The EU's new data protection regime

Key implications for marketers and adtech service providers

Nick Johnson and Stephen Groom

11 February 2016

General Data Protection Regulation ("GDPR") timeline

24.10.95	Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data ("**DPD**") signed off
24.10.98	DPD implementation deadline
05.01.12	First draft of General Data Protection Regulation ("**GDPR**")
12.12.15	European Parliament and EU Council of Ministers ("**Council**") reach political agreement on a compromise GDPR text
Mar 2016?	Formal adoption by the European Parliament and Council
Jul 2016?	After approval of all EU official language translations publication in the Official Journal
Jul 2018?	GDPR comes fully into force

GDPR: general key features and impacts

GDPR general key features and impacts #1

A new dimension in privacy control

- High level of **complexity**
- Packed with **stricter** requirements
- **DPD**: 25 pages, 72 Recitals and 34 Articles
- **GDPR**: 204 pages, 135 Recitals and 91 Articles

GDPR general key features and impacts #2

The headline changes: harmonised and higher sanctions

- **DPD**: "*Member states shall lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive*."
- **GDPR**: Fines up to *(Article 79)*:

Higher of €20m or <4% of worldwide turnover	Breaches of conditions for consent and other basic processing principles (Arts 5,6,7,9), rights of data subjects ("DSs") (Arts 12-20), ex EEA transfer rules (Arts 40-44) and breaches of Data Protection Authority ("DPA") orders under "corrective powers" in Article 53
Higher of €10m or <2% of worldwide turnover	Data controller or data processor breaches of Articles 8,10,23-37, 39 and 39a

GDPR general key features and impacts #3

The headline changes: extra extraterritorial effect

DPD: Member state ("MS") data protection laws apply where:

1. the processing of personal data ("Processing") is carried out **in the context of the activities of an establishment** of the Controller on that MS's territory or
2. the Controller is not established on EU territory but **makes use of equipment situated in that MS** for Processing unless this is only for transit purposes

GDPR: applies to processing of personal data ("PD") of DSs in the EU:

1. in the context of the activities of an establishment of a Controller or Processor in the EU, **regardless of whether the Processing takes place in the EU**
2. by a Controller or Processor **not in the EU**, where the Processing relates to:
   - the **offering of goods or services to DSs in the EU**, whether or not payment required or
   - the **monitoring of their behaviour** as far as the behaviour takes place **within the EU**

GDPR general key features and impacts #4

Controller/Processor relationships, responsibilities and processes: an exponential increase in regulation

- **Controller/Processor relationship** much more **heavily regulated** *(Article 26)*
- Processors for the first time (in the UK) **directly responsible** for compliance (and paying the penalty) in many areas including:
  - only Processing under a **binding and compliant agreement** with a Controller *(Article 26)*
  - **Not sub-contracting** Processing **without Controller consent** *(Article 26)*
  - **maintaining records** of all categories of Processing for Controllers *(Article 28)*
  - **data security** and **breach notification** *(Articles 30 and 31)*
  - appointing a **data protection officer** where its core activities involve, on a large scale, regular and systematic monitoring of data subjects or processing of special categories of data *(Article 36)*
  - **monitoring** of behaviour of EU DSs by **non EU Processors** *(Article 3)*
  - **transfers** of PD out of the EU *(Articles 40-44)*

GDPR general key features and impacts #5

Data security and breach notification: processes, systems and high vigilance essential

- New list of possible measures for **Controllers and Processors** to implement to ensure a level of security which is "**appropriate to the risk**," including *(Article 30)*:
  - *a process for **regularly testing**, assessing and evaluating the effectiveness of technical and organisational data security measures;*
  - *the **ability to restore** the availability and access to data in a timely manner in the event of a physical or technical incident .*
- "Personal data breaches" ("PDBs") to be reported within **72 hours**. PDB definition:
  - *a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (Article 31).*
- **Affected DSs** must also be notified **without undue delay** if rights and freedoms put at **high risk** *(Article 32)* but see exceptions at Article 32.3.

GDPR general features and impacts #6

Cross-border data transfers: more "gateway" options but these still need work

Main DPD PD transfer rules and derogations unchanged, but…

- New "derogation" in Article 44 allowing ex EEA PD transfers where the other standard derogations could not be used, provided the transfer is:
  - **not repetitive**, concerns only a **limited number** of DSs, is necessary for the purposes of **compelling legitimate interests** of the Controller **not overridden** by the interests, rights or freedoms of the DS, where the Controller has **assessed all the circumstances**, adduced **suitable safeguards**, **informed its DPA** and **notified the DS** of the **transfer** and the "**compelling legitimate interest**" of the Controller
- The "Codes of Conduct and Certification" Article 38 offers another derogation:
  - **associations** representing **categories of Controllers or Processors** (e.g. marketers or adtech service providers) may **obtain approval** of their national DPA to **codes of conduct** specifying the application of listed GDPR provisions, including the data transfer provisions. If member Controllers or Processors give **binding commitments** to comply with these and **authorisation procedures** are followed, relevant transfers could thereby be legitimised

GDPR general features and impacts #7

"One stop shop": fatally diluted by Article 51a 2a?

- Controllers or Processors with establishments in > one EU state will be able to **deal primarily** with their "**lead supervisory authority**" ("LSA") *(Article 51)*
- This is the DPA of the EU state of their "**main establishment**" ("ME")
- For **Controllers** *(Article 4)* this is the EU state where their "**central administration**" ("CA") sits unless decisions on the purposes and means of the Processing are taken in **another establishment** of the EU which has the power to have these implemented, in which case the latter will be regarded as the ME
- For **Processors** *(Article 4)* the CA rule applies, but if there is no CA in the EU, their ME will be the EU state where the **main Processing activities** in the **context** of the activities of an establishment of the Processor take place to the extent that the Processor is under specific GDPR obligations
- But regardless of who is the LSA, **any DPA** shall be **competent** to deal with a complaint lodged with it if the subject matter relates **only** to an **establishment in that state** or **substantially affects** only DSs there *(Article 51a 2a)*

GDPR general key features and impacts #8

Enhanced data subject rights: could Article 76 change the enforcement game?

- **Wider access and info rights**: e.g. right to obtain, "where possible," info about the envisaged PD storage period and if not possible, the criteria used to determine this period (Article 15).
- New **right to erasure** (Article 17) builds on and expands the "right to be forgotten" recognised by the ECJ in Google Spain v Gonzalez.
- New right to **data portability** allowing individuals to move their PD from one service provider to another in a prescribed, user-friendly format (Article 18).
- "Representation of data subjects" Article 76 creates **a class action threat**. MSs:
  - **must** give DSs the right to mandate non-profit associations or organisations whose statutory objectives are in the public interest and are "active" in the field ("NPOs") to pursue GDPR breach complaints and claims on their behalf and
  - **may** provide that even without the go-ahead of an affected DS, NPOs can bring such complaints/claims if they consider that DSs' rights have been infringed.

GDPR: marketing-related key features and impacts

GDPR marketing-related key features and impacts #1

Revised definitions of personal data and special categories of personal data

- **Personal data**

  "Any information relating to an identified or identifiable natural person; an identifiable person is one who, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, economic, cultural or social identity of that person." *(Article 4(1))*

- **Special categories of personal data**

  "Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data in order to uniquely identify a person or data concerning health or sex life and sexual orientation." *(Article 9(1))*

GDPR marketing-related key features and impacts #2

Consent: it could have been a lot worse but watch out for Article 7(4)

Consent: Any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed *(Article 4)*

- In DPD, **consent must already be "unambiguous"** (1) where consent as opposed to for example "**legitimate interests**" is used as a basis for fair and lawful processing and (2) where consent instead of e.g. standard contractual clauses, is used as a basis for **ex EEA transfers**
- But how will the new GDPR consent definition play out in the context of the **Privacy and Electronic Communications Directive** e.g. will "implied consent" still work for **cookies**?
- Requests for consent to Processing must be "**clearly distinguishable**" from any other matters in a written document and provided "**in an intelligible and easily accessible** form, using **clear and plain language**"
- In assessing if consent has been freely given, "**utmost account**" shall be taken of whether the performance of a **contract**, including the provision of a service, is made **conditional on consent** to processing of personal data that is **not necessary** for the performance of the contract *(Article 7(4))*

GDPR marketing-related key features and impacts #3

Children: fudged age harmonisation attempt and tech-related parental consent verification standard will pose challenges

Where **information society services** are offered **directly to a child**,

- the processing of PD of a child **below the age of 16** years
- or **if provided for by Member State law**, a **lower age** which **shall not be below 13 years**

shall only be lawful to the extent that **consent is given or authorised by the holder of parental responsibility** over the child

In such cases, the Controller **shall make reasonable efforts to verify** that consent is given by the holder of parental responsibility over the child, **taking into consideration available technology** (Article 8)

GDPR marketing-related key features and impacts #4

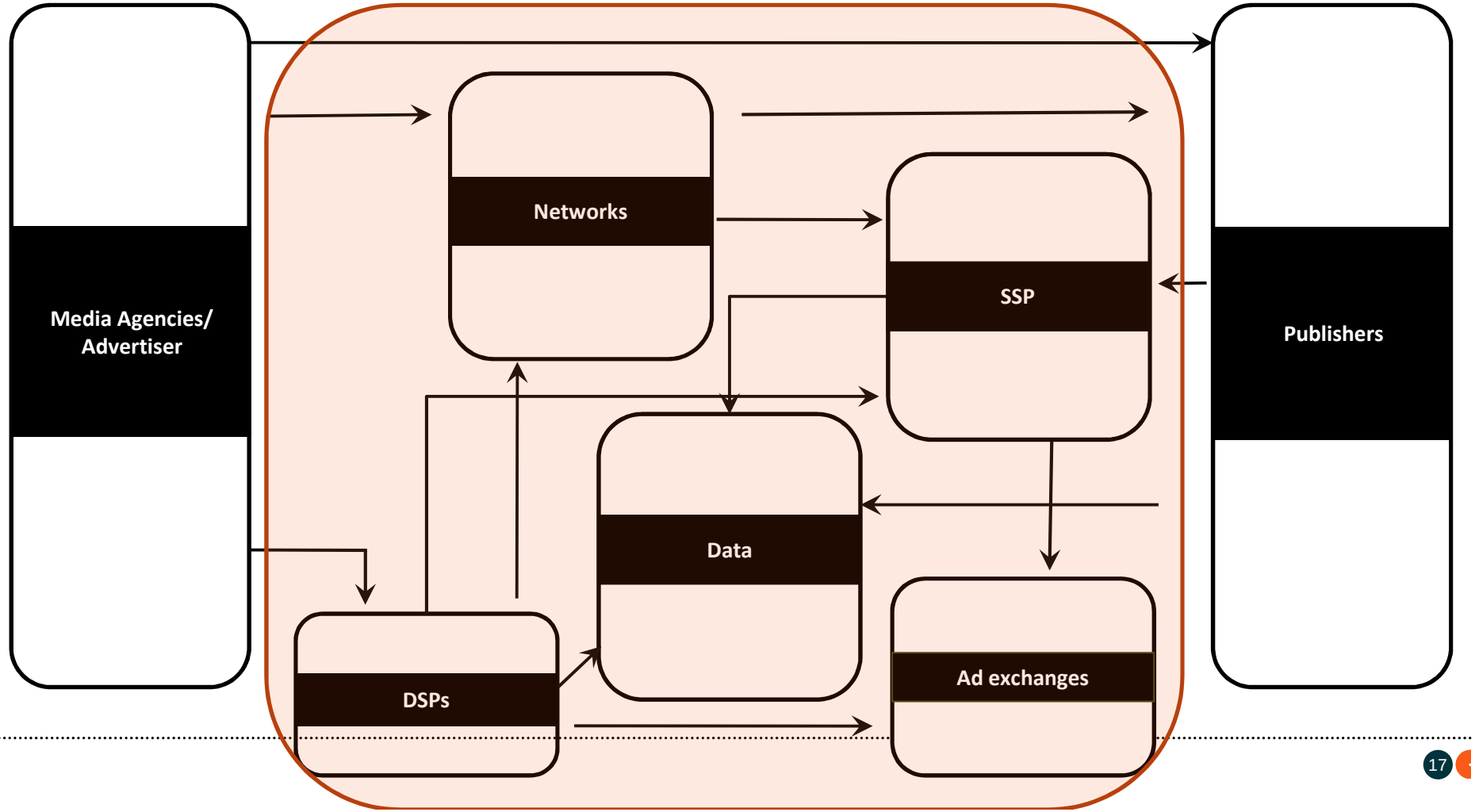
A new set of rules around Controller/Processor accountability

- New obligation on Controllers to implement "**appropriate data protection policies**" where this is **proportionate** in relation to the contemplated Processing *(Article 22)*
- New obligation on Controllers & Processors to **keep records of Processing activities.** Replaces registration with DPAs. Records must cover mostly the same basics as the existing registration system *(Art.28)*. Could this be a pretext for a new **ICO registration system**?
- A new "**Data protection by design and by default**" principle *(Article 23)* dictates that subject to various factors including the state of the art, implementation cost and the level of risk , Controllers must implement **appropriate technical and organisational measures** designed to integrate necessary safeguards into all Processing activities (1) when the means for Processing is decided and (2) when the Processing occurs
- A new obligation on Controllers to carry out pre-Processing **Data protection impact assessments** *(Article 33)* when Processing, particularly using **new technology**, is likely to result in **high risk** to DS rights. More on this in the Adtech section…

The GDPR and adtech businesses

Adtech: "behind-the-scenes" entities

Processing data without direct data subject contact



"Cookies law" still applies
ePrivacy Directive 2002/58/EC

Additional GDPR obligations not applicable where processing subject to specific obligations with same aim in 2002/58/EC *(Art 89)*

So consent rules for simply setting/ accessing cookies arguably unaffected (Cf processing outside scope of ePrivacy Directive)

But could local courts/DPAs seek to apply GDPR standards? Also, ePrivacy Directive review now going ahead

Are "personal data" being processed?

GDPR definition of "personal data"

Personal data: "any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, economic, cultural or social identity of that person" *(Article 4 (1))*

"Individuals may be associated with online identifiers, such as Internet Protocol addresses… [and] cookie identifiers… This may leave traces which… may be used to create profiles of the individuals and identify them" *(Recital 24)*

Are "personal data" being processed?

IP addresses, cookie data etc

- ***Data about unique users:*** Data about a unique user is likely to be "personal data" even where you don't know their name and can't contact them.

- ***Current positions in some member states:*** Some DPAs/courts have already held that IP addresses, mobile device identifiers and in certain cases cookie IDs qualify as personal data.

- ***Judgment expected on IP addresses:*** Further clarification on IP addresses expected from CJEU in Case C-582-14, *Breyer*.

Grounds for lawful processing

Is consent feasible; is "legitimate interests" relevant?

- ***Grounds for lawful processing:*** As under DPD, consent and "legitimate interests" both available as grounds

  - ***Consent:*** Hard to see how behind-the-scenes adtech businesses can realistically get prior consent to GDPR standards

  - ***Legitimate interests:*** Some EU DPAs have been resistant to the idea of adtech data processing falling within scope of "legitimate interests" under DPD – but position under GDPR may be different

Legitimate interests

Changes under the GDPR

Direct marketing called out: "Processing for direct marketing purposes may be regarded as carried out for a legitimate interest" *(Recital 38)* – though no corresponding express statement in relation to targeted online advertising

Shift in balancing exercise to assess legitimate interests: Position changed due to stronger protections for individuals under GDPR?

- Easier opt-out from processing carried out under "legitimate interests" ground – if individual objects, business must now prove "compelling legitimate grounds" over-riding individual's interests
- More transparency and more control for data subjects

Legitimate interests: limits

Even if "legitimate interests" may be relevant…

Profiling activities leading to "legal effects" for or that "significantly affect" individuals generally need ***explicit prior opt-in consent***

Sensitive personal data needs ***explicit consent*** if it hasn't been "manifestly made public" by data subject and no other exception applies

Existing consent requirements for **setting/accessing cookies** under the ePrivacy Directive still apply and may yet evolve…

Disclosure challenges

Enhanced transparency requirements

- ***Directly obtained data:*** Where personal data obtained direct from data subject, disclosures required at time of collection inc: your and your DPO's contact details, details of legal basis for processing, how long data to be stored, rights to object to processing and "meaningful information about the logic involved" in any profiling and its significance/consequences *(Art 14)*
- ***Indirectly obtained data:*** Where data not obtained direct and disclosure "impossible or would involve disproportionate effort", controller may instead use other "appropriate measures" – eg disclosure on own website *(Art 14a)*
- ***Rights to object:*** However, separate obligations to notify individual of rights to object to profiling, processing for direct marketing and "legitimate interests" processing are not subject to the same "disproportionate effort" exemption: info must be given separately from other information and "at the latest at the time of the first communication with the data subject" *(Art 19)*

Data processor and joint controller changes

Positioning yourself as a mere data processor no longer so useful for avoiding DP liability

Joint controller concept will now be recognised across all EU member states

Opportunity to agree formal split of responsibilities, eg as between publisher and adtech provider?

What do you need to do?

What do you need to do?
A non-exhaustive list (1)

Project planning:	Establish multi-disciplinary team; scope work and timescales; allocate responsibilities; negotiate resource/budget
Data flows:	Review what data is likely to be seen as "personal data" under the GDPR and map data flows
Data Protection Officer:	Assess if you need a DPO and train/hire as required
Impact assessment:	Assess if your processing is high risk, requiring a formal assessment
Privacy notice:	Review and amend to meet GDPR requirements
Third party contracts:	Review liability caps and data protection provisions
Record-keeping:	Review record-keeping processes for compliance with GDPR
Breach notification:	Ensure adequate processes in place to deal with notification duties

What do you need to do?
A non-exhaustive list (2)

Controller/processor status:	Assess position of your business and its partners under GDPR, inc joint controller status
Grounds for processing:	Assess whether "legitimate interests" may be an appropriate justification for processing: consider additional measures to support this position, inc pseudonymisation, enhanced notice etc
Consent mechanisms:	Amend as necessary to comply with GDPR requirements: - do tick-box consents need to be split out? - is it just as easy to withdraw consent as to give it?
Conditional consent:	Assess incentives offered for data capture: could any be vulnerable to challenge under GDPR?
Industry developments:	Keep an eye on industry-wide initiatives – codes of conduct, development of the EDAA framework etc

Any questions?

Nick Johnson
Partner

+44 (0) 20 7105 7080
nick.johnson@osborneclarke.com

Stephen Groom
Consultant

+44 (0) 20 7105 7078
stephen.groom@osborneclarke.com

marketinglaw.osborneclarke.com