Key Takeaways on the General Data Protection Regulation (GDPR)

Effective 25 May 2018. Fines for violation*: € 20,000,000 or 4% global annual turnover*.

Our Privacy Committee has been holding monthly calls all year (plus 4-5 last year) to focus on GDPR issues. There are many and not easy to summarize. We began compiling all the material from our sessions and guest presenters with the intention to post it all, plus recordings, on the Privacy program page.

However, it became unwieldy and potentially confusing, so we are doing something different. We have officially joined the Future of Privacy Forum (the Executive Director, Jules Polonetsky, has been a guest expert at numerous MMA Summits and Forums) and we will be jointly preparing some material for the MMA site. Specifically, we will first focus on the "top 10 things brands need to know about GDPR.".

MMA has also prepared a high-level summary of key aspects of the GDPR, which will educate you a bit, but it is by no means the authority on the topic. As they say, consult counsel before taking any firm action from our documents.

We will **not be issuing any formal MMA POV**, and we are working closely with our lawyers Reed Smith to make sure we, the MMA, are compliant, and if members need support we will seek inputs from both RD and FPF.

The following points are drawn from the material presented to and shared with MMA members via our regular Privacy Committee meetings. These are summaries of detailed and, in many cases, highly specific interpretations of various aspects of the GDPR.

Important Note :

This is not legal guidance and companies should always consult with counsel before taking any action implied or inferred by our material. *We urge you to dig into the materials so that you get a better sense of the scope, complexity and nuance associated with the GDPR and ePrivacy Directive.*

Global Scope:

Although the General Data Protection Regulation emanates from the European Union, it's geographic scope is worldwide. If a company in the EU is a ***controller*** or ***processor*** of data from EU data subjects (consumers) then the GDPR applies. If the company is outside the EU, the GDPR applies if:

- you monitor the behavior of people in the EU or
- you offer goods and services to people in the EU.

Key Classification: Controller or Processor

- ***Controller*** = determines the purposes and means of processing personal data.
- ***Processor*** = processes on behalf of a controller but doesn't determine purpose and means.

Material Scope: GDPR applies to the processing of personal data

- Processing: Any operation performed on personal data, including its collection, storage, or deletion.
- Personal data: Any information relating to an identified or identifiable natural person.

Material Scope: Personal Data

- The definition of personal data goes beyond the notion of PII.
  - e.g. pseudonymized data is considered personal data.
- The mode of identification is irrelevant.
  - e.g. singling out (unique cookie ID) without knowing identity of the user is a form of identification.
- The holder of the means of identification is irrelevant.
- The notion of personal data will expand with technological progress.

Consent - Consent is one way to comply with the GDPR, but it's not the only way (see Understanding Lawful Processing, below).

- Consent is a statement or clear affirmative action signifying agreement to the processing of personal data. It must be
  - freely given (not bundled with consent to other terms or a condition of receipt of a service)
  - specific (no blanket consent)
  - informed (full transparency, who controls and for what purpose; includes the right to withdraw)
- Controllers must be able to demonstrate that the data subject has consented to the processing of their personal data.
- Consent must be revocable at any time. Revoking consent must be as easy as granting consent.

Legitimate Interest

- If a Controller wishes to rely on Legitimate Interests for processing Personal Data it must carry out an appropriate assessment, which can be called a Legitimate Interests Assessment, or LIA.
- When carrying out an assessment, the Controller must balance its right to process the Personal Data against the individuals' data protection rights.
- In certain circumstances an LIA may be straight forward. However, under the accountability provisions of the GDPR, the Controller must maintain a written record that it has carried out an LIA and the reasons why it came to the conclusion that the balancing test was met.
- Legitimate Interests may be considered where:
  - another legal basis is not available due to the nature and/or scope of the proposed processing; or
  - where there are a number of legal bases that could be used but Legitimate Interests is the most appropriate.

Understanding Lawful Processing

According to the Regulation, the condition of lawfulness is fulfilled only when at least one of the six legitimate grounds for processing as detailed in Articles 6 applies:

1. **Consent:** The data subject has given consent to the processing of his or her personal data for one or more specific purposes5.
2. **Performance of a contract:** Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract6.

3. **Legal obligation:** Processing is necessary for compliance with a legal obligation to which the controller is subject.
4. **Vital interests:** Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
5. **Task in the public interest:** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. **Legitimate interests:** Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Any processing of personal data must be based on one of these six grounds, with the exception of processing special categories of data (sensitive data), which enjoys additional, special rules. It is important to note that there is no hierarchy among the legitimate grounds for processing.

Processing Personal Data on the Basis of Legitimate Interests

Processing is lawful if it is "necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child". [Article 6(1)(f)]

There are three elements for this lawful ground for processing to be applicable:

- Necessity - the personal data being processed must be "necessary" for those legitimate interests to be achieved.
- Existence of a legitimate interest – applies to the controller or a 3rd party, refers "to (any kind of) legitimate interest pursued by the controller (in any context)"; the interest must be real and present, sufficiently clearly articulated, and must be legitimate and lawful, permitted by EU and national law.
- Balancing exercise – The last element that needs to be complied with is a balancing test between the interests of the controller and the interests or fundamental rights and freedoms of the individuals whose data are processed. More weight is added to the latter if the data subject is a child.

Token of Thanks:

We want to expressly thank the following organizations for their contributions to this body of work: Future of Privacy Forum, IAB EU, Data Protection Network/Bristows, Morrison Foerster, Wilson Sonsini Goodrich & Rosati, and of course the Co-Chairs of the MMA Privacy Committee, Noga Rosenthal, Chief Privacy Officer at Epsilon/Conversant and Alan Chapell, President of Chapell & Associates.