EUROPEAN ASSOCIATION OF COMMUNICATIONS AGENCIES

ePrivacy Directive

Background

The ePrivacy Directive particularises and complements the Data Protection Regulation by, among others, setting-up specific rules concerning the processing of personal data in the electronic communication sector.
The new General Data Protection Regulation was adopted in April 2016, will replace the current Data Protection Directive to ensure modernised rules fit for the digital age.

Given that the ePrivacy Directive complements the GDPR, it will have to be reviewed and revised. To that extent the European Commission launched a public consultation asking stakeholders their opinion on many issues embedded in the ePD. Below you will find the main issues and EACA position.

Issues and EACA positions

Has ePD achieved its objectives?

The ePrivacy Directive (ePD) particularises the current Data Protection Directive (95/46/EC) and is expected to complement also the General Data Protection Regulation starting from May 2018.
To that end, it is fair to say that the objectives as well as the scope of the ePD should be aligned with the overarching data protection legislation. A Directive as a legal instrument has to be transposed, which usually means the adaptation of its provisions to very different regimes across the EU. This is also what happened to the 95/46/EC Directive which was a source of fragmentation of data protection regimes. Instead of having a harmonised approach, which would help businesses to operate with a full legal certainty, businesses have to comply with 28 different regimes. Moreover, since the harmonisation pursued by the ePD was supposed to build on the disharmonised 95/46/EC Directive, a full business-friendly harmonisation was difficult to achieve. Having said this, the ePD has only moderately achieved its objectives.
To that end, the objective of protection of privacy and confidentiality was achieved even though Member States transposed the Article 5(3) of the ePD differently, partly due to diverging transposition of the Directive 95/46/EC. This also impeded free movement of personal data as businesses faced diverging member states views and consecutively impeded free movement of digital commercial communications.

Confidentiality of information: Article 5

Article 5 of the ePD is probably the most complex element of the Directive. It aims to protect the confidentiality of communications while simultaneously regulating when cookies and other trackers can be stored and accessed in a terminal equipment of a user (Article 5(3)). This provision was much debated and caused many fractions in legal requirements and interpretations across Europe.
While some Member States interpreted the Article 5(3) as an opt-in requirement (i.e. Austria and Bulgaria), other Member States decided to take another path and not to ask for it (i.e. Czech Republic, Hungary, Ireland). This led to confusing legal requirements and legal and business uncertainty for international companies which have to comply with different regimes depending on

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

the country they operate in. In the EU Single Market, free movement of electronic services is of crucial importance for growth empowered by digital technologies.
Furthermore, many Member States implemented Recital 66 of the Citizens' Rights Directive which states that 'the user's consent to processing may be expressed by using the appropriate settings of a browser or other application.' This recital was independently added to laws of about ten Member States (France, Ireland, Luxembourg, Greece, Poland, Slovakia, Spain and the UK). The Article 29 Working Party then issued its Opinion 2/2010 setting new conditions for the user's consent which added to the confusion.
The confidentiality rules in the ePD represent a complex compromise achieved in 2009 which proved to challenging to transpose and implement equally in all Member States. The solution is to align ePD to GDPR and its overarching provisions.

Cost of compliance

Having determined previously that the transposition of the ePD has been particularly divergent across Europe, it is obvious where extra compliance costs for international businesses derive from. For example, the transposition of Article 5.3 varies from member state to member state on many levels: scope, legal instrument, competent authorities and consent rules. Namely, in Bulgaria Article 5(3) applies only to information society services, in Germany there was no transposition at all because it was considered that existing rules were sufficient and relevant, the Czech Republic still maintains the 2002 version of the Directive. Furthermore, a couple of member states introduced separate rules for analytical tools (cookies) and for devices (desktop, laptops, mobile phones etc.). As previously mentioned, 10 EU member states introduced a rule that browsers can be used by users to give their consent.
This is only an excerpt of legislative granularity. Granularity of rules does not exist only for international businesses trading across European market but for national businesses that have to find their way through a myriad of different data protection legislative pieces, take into consideration the difference between personal and non-personal data, which network they are using to provide their services (public or private) or where to place a cookie banner according to different devices.
Competent authorities, in order to ensure the more or less consistent legal framework, issued guidance documents which again brought other layers of compliance requirements. Hours of legal research, complying with different pieces of legislation, understanding the scope are only some contributors to large compliance costs of the ePD.

Opt in or opt out

Informing consumers about processing of their data is crucial to build a well trusted relationship between service providers and consumers. Consumers should be informed via comprehensible privacy policies and terms and conditions about how their data is used and processed. The advertising industry understands this and that is why we have developed a self-regulatory programme focused on the OBA. Too many consent requirements can overwhelm a consumer.
The opt-in policy would influence the consumer experience negatively overall by defaulting to basic websites lacking functionality and personalisation because important data used to provide services would not be available. It would automatically influence the consumer experience negatively by removing personalisation of webpages and apps which would lead to a greater degree of adblocking and consequently hurt media budgets and threaten their independence. Moreover, the

Article 29 Working Party Opinion 04/2012 on Cookie Consent Exemption identifies first party cookies which are necessary to deliver a service as an exemption to a consent rule.

OBA self-regulation

EACA is a founding member of the European Interactive Digital Advertising Alliance (EDAA), a cross-industry self-regulatory initiative developed by leading European bodies to introduce pan-European standards to enhance transparency and user control for online behavioural advertising (OBA). The OBA programme is a good example of how the advertising industry is responsibly approaching the privacy issue by giving users a clear choice.
EDAA's principal purpose is to licence the 'OBA Icon' to companies involved in Online Behavioural Advertising across Europe. The OBA Icon is a consumer-facing, interactive symbol that links consumers to an online portal, www.youronlinechoices.eu, where they can find easy-to-understand information on the practice of OBA as well as a mechanism for exercising informed choice – if they so wish, consumers may 'turn off' OBA by some or all companies. EDAA is governed by EU-level organisations which make up the value chain of OBA within Europe and acts to ensure consistency in the European self-regulatory approach. The EDAA's guiding principles are laid out in the Interactive Advertising Bureau Europe (IAB Europe) OBA Framework and the Best Practice Recommendation for Online Behavioural Advertising of the European Advertising Standards Alliance (EASA).
The OBA principles were extended to mobile web-browsing and involved the scope of the Programme to cover the collection and use of: cross-application data, location data and personal device data (such as address book). Companies in the mobile advertising space will be required to provide enhanced notice and choice to consumers with regard to their OBA practices, through the well-recognised 'OBA Icon', and Consumer Choice Platform. A pan-European consumer choice mobile app will be released to improve the user experience when exercising choice on mobile.

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