EUROPEAN ASSOCIATION OF COMMUNICATIONS AGENCIES

GDPR Implementation

Background

In 2012, the European Commission proposed a major reform of the EU legal framework on the protection of personal data, by proposing the General Data Protection Regulation (GDPR) The proposal aims to ensure the same level of protection for data subjects in online and offline environments. The European Parliament adopted its position on 12 March 2014, and the Council of Ministers followed suit on 15 June 2015. The trialogue between the Commission, the Parliament and the Council began in June and agreement was reached on 15 December 2015. Following the political agreement reached in trialogue, the final texts were formally adopted by the European Parliament and the Council at the beginning of 2016. The new rules will become applicable in May 2018.

Agencies have until 25 May 2018 to be fully compliant with the GDPR. Given that it is such a large piece of regulation and that it introduces a lot of new concepts, additional implementation guidance from data protection authorities is required. To that end, the Article 29 Working Party, which represents all European data protection authorities will issue guidelines on how certain unclear provisions should be applied in the future. Here is there working plan.

The following guidelines have been adopted and finalised:

Data portability

Article 20 of the General Data Protection Regulation (GDPR) introduces the new right of data portability. This right allows consumers (data subjects) to receive their personal data, which they have provided to a business provider (data controller), in a structured, commonly used and machine-readable format and to transmit those data to another data controller without hindrance.

Data protection officers (DPO)

Under the GDPR, it is mandatory for certain controllers and processors to designate a DPO. DPOs are supposed to assist their organisations to monitor internal compliance with the GDPR.

Data protection impact assessment (DPIA)

A DPIA is a process designed to describe the data processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (see also Article 24). In other words, a DPIA is a process for building and demonstrating compliance.

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

Identifying a controller or processor's lead supervisory authority

Identifying a lead supervisory authority is only relevant where a controller or processor is carrying out the cross-border processing of personal data. Article 4(23) of the GDPR defines 'cross-border processing' as either the processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Application and setting of administrative fines for the purposes of the GDPR

Under the GDPR, the scope and nature of administrative fines which supervisory administative authorities can impose on non-compliant organisations has significantly increased. Such fines may be up to €20 million or 4% of total worldwide annual turnover (whichever is greater) of the undertaking for breaches of GDPR.

The following guidelines have been drafted, and are still in the making:

Automated individual decision-making and Profiling for the purposes of the GDPR

The GDPR introduces provisions to ensure that profiling and automated individual decision-making (whether or not this includes profiling) are not used in ways that have an unjustified impact on individuals' rights.

Personal data breach notification under the GDPR

The GDPR introduces the requirement for a personal data breach (henceforth "breach") to be notified to the competent national supervisory authority and, in certain cases, communicate the breach to the individuals whose personal data have been affected by the breach.

Guidelines on consent and transparency requirements are expected to be released by the end of the year/beginning of 2018.

EACA actions

EACA supports transparent data collection and processing practices. We believe that consumers should be informed about different data processing practices. EACA members uphold high standards of data protection throughout the whole process. We also believe that legislation should be complemented with self-regulation. EACA is actively participating in all workshops organised by the Article 29 Working Party.