Internet Advertising Bureau UK

The EU General Data Protection Regulation (GDPR)

A briefing for the digital advertising industry

Contents

Introduction

Introduction

- On 27 April 2016, the European Union (EU) formally adopted the EU General Data Protection Regulation (GDPR) (EU Regulation 2016/679), a new legal framework for governing the use of personal data across EU markets.

- The aim of the new law is to update the existing EU data protection legal framework in light of today's digital world. The full text of the new law is available at: po.st/BXClww

- The GDPR will apply across all EU markets from 25 May 2018**.** The GDPR will repeal and replace existing national data protection laws across the EU. However these continue to apply until then.

"The GDPR will apply across all EU markets from 25 May 2018"

- As an EU Regulation it applies directly and equally in all EU countries thereby seeking to avoid local fragmentation and to meet one of the new law's stated aims: a consistent level of protection for citizens and a streamlined approach for businesses across EU markets in the spirit of 'one continent, one law'. However, there are a number of areas where there will be greater flexibility at national level, such as at what age parental consent will be required to collect personal information from a child.

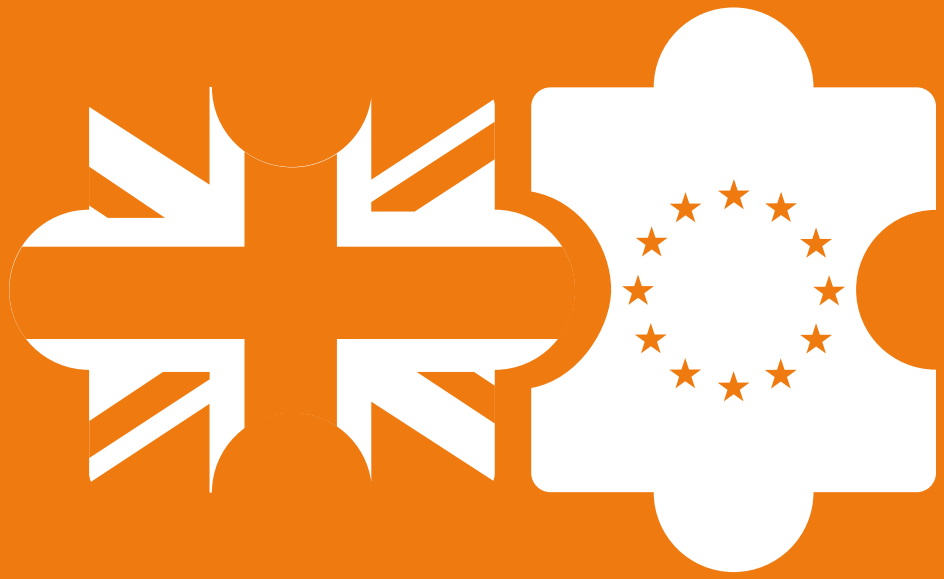
- The GDPR will apply when (a) an organisation is offering goods or services to individuals in the EU, regardless of whether a payment is used; and (b) when an organisation is monitoring an individual's behaviour in the EU. Therefore when an organisation is processing the personal data of individuals based in the EU then the new law applies regardless of whether the business is located inside or outside the EU.

- The GDPR builds upon the existing legal framework (i.e. the UK Data Protection Act 1998). For digital advertising there are some very significant new aspects that may transform the way data is collected, shared and used. Many businesses may be faced with new obligations for the first time. The GDPR captures the use of personal data in digital advertising. The obligations and liabilities imposed by the GDPR extend to all entities involved in collecting or using personal data.

"For digital advertising there are some very significant new aspects that may transform the way data is collected, shared and used. Many businesses may be faced with new obligations for the first time"

- This briefing outlines the most significant aspects of the GDPR for digital advertising and provides a series of steps organisations should consider taking to prepare.

- The IAB will continue to provide updates to its members, particularly as guidance by local Data Protection Authorities (DPAs), such as the UK Information Commissioner's Office (ICO), as well as the collective group of EU DPAs (known as the Article 29 Working Party (A29WP)), is published.



Brexit: GDPR or New UK Law?

Brexit: GDPR or New UK Law?

- The GDPR will apply directly to the UK from 25 May 2018 if, as is quite likely, it still is a member of the EU. However, whether the GDPR directly applies to the UK when it has left the EU depends entirely on the future relationship between the UK and the EU.

- For example: if the UK remains a member of the European Economic Area (EEA) then the GDPR is likely to apply directly. If the UK is part of the European Free Trade Area (EFTA) or another arrangement then it is likely that the UK will need to pass a new UK law updating the existing 1998 Data Protection Act. This will be required in order to facilitate the transfer of personal data from the EU to the UK.

- The UK's departure from the EU may have implications for compliance and enforcement. If the UK is no longer a member of the EU then the UK may not be deemed an organisation's 'main establishment' for GDPR purposes.

- However, due to its territorial scope, the GDPR will apply directly for the vast majority of digital advertising businesses operating across EU markets, including the UK.

"Due to its territorial scope, the GDPR will apply directly for the vast majority of digital advertising businesses operating across EU markets, including the UK"

The ePrivacy Directive

The ePrivacy Directive

- The GDPR will not supersede the ePrivacy Directive (aka 'the cookie law' – implemented in the UK as the Privacy and Electronic Communication Regulations (PECR)). This law – which sets out rules on the storing of information or gaining access to information already stored on a device (whether personal data or not) – remains in force in the UK as well as other EU countries that have implemented it. See the IAB's FAQs: iabuk.net/eprivacyfactsheet

- Brexit will not affect this as the UK implemented the Directive into national law. However, the European Commission is currently reviewing the ePrivacy Directive to ensure that it is aligned with the GDPR. It is unclear what the final outcome will look like. IAB UK believes that Article 5.3 of the ePrivacy Directive can be repealed as all of its privacy-related obligations are now adequately addressed in the GDPR. See: http://po.st/xpqZau

- If the European Union implements a new ePrivacy law to coincide with the application of the GDPR it will apply directly as long as the UK is a member of the EU. In the long-term, when the UK is not part of the EU, any new Regulation may still apply to the UK. However, similarly to the GDPR, this all depends on the UK's future arrangements with the EU as well as the territorial scope of any future ePrivacy law.

"The GDPR will not supersede the ePrivacy Directive (aka 'the cookie law' – implemented in the UK as the Privacy and Electronic Communication Regulations (PECR))"

The GDPR: 10 Key Areas for Digital Advertising

The GDPR: 10 Key Areas for Digital Advertising

The GDPR regulates the use of all personal data in digital advertising. All organisations engaged in digital advertising – whether brand advertisers, agencies, advertising networks or data / technology businesses or publishers – should be aware of the following:

1. *Scope: The GDPR applies to all personal data*

- The inclusion of an online identifier in the definition of personal data could be interpreted as an expansion of scope on existing law. The UK Information Commissioner's Office (ICO) (see: http://po.st/uSPc4n) says in its overview of the GDPR:

  "…the GDPR's definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people."

- To this extent unique identifiers (e.g. cookies or advertising IDs) should not be assumed to be 'anonymous' or 'non-personally identifiable' unless a valid argument can be made to treat them as such. If such an argument cannot be made, then the data should be treated as personal under the GDPR.

- IAB UK members may find it simplest to treat all online identifiers as personal data under the GDPR. However, this does not prevent members from arguing that they only amount to personal data in certain circumstances.

"IAB UK members may find it simplest to treat all online identifiers as personal data under the GDPR. However, this does not prevent members from arguing that they only amount to personal data in certain circumstances"

- The GDPR also refers to 'special categories of personal data' (i.e. sensitive personal data). These are broadly the same as under the existing legal framework and include the processing of personal data revealing:

  » Racial or ethnic origin
  » Political opinions
  » Religious or philosophical beliefs
  » Trade union membership

- Special categories of personal data also include the processing of genetic data and biometric data for the purpose of uniquely identifying an individual, as well as data concerning health or data concerning an individual's sex life or sexual orientation.

2. *Privacy by Design: The GDPR encourages pseudonymisation*

- The new Regulation introduces the concept of 'pseudonymisation' into EU data protection law (Article 4) to encourage risk reduction. The GDPR defines pseudonymisation as:

  "…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

- Pseudonymisation is therefore a process that personal data can go through – for example encryption, hashing or tokenization techniques – to ensure the data is no longer linked to an identified or identifiable individual. For example, a company could strip out details directly identifying an individual (e.g. name and postal address) from its subscriber data (and keep them separately).

- Personal data that does not have any directly identifying details could also be pseudonymised at the point of collection. For example, a randomised cookie token that allows a user to be recognised but not directly identified.

"Personal data that does not have any directly identifying details could also be pseudonymised at the point of collection. For example, a randomised cookie token that allows a user to be recognised but not directly identified"

- However, it depends on an organisation's operational and / or technical matters. The IAB is exploring how pseudonymisation might apply to the digital advertising sector.

- Organisations that pseudonymise data are alleviated of some of the GDPR's obligations that require identification (such the right to erasure, data portability etc. – see Article 11 of the GDPR). Many of these obligations will not be practical or workable for many digital advertising businesses so how pseudonymisation works in digital advertising will be important.

3. *Territorial Applicability: The GDPR has global significance*

- The new law no longer applies to where the data processing equipment is located but where the individual is located. To this extent, if an organisation is processing personal data about a person who is in the EU (NB this person does not have to be an EU national) then the new law applies regardless of where the business is located.

"The new law no longer applies to where the data processing equipment is located but where the individual is located"

- The GDPR makes that clear by specifying that the new rules will apply if (a) an organisation is offering goods or services to individuals in the EU, regardless of whether a payment is used; and (b) when an organisation is monitoring an individual's behaviour in the EU.

4. *Legal Bases: The GDPR outlines six ways to lawfully process personal data*

- Organisations will require a legal basis to process personal data. There are six legal bases available: consent; contractual; legal compliance; protecting the vital interests of a person; public interest; and legitimate interests.

- The two legal bases most commonly used in the digital advertising sector are consent and legitimate interests.

"The two legal bases most commonly used in the digital advertising sector are consent and legitimate interests"

- The GDPR strengthens the conditions for consent when used to process personal data: When relied upon as a legal basis for the processing of personal data, consent will need to meet very high standards (e.g. it cannot be bundled with T&Cs). The user will also need to give consent "unambiguously" with an affirmative action. Processing "sensitive" (e.g. racial or ethnic origin / sexual orientation) personal data requires the explicit consent of the user.

"The GDPR strengthens the conditions for consent when used to process personal data"

- Where consent to process personal data has been obtained prior to the application of the GDPR (i.e. under the current legal framework), it is not necessary for the individual to give his or her consent again as long as it has been obtained in line with the new GDPR requirements.

- In all cases, evidence that the consent has been obtained will have to be recorded. Where there is no direct relationship with the user, the organisation will have to find a way to obtain the consent indirectly. The ICO is expected to publish further guidance on consent.

- The European Commission is currently revising the ePrivacy Directive to ensure it is aligned with the GDPR. The conditions for consent in any revision of the ePrivacy Directive will derive from the GDPR.

- Legitimate interests can be relied upon as a legal basis to process personal data but organisations will need to balance these with the rights and interests of the individual: The GDPR permits the processing of personal data when it is in the legitimate interests of an organisation.

"Legitimate interests can be relied upon as a legal basis to process personal data but organisations will need to balance these with the rights and interests of the individual"

- The recitals in the GDPR specifically state that these purposes include:

  a) Where there is a relationship between the organisation and the individual (e.g. subscription service);
  b) For internal administration purposes (e.g. client / employee data) [NB international transfer rules would still apply];
  c) The prevention of fraud;
  d) Network security (e.g. preventing unauthorised access to a network);
  e) Meeting legal obligations (e.g. reporting criminal acts to an authority); and
  f) Direct marketing [NB: there is no definition of direct marketing in the GDPR and it is unclear how it might apply to many digital advertising disciplines].

- In order to use this legal basis, organisations will have to carry out a balancing test, weighing their interests to process personal data against the interests, fundamental rights and freedoms of the individual. As part of this assessment, organisations will have to consider whether individuals would reasonably expect their personal data to be processed based on the relationship they have with the organisation but also how their data is processed.

- Overall, key to using legitimate interests as a legal basis is that the interests, fundamental rights and freedoms of the individual are not overridden. It will be the responsibility of the data controller(s) to justify and document the decision, and include its use in an information or privacy notice. This is particularly the case if processing children's personal data. The individual also has the right to object at any time.

- The Article 29 Working Party has, in the past, regarded this legal justification as unsuitable for a large part of the digital advertising sector, particularly if personal data is used to specifically target an ad at a group of users. Pseudonymisation, as well as the increased rights offered to individuals under the GDPR, may make this a more attractive legal basis for parts of the sector moving forward. However, digital ad businesses will still have to comply with the ePrivacy Directive (or its replacement unless it is repealed) that requires the consent of the user.

5. Obligations for Data Controllers and Data Processors:

- The GDPR applies to both 'data controllers' (i.e. an organisation that decides how and why personal data is processed) and – for the first time – 'data processors' (i.e. an organisation that specifically acts on a controller's behalf). It also includes the concept of 'joint controllership' for situations where two or more data controllers determine the purposes and means of processing of personal data.

- Businesses involved in the processing of personal data for digital advertising purposes will be classified as either a data controller or a data processor under the GDPR. Both have obligations and therefore it is important for organisations to clarify their role as either a data controller or data processor or, in some cases, both.

"Businesses involved in the processing of personal data for digital advertising purposes will be classified as either a data controller or a data processor under the GDPR"

- Obligations for data controllers include:

  a) Transparency: The GDPR extends the amount of information organisations must provide to individuals about how they use personal data (e.g. an organisation's legal basis for processing personal data, data retention periods, the use of third party data etc.). This information will usually be provided in a Privacy Notice. In cases where it does not have a direct relationship with the user, the organisation will need to determine how it will achieve the transparency requirements. The ICO is expected to publish a revised Code of Practice on Privacy Notices.

  b) Accountability: The GDPR introduces new accountability obligations for organisations (e.g. documenting what personal data is held, recording compliance and, where appropriate, conducting Data Protection Impact Assessments (DPIAs)).

- The GDPR includes - for the first time - direct obligations for data processors. Data processors will be liable for non-compliance or breaches.

"The GDPR includes – for the first time – direct obligations for data processors. Data processors will be liable for non-compliance or breaches"

- These also include accountability obligations (e.g. maintaining records of processing activities carried out of behalf of a data controller). Data processors will be required to have a written contract with the data controller and this will set out the obligations and responsibilities.

- Where two or more organisations are joint controllers, the GDPR states that, between them, they must agree obligations and responsibilities (e.g. where notice and consent is obtained). This is particularly helpful for the digital advertising sector where – for example – many data controllers may be operating on one digital property, or where third party data is purchased.

"Where two or more organisations are joint controllers, the GDPR states that, between them, they must agree obligations and responsibilities (e.g. where notice and consent is obtained)"

- Such a contract must contain sufficient detail to specify responsibilities and obligations under the GDPR, including a designated point of contact for the user. A summary of the contract must be made publicly available and both joint controllers will be individually liable for compliance with the GDPR. An individual is entitled to enforce their rights against either.

- Regulators are expected to publish further guidance on the data controller / data processor relationship.

- Organisations will need to complete a Data Protection Impact Assessment (DPIA) if they process personal data using 'new technologies' or if the personal data processing is likely to present a 'high risk' to the user. The intention behind this is to help organisations build privacy good practice into the product cycle and help them comply with the law. This assessment will need to take place before any data processing and will require consultation with the Supervisory Authority (NB the new name for a Data Protection Authority) to ensure compliance with the GDPR.

"Organisations will need to complete a Data Protection Impact Assessment (DPIA) if they process personal data using 'new technologies' or if the personal data processing is likely to present a 'high risk' to the user"

- In the UK the ICO has already published guidance on Privacy Impact Assessments under the existing legal framework – http://po.st/aL1TiH and it is likely to update this. The A29WP is also expected to provide guidance on this.

6. The Data Protection Officer (DPO): The GDPR introduces the new role

- All data controllers and data processors processing personal data that requires "regular and systematic monitoring of data subjects on a large scale" will need to hire a Data Protection Officer (DPO) (Articles 37-39).

"All data controllers and data processors processing personal data that requires 'regular and systematic monitoring of data subjects on a large scale' will need to hire a Data Protection Officer (DPO) (Articles 37– 39)"

- The GDPR doesn't specify the DPO's precise credentials but he or she should be an expert in data protection law and practices. A DPO is expected to inform and advise an organisation and its employees about their obligations under the GDPR / privacy law; monitoring compliance and advising on impact assessments; as well as being the first point of contact for Supervisory Authorities as well as employees / customers.

- The DPO is granted a special status within an organisation (he or she can't be removed for performing the role!). He or she should report to the Board but work independently and be given adequate resources to meet their obligations. An existing employee can perform the role or it can be contracted out.

- The A29WP is expected to provide further guidance on the role of DPOs.

7. Individual Rights & Control: The GDPR seeks to give people greater control

- The GDPR aims to put individuals more in control of their personal information. This is reflected in the strengthening of the consent provisions (see previous) as well as significantly reinforced individual rights, such as the right to erasure (often understood to be the 'right to be forgotten') (Article 17), the right to data portability (Article 20) and the right to object (Article 21). The ICO will be publishing further guidance on individual rights and the A29WP is expected to publish guidance specifically on data portability.

"The GDPR aims to put individuals more in control of their personal information"

- The GDPR introduces a specific user right not be subject to a decision based solely on automated processing, including profiling. [NB This is a separate right to the right to object that includes profiling for direct marketing purposes] Individuals will have the right not to be subjected to profiling or the 'automatic processing of personal data' (Article 22) where it may cause 'legal effects concerning him or her or similarly significantly affects him or her' (e.g. automatic refusal of a credit application). Profiling is defined as including an individual's personal preferences, interests, behaviour, and location or movements, so it is likely to include behavioural or interest-based advertising.

"The GDPR introduces a specific user right not be subject to a decision based solely on in automated processing, including profiling"

- Where automatic processing, including profiling, does cause legal or similarly significant effects the explicit consent of the user will be required, unless there is a contract in place or a national law permitting it (e.g. for the monitoring of tax evasion). Automated processing is prohibited where a child is concerned or if sensitive personal data is being processed (unless the user has given his / her explicit consent). The ICO / A29WP is expected to publish further guidance on automated processing, including profiling.

8. Children: The GDPR introduces special protection for their personal data

- The GDPR introduces special protection for children's personal information: If an organisation collects information about a child and is relying on consent to process it lawfully then it will need a parent's / guardian's consent in order to process the information lawfully where the child is under 16 years old.

"The GDPR introduces special protection for children's personal information"

- Please note that, according to the GDPR, it is up to EU Member States to determine the child's age when this consent is required so long as this is not below 13 years old. It remains to be seen if the UK decides to make use of this flexibility.

9. Compliance & Enforcement: A One-Stop Shop

- The GDPR significantly increases the sanctions available to regulators: EU Supervisory Authorities will be able to fine organisations up to €20m or 4% of annual turnover (whichever is greater) in the event of a breach of the law in the UK. Under the current law, the ICO can issue fines of up to £500K for serious breaches so these new fining powers will be a real game-changer.

"The GDPR significantly increases the sanctions available to regulators: EU Supervisory Authorities will be able to fine organisations up to €20m or 4% of annual turnover (whichever is greater) in the event of a breach of the law in the UK"

- The GDPR seeks to create greater consistency in enforcement across EU markets: where organisations are processing personal data across all or many different EU markets, they will be 'monitored' by a lead supervisory authority but in co-operation with other supervisory authorities concerned. The lead supervisory authority will be located in the EU country where an organisation has its main or single establishment. In practice this means that several supervisory authorities will work together on issues rather than one alone, particularly when these are cross-border in nature. The A29WP is expected to provide further guidance on the main establishment and the role of the 'lead' supervisory authority.

"The GDPR seeks to create greater consistency in enforcement across EU markets"

- As a result of Brexit, those organisations with their European headquarters in the UK may have to consider their 'main establishment' for data protection purposes elsewhere in the European Union.

- The GDPR beefs up the Article 29 Working Party: The Article 29 Working Party, the group of all EU DPAs, will be replaced by the European Data Protection Board (EDPB) which shall 'ensure the consistent application' of the new law. The EDPB will issue legally enforceable guidance and be able to determine disputes between national supervisory authorities.

"The GDPR beefs up the Article 29 Working Party"

- The GDPR allows for industry self- and co-regulation: The new law encourages the drawing up of Codes of Conduct 'to contribute to the proper application' of the GDPR. The GDPR also allows for the establishment of data protection certification schemes, including marks and seals. It remains to be seen how the EU Industry Initiative for Online Behavioural Advertising (i.e. AdChoices – www.edaa.eu) might fit into this but – for now – it still represents a way for digital advertising businesses to deliver transparency and control to European citizens.

"The GDPR allows for industry self- and co-regulation"

10. International Data Transfers:

The GDPR allows for international data transfers (Article 44): The GDPR allows for the transfer of data to third countries outside the EU/EEA, including:

- Where the European Commission has decided through a so-called 'adequacy decision' – that a third country provides an adequate level of protection of personal data; or
- Where necessary safeguards are in place. These include binding corporate rules, standard data protection contract clauses or a code of conduct with the third party or a certification mechanism that applies the appropriate safeguards; or
- Where the explicit consent of the individual has been obtained, after having been informed of possible risks in the absence of an adequacy decision or appropriate safeguards.

The EU-U.S. Privacy Shield – itself an 'adequacy decision' – has replaced the Safe Harbour mechanism for data transfers between the EU and U.S. See IAB UK's FAQs: iabuk.net/eusafeharbour. The ICO / A29WP is expected to publish guidance on international transfers following stakeholder consultations. NB The EU-U.S. Privacy Shield is based on the current legal framework for data protection in Europe so it may need updating once the GDPR applies.

"The GDPR allows for international data transfers"

Five Things To Consider Now:

1. **Get GDPR Proficient**: Familiarise yourself with the new rules and what they might mean for your organisation. Raise internal awareness: changes are likely to be needed. IAB UK will be hosting a series of events to help raise awareness of key obligations.

2. **Designate a Responsibility Lead**: Assign responsibility for transition to a member of staff within your organisation. They should bring together key departments / teams and have senior buy-in. They should also be allocated budget and resources for an assessment and any solutions required.

3. **Develop a Compliance Roadmap**: Take stock / assess current practices, technologies and workflows, as well as any existing privacy solutions (e.g. AdChoices).

4. **Engage with Key Trade Bodies:** The ICO suggests keeping engaged with key trade bodies, such as the IAB, as it will be working closely with them in the implementation of the GDPR. IAB UK will be exploring key areas, such as pseudonymisation.

5. **Follow your local Data Protection Authority (DPA)**: They will be a valuable source of guidance. For example, the UK ICO has a dedicated section of its site for the GDPR – https://ico.org.uk/for-organisations/data-protection-reform/

Further Information

- UK Information Commissioner's Office (Overview of GDPR): https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
- UK Information Commissioner's Office (12 preparatory steps): https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- UK Information Commissioner's Office (what to expect and when): https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/
- The EU Article 29 Working Party (EU guidance): http://ec.europa.eu/justice/data-protection/article-29/index_en.htm
- IAB UK FAQs on GDPR: https://www.iabuk.net/policy/briefings/eu-general-data-protection-regulation-gdpr-faqs-updated-july-2016

Acknowledgements

This briefing was produced by the IAB UK Regulatory Affairs and Public Policy team, with the support of the IAB UK's Public Policy consultant, Nick Stringer.

Internet
Advertising
Bureau
UK

Follow us: @iabuk
Email: info@iabuk.net
Visit us: www.iabuk.net
Call us: 020 7050 6969

Published October 2016