proposal

GDPR obligations are not fully respected or endorsed

EACA believes that the Proposal does not sufficiently build on the recently adopted General Data Protection Regulation, as it does not take into consideration many of its crucial elements which are beneficial to European data-driven businesses and consumers. For example, EACA has identified some specific areas for improvement: a clear lack of diverse legal grounds for data processing, no endorsement of data protection safeguards and measures (pseudonymisation and anonymization) and impaired consent requirements regarding information to be provided to end-users.

Consumers will not get a real choice and will be burdened by consent requirements

The Proposal stipulates that consumers will give their consent via browsers or other software. This consent would not be fully informed, as the proposal envisages blanket acceptance or rejection of 1st or 3rd party identifiers. Consumers would not get a full insight about the data controllers collecting their data and for which purpose. Moreover, as they would have to consent upon every installation, and as many publishers would ask them to whitelist their websites, cookie banners would not disappear, but would become more common and intrusive. That is why the Proposal needs to encourage development of diverse privacy tools.

Further erosion of the European data market and impact on the advertising eco-system and new data-driven business models

The data market reality is that a small number of global tech companies are in control of immense volumes of data. They act as first party data collectors and processors and collect a lot of consumer data via their consumer facing services which often require a log in (social media profiles, searches etc.) This is a trend which will only gain in prominence as these companies' services proliferate, due to which they will continue to obtain more and more consumer data. The Proposal may lead to a complete exclusion of those data providers who do not have a direct relationship with the consumer and therefore cannot obtain a direct consent, with the result that the global tech companies' data collection could be empowered; they will continue to gather large volumes of data while their competition will be suffocated by this Regulation, even more so as many of them operate successful browsers and other applications allowing access to the Internet. These global companies already have a large (if not dominant) position in the digital advertising market. If the Proposal comes into force as it stands, digital advertising will increasingly rely on a very few companies which will continue to be

152 Boulevard Brand Whitlock
1200 Brussels, BELGIUM
+32 2 740 07 10
+32 2 740 07 17
info@eaca.eu
www.eaca.eu

able to provide high quality data.

Media funding threatened

Online media depend on advertising to fund their daily activities and to support the freedom of journalism. Advertising on different online media will continue appearing despite the final text of the Proposal. However, if 3rd party data processing can only be done as the result of consent, advertising will be far less relevant and therefore less financially rewarding for the media. The benefit of online advertising is to attract people according to their preferences. Only advertising which appeals to specific profiles is able to attract enough investment from advertisers. Advertisers are prepared to pay more to place ads which are likely to be registered and/or acted upon by consumers. That in turn means that websites will be able to charge more for those advertising slots which are more likely to attract consumers, that is to say for slots filled by behavioural advertising, rather than irrelevant ads. It is worth noting that if ads are to become increasingly irrelevant, this may lead to an even higher adoption rate of adblocking, eroding media funding even further. A report by KPMG found that 40% of people installing adblocking software do so because they find the ads irrelevant. On the other hand, when asked why they click on an ad, 40% said that they were interested in that ad.

EACA position – Article by article

Article 8.1 Protection of information stored in and related to end-users' terminal equipment

Article 8.1 regulates when and under which conditions a person or an entity can store or access data (e.g. online identifiers) on end-users' terminal equipment (e.g. mobile phones, tablets, desktop computers etc.)

Article 8.1
Protection of information stored in and related to end-users' terminal equipment

The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:
(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or
(b) the end-user has given his or her consent; or
(c) it is necessary for providing an information society service requested by the end user; or
(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end user.

EACA perceives a couple challenges and areas for improvement in this Article:

- Reliance on consent and ignoring other legal grounds for data processing, as embedded in the GDPR;
- Lack of incentives for businesses to deploy data protection measures and safeguards such as pseudonymisation and anonymization of data;
- Overly narrow exception 8.2(d) for web-analytics which does not allow 3rd party measurement;

Consent is not a silver bullet

Online identifiers such as cookies, which carry personal data, are recognised by the GDPR as personal data (Article 4.1 and Recital 30, GDPR). Furthermore, Article 6 of the GDPR lays down specific legal grounds for the

processing of personal data, beyond consent. It provides data controllers with many legal grounds including consent, processing necessary for the performance of a contract and legitimate interest pursued by a controller or third party.

Nevertheless, the Proposal itself narrows down legal grounds for data processing to consent and a couple of confined exceptions.

According to the Proposal, a consumer will have to consent to any entity using or processing data stored on their terminal equipment. In combination with Article 10, which stipulates that an end-user would have to consent to this via a browser or software, it will effectively mean that every time a consumer downloads a piece of software they will have to choose a different level of privacy protection and to consent to 3rd party tracking. However, since publishers will want to be white-listed during each visit of any website, a consumer will again see a banner asking them to whitelist the website. We feel that this will not lead to the reduction of consumer-fatigue, as argued by the European Commission, but is more likely to increase it.

EACA believes that end-users should be allowed to exercise their choice to opt-in, opt-out and be informed, all according to the GDPR, which stipulates end-users' rights in great detail. EACA recognises the need for greater transparency and accountability towards end-users.
However, we feel that over-reliance on consent will over-burden them and cripple the European data market by advantaging those companies who will be able to obtain consent much more easily than others (via their product offerings such as social media, search etc.)

Consequently, EACA advises the legislator to introduce other legal grounds for data processing in the Proposal while additionally safeguarding end-users' rights by recognising privacy and data protection risk minimisation techniques and safeguards, such as data pseudonymisation and anonymisation.

Legal grounds for data processing beyond consent and a risk-based approach should be recognised

As the Article 29 Working Party rightfully outlines, in its 06/2014 opinion, consent is one of several legal grounds for data processing, but not the main one. Additionally, it says that other legal grounds may be more appropriate depending on the context.

Data-processing context is a key area to consider. A consent requirement may be completely appropriate and justified for data-processing operations stripped of any safeguards. However, if a data-controller is required and/or encouraged to deploy a risk-based data processing approach, other data processing legal grounds should be considered.

This is where the Proposal fails to build on the requirements and hard-won compromises embedded in the GDPR. While the GDPR encourages a risk-based approach and different safeguards applicable to different data-processing operations, the Proposal neglects them. By insisting on consent, the Proposal imposes a one-size-fits-all approach regardless of the context and specifics of the data-processing operation.

Option 3 of the Impact Assessment accompanying the Proposal did suggest that one of the exceptions to a consent rule should be data processing based on legitimate interests with appropriate safeguards such as pseudonymisation and anonymization taken into consideration.

However, it was decided that this specific derogation would be left out, despite clear indications in the Assessment that SMEs would be negatively affected and that newcomers to the market would feel the lack of it more than already established ones. Furthermore, the Commission recognises that this derogation would spur research and development of new anonymization and pseudonymisation technologies.

Therefore, EACA advocates for an inclusion of different legal grounds, such as legitimate interests, for data processing by taking into consideration risk-based data processing approach. Data controllers should be incentivised to use the GDPR data protection safeguards and to further evolve them. Without these safeguards being recognised in the final ePrivacy Regulation, the GDPR promise of risk-based data processing will not be fulfilled..

Web measurement audience exception is welcome, but needs improvement

EACA welcomes the exception outlined in Article 8.1(d) which allows storage of, and access to, terminal equipment *if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.*

This is an improvement from the last version of the ePrivacy Directive. However, the Proposal does not take into consideration a serious need for the advertising industry to verify that ads online are delivered and seen. The entire online advertising ecosystem relies on third party vendors to verify whether an ad placed on a website was seen or not. This allows them to assess whether they are targeting the right audiences (driven by data or contextuality). It also permits them to assess whether their media investment was well spent.

That is why the proposal should take into consideration that this kind of service is often delivered by 3rd parties and not publishers themselves, by deleting the obligation that the measurement has to be provided by the information society service requested by the end user.

Article 10 – Information and options for privacy settings to be provided

Article 10 of the proposal stipulates that the browsers and other software placed on the market will offer options to end-users, who will be able to choose different privacy settings, rejecting or accepting 1st or 3rd party cookies.

Article 10
Information and options for privacy settings to be provided

1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.
2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.
3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.

EACA envisages some implementation problems with this particular article, as outlined below.

Browsers as gate-keepers

This provision effectively makes browsers gate-keepers of the online eco-system. First and third party businesses may want to engage in a dialogue with users to encourage them to consent to online tracking for the purpose of delivering more relevant ads to their interests. Even if a first party obtains consent from end-users, browsers may decide not to recognise this consent, as they are not required to do so by the proposal itself. The proposal

currently encourages browsers to allow consumers to whitelist certain publishers (Recital 23), but it does not require them to do so.

Furthermore, first parties often rely on third parties for many services, such as web-measurement. Whereas browsers are capable of differentiating first party from third party cookies, they are less well equipped to do so when dealing with third party with or without consent.

Therefore, browsers should not be given the powers of gatekeepers and ultimate law enforcers; instead they ought to accept consumer preferences expressed via different channels (publisher's portal, different privacy tools). Essentially, an end-user should be able to consent via a publisher's request or via another privacy tool, deployed by different players on the market.

Finally, browsers should recognise and act on the expression of consumer preference. This can be achieved by changes in the text which would require them to:

- Whitelist websites or other services, as publishers should not rely on a regulatory encouragement for that to happen. The regulation should require browsers to allow consumers to interact with publishers and other internet service providers.
- Communicate any external opt-in or opt-out from an end-user, specific or not, to the provider of internet information services;

Consent is not a GDPR-proof one

According to Article 10 of the Proposal, an end-user is invited to accept or reject 3rd or 1st party cookies upon installation, which effectively means that browsers are supposed to allow blanket consent. Recital 23 of the Proposal further expands this stipulation: *End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies'). Such privacy settings should be presented in an easily visible and intelligible manner.*

Indeed, browsers are encouraged to allow consumers to whitelist certain publishers, but before that they are expected to consent or reject blanket data processing without any specific information provided. Therefore, the Proposal does not meet the GDPR standards regarding consent for two reasons:

The ePrivacy consent is not a specific one and it does not address the purpose of data processing but the provenance of the data controller

The envisaged consent in the Proposal does not meet legal consent obligations as stipulated in the GDPR. Namely, Article 6(a) clearly states that consent should be given for data processing for one or more specific purposes. Current wording in the Proposal, instead, allows consent to be general and to be provided based on provenance (1st or 3rd party). Whereas GDPR Article 6(1) and Article 7 do not foresee the possibility of an end user providing their consent based on provenance, they do foresee it based on purpose - and the purpose should be specific.

The Proposal does not build on this GDPR obligation, but instead requires end-users to consent to unknown data controllers based on their origin (1st or 3rd parties).

EACA therefore recommends differentiation based on purpose for concrete data-processing, as described and codified in the GDPR. Instead of differentiating 1st and 3rd party online identifiers, EACA recommends differentiation based on the purpose for concrete data-processing.

152 Boulevard Brand Whitlock
1200 Brussels, BELGIUM
+32 2 740 07 10
+32 2 740 07 17
info@eaca.eu
www.eaca.eu

End-users are expected to provide consent with little information

One of the main objectives of the Proposal is to make data collection and data processing in an online environment more transparent. However, the Proposal currently does not build on this promise. As an end-user is expected to consent via a browser or software, there will be obvious challenges to provide them with all the information about the purpose of data processing, data controller identity and other information requirement as stipulated in Articles 13 of the GDPR (Information to be provided where personal data are collected from the data subject).

Essentially, according to the Proposal, end-users would be consenting to their data being processed with little information provided and additionally they would be consenting to all 3rd party or 1st party data processing without knowing specificities.

In order to improve data processing transparency and accountability, in accordance with the GDPR, EACA is believes that the Proposal should encourage the development of different privacy tools, including self-regulatory ones, that would provide end-users with all the tools needed to be informed and to take control of their data, should they so desire.

Direct marketing – Article 4(f) and Article 16

The core concept of direct marketing is that the communication is directed to a particular individual. Direct marketing is not defined by the nature of the communication. Such communication can be commercial, political or charitable while being direct marketing. Additionally, direct marketing is not defined by the channel or the communication tool used. It can happen using any communication channel which enables access to particular individuals. It is technology neutral and omni-channel. Direct Marketing is communication of any advertising or marketing material which enables organisations to dialogue with a particular individual, either on or offline.

The Proposal defines direct marketing as any form or advertising directed to an identifiable and identified person. An identifiable person is not the same as a particular individual. The Proposal's wording could extend all obligations of direct marketing to all advertising, which should not be the intention.

Article 16 of the Proposal also requires end-users to consent in order to receive direct marketing messages. If the proposal requires a broad definition of direct marketing and a consent obligation, it may well mean that end-users would need to consent to receiving any advertising online. This is not and should not be the intention of the Proposal. Furthermore, the GDPR does recognise legitimate interest for direct marketing, while the proposal takes it away. This is very far away from required legal consistency, sought by this reform.

152 Boulevard Brand Whitlock
1200 Brussels, BELGIUM
+32 2 740 07 10
+32 2 740 07 17
info@eaca.eu
www.eaca.eu