Internet Advertising Bureau UK

DCMS - Call for Views on GDPR derogations

Submission by the Internet Advertising Bureau UK – May 2017

Introduction

1 The Internet Advertising Bureau UK (IAB UK) is the industry body for digital advertising in the UK. It represents over 1200 businesses engaged in all forms of online and mobile advertising, including media owners and advertising technology businesses.

2 We are actively engaged in working towards the optimal policy and regulatory environment for the digital advertising market to continue to thrive. We also seek to promote good practice to ensure a responsible medium. Further information is available at www.iabuk.net.

3 We consider the General Data Protection Regulation (GDPR) the most important policy development for the digital advertising industry in recent years. Our industry sits at the heart of the UK's digital economy and acts as the main driver for funding online services from news and entertainment, to gaming, social media and education at little or no additional cost to citizens at home and abroad.

4 The GDPR will have a profound impact on the digital advertising industry. Government must therefore ensure that the implementation process takes into account the views put forward in this and any subsequent submission on the UK's data protection landscape so that the industry can continue to play its vital role in supporting the ad-funded internet within a new environment shaped by the GDPR and the UK's decision to leave the European Union (EU).

General comments

5 We welcome the opportunity to submit our views on the derogations contained in the GDPR. However, given the significance of the new legislation to our industry and the wider digital economy, we think that this call for views does not suffice in allowing stakeholders to adequately inform the department on the implementation process.

6 We recognise that Government is working to tight timescales for its consultation before implementing the derogations required of it, and, owing to the importance of digital advertising not just to the UK's digital economy but also the UK economy overall, we and our members are very prepared to work with Government to arrive on an effective and practical implementation. As such, we believe that further consultation is required which could be assisted by Government setting out its policy preferences.

7 On a general note, we welcome the aim of harmonising data protection laws across EU markets as a result of the GDPR. Harmonisation can have many benefits to businesses, reducing the number of burdensome administrative and legal hurdles that have been in place since the implementation of the Data Protection Directive 95/46/EC. This said, Member State flexibility can be useful, particularly in those areas where tailored national approaches have proven to be effective or could be beneficial to UK-based businesses as a result of the derogations afforded by the GDPR.

policy@iabuk.net
020 7050 6969
67-68 Long Acre
London WC2E 9JD

Theme 1– Supervisory Authority

8 The Information Commissioner's Office (ICO) has long pursued an enforcement strategy that follows a risk-based and pragmatic approach to applying data protection laws in the UK. We believe this strategy has contributed to a conducive business environment which has allowed the digital advertising sector in the UK to grow from an industry worth £20 million to its current size of £10.3 billon.

9 We think it is critically important that the derogations contained in the GDPR do not undermine the ICO in its ability to continue to follow this pragmatic approach to enforcing data protection rules.

10 The GDPR will likely result in a substantial increase in resources required to deal with the provisions brought in by the new rules. As such, we believe Government needs to put forward a vision on how Article 52 (4) & (6) will be transposed in the UK and consult interested parties on how the ICO's funding can be secured, particularly in light of the removal of notification fees under the GDPR.

11 There are a number of options available to fund the ICO's data protection work. However, we would strongly oppose the idea of the ICO being primarily funded by fines. We have seen the negative impact a funding mechanism underpinned by fines can have in the example of Spain's supervisory authority, AEPD. We strongly believe that this approach sets the wrong incentives and undermines the foundations of a pragmatic and measured approach to data protection enforcement that ideally fosters a climate of mutual respect between the supervisory authority and organisations processing personal data.

12 With respect to Article 58 (6), we believe that further consultation would be required if Government wanted to provide the ICO with additional powers.

13 Article 62 sets out the process supervisory authorities should follow when conducting joint operations. We generally believe that it is important that the One-Stop-Shop mechanism introduced by the GDPR fulfils its promise and delivers on ensuring consistency between approaches taken by supervisory authorities. To that end, it would be helpful to get clarity on the jurisdiction of the ICO in the event where the ICO is conducting operations as a result of breaches occurred outside the UK. It would also be helpful to understand the powers granted to supervisory authorities other than the ICO in situations where breaches originate in the UK.

Theme 3 – Demonstrating compliance

14 We believe that – under certain circumstances – Codes of Conduct can play a valuable role in demonstrating compliance with the GDPR.

15 However, we think that the option to demonstrate compliance via Codes of Conduct as set out in Article 40 should not comprise the ability of the digital advertising industry to

adopt self-regulatory approaches to data protection and privacy that provide added value to consumers and businesses without acting as legal compliance tools.

16 The digital advertising industry has a proven track record in delivering bottom-up self-regulatory solutions that work for consumers and businesses, evidenced by the success of the pan-European initiative for online behavioural advertising (OBA). Devised to provide greater transparency and control to users over the way their data is used, the initiative is now active in 33 European countries, comprising over 120 companies with sister programmes running in the US and Canada. Awareness of the self-regulatory initiative in Great Britain has steadily increased for five consecutive years, from 13% in 2012 to 34% in 2016.[1] More information on the OBA initiative is available at www.edaa.eu and www.youronlinechoices.eu.

17 It is likely that self-regulatory approaches to privacy and data protection will continue to play an important role in the industry's toolkit to provide education and control to users with respect to the use of their data. We believe that where these have not been created as legal compliance tools, supervisory authorities should not assess any such initiatives against the requirements of the GDPR, but rather on the basis of their value to users and businesses.

Theme 4 – Data Protection Officers

18 Under certain conditions, companies are obliged to appoint a Data Protection Officer under the GDPR as set out by Articles 37 – 39. The GDPR's provisions on DPOs already provide a prescriptive and broad approach to the position of and the need for DPOs and we think that Government should avoid any attempt to go further than what the GDPR requires.

Theme 6 – Third country transfers

19 We believe that unimpeded cross-border data transfers between the UK and the EU and the UK and the US play a crucial role in the continued success of the UK's digital advertising industry, and the wider digital economy. The UK digital advertising market is by far the most advanced digital advertising market in Europe, commanding a bigger share of advertising spend than the next two biggest European market (Germany and France) combined.

20 Advertisers often run their European (and global) digital advertising campaigns out of the UK by partnering with advertising technology providers based here. As part of these deals, data processing is required to support and drive these cross-border campaigns, often managed out of the UK.

21 It is therefore critical for the future of the digital advertising industry in the UK to retain the ability to transfer data across borders with as little obstruction as possible. We

have previously urged Government to make this issue a priority in the negotiations to leave the EU and continue to believe that achieving an adequacy decision from the European Commission and working on an agreement with the US along the lines of the EU – US Privacy Shield would provide the most effective solutions for post-Brexit Britain.

22 For the purpose of this consultation, the above also means that Government should aim to work towards harmonisation in the context of Article 49 and be mindful not use derogations on third country transfers in a way that could compromise the ability to achieve adequacy post-Brexit.

Theme 7 – Rights and remedies

23 Article 22 (2) (b) of the GDPR allows Member States to authorise by law decisions that are based solely on automated processing, including profiling, which produce legal effects concerning data subjects or similarly significantly affect them.

24 We think that Government should not use this derogation to introduce requirements that go beyond Article 22 (1). We believe that no attempt should be made at national level to divert from the intention of Article 22 (1), i.e. to regulate decisions solely based on automated processing that produces the effects mentioned above.

Theme 8 – Processing of children's personal data by online services

25 Article 8 (1) provides Member States the opportunity to lower the age threshold for processing the personal data of children to 13 for the purpose of offering information society services.

26 We strongly believe that Government should make use of this flexibility and set the age at 13 years old. We also support the harmonisation of rules to avoid fragmentation across EU markets and Government should work together with other EU national governments to achieve a harmonised approach on this issue across EU markets.

27 Differing rules on the age of consent in EU member states, as well as between the EU standard and the COPPA age 13 rules applicable in the US, will create significant challenges for companies that offer international services.

28 The UK is a key market for many international services, many of them funded by advertising such as social media platforms. In fact, the vast majority of today's ad-funded digital services available in the UK today – including social media and entertainment sites, music streaming sites and webmail – are built upon the existing UK approach to the age of a child which recommends that parental consent should be

obtained for young children (12 years and under) for the collection of personal data (e.g. name, address or email address).[1]

29 Raising the age of consent from 13 to 16 would have far-reaching consequences, such as:

- Denying many digital services to children under the age of 16 years, as well as establishing an obstacle in the educational development of teenagers (e.g. on privacy issues);
- Preventing many legitimate businesses from offering goods and serves – designed for children, to children – moving them to sites that are less appropriate;
- Creating a barrier between teenagers and vital health / support services, as well as denying teenagers from expressing their right to free speech and from engaging in online discussions;
- Overlooking decades of industry good practice around offering online content and services to teenagers. For example: the existing EU self-regulatory approach prohibits the targeting of behavioural advertising specifically at children under the age of 13 years (see more above); and
- Creating additional and impractical burdens on many digital businesses when processing personal data for advertising purposes, particularly where the age of the user is not known.

Cost impact

30 We are unable to comment on the cost impact of any derogation seeing that without concrete policy proposal this would be a matter of speculation. We believe that Government should consider preparing an impact assessment on the basis of which we should be able to provide feedback.

For more information about this response, please contact Yves Schwarzbart, Head of Policy and Regulatory Affairs at yves@iabuk.net

[1] See https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf