A Summary of the EU General Data Protection Regulation

In December 2015 the long process of agreeing a new set of legislation designed to reform the legal framework for ensuring the rights of EU residents to a private life was completed. This was ratified in early 2016 and becomes widely enforceable on the 25th May 2018. This blog is an Introduction to this important new General Data Protection Regulation.

The reforms consist of two instruments:

The General Data Protection Regulation (GDPR) which is designed to enable individuals to better control their personal data. It is hoped that these modernised and unified rules will allow businesses to make the most of the opportunities of the Digital Single Market by reducing regulation and benefiting from reinforced consumer trust.

The Data Protection Directive: The police and criminal justice sectors will ensure that the data of victims, witnesses, and suspects of crimes, are duly protected in the context of a criminal investigation or a law enforcement action. At the same time more harmonised laws will also facilitate cross-border cooperation of police or prosecutors to combat crime and terrorism more effectively across Europe.

The GDPR was ratified mid 2016 and immediately became law. Member states now have a 2 year implementation period. Enforcement will commence by 25th May 2018 **at the latest.**

This document summarises the key components of the GDPR – it should be noted that this is only a simplified summary and that the full text (all 204 pages) contains much more detail.

Key Components

Harmonisation across and beyond the EU

The regulation (rather than the current directive) is intended to establish one single set of rules across Europe which EU policy makers believe will make it simpler and cheaper for organisations to do business across the Union.

Organisations outside the EU are subject to the jurisdiction of the EU regulators just by collecting data concerning an EU resident. Such organisations will only have to deal with one single supervisory authority producing an estimated saving of €2.3 billion per year (according to EU figures).

What is “Personal Data”?

“Personal data” is defined in both the Directive and the GDPR as any information relating to an person 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, mental, economic, cultural or social identity of that person.

So in many cases online identifiers including IP address, cookies and so forth will now be regarded as personal data if they can be (or are capable of being) without undue effort linked back to the data subject.

To be clear there is no distinction between personal data about individuals in their private, public or work roles – the person is the person.

Controllers and Processors

The Regulation separates responsibilities and duties of data controllers and processors, obligating controllers to engage only those processors that provide "sufficient guarantees to implement appropriate technical and organisational measures" to meet the Regulation's requirements and protect data subjects' rights.

Controllers and processors are required to "implement appropriate technical and organisational measures" taking into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals."

The regulation provides specific suggestions for what kinds of security actions might be considered "appropriate to the risk," including:

- The Pseudonymisation and/or encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.
- The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Controllers and processors that adhere to either an approved code of conduct or an approved certification may use these tools to demonstrate compliance.

The controller processor relationships must be documented and managed with contracts that mandate privacy obligations – ultimately controllers must assure themselves of processors privacy capabilities.

Fines and Enforcement

There will be a substantial increase in fines for organisations that do not comply with the new regulation.

Regulators will now have authority to issue penalties equal **to the greater of** €10 million or 2% of the entity's global gross revenue for violations of data security, breach notification, and privacy impact assessment obligations.

However violations of obligations related to legal justification for processing (including consent…), data subject rights, and cross-border data transfers may result in penalties of the greater of €20 million or 4% of the entity's global gross revenue.

It remains to be seen how the supervisory authority tasked with asking for these fines will work. The current ICO framework will probably need to change as funding mechanisms will be different (no notification fees) – Fines may become a driving force.

Data Protection Officers

Data Protection Officers must be **appointed for all public authorities**, and where the core activities of the controller or the processor involve "regular and systematic monitoring of data subjects on a large scale" or where the entity conducts large-scale processing of "special categories of personal data" (such as that revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and the like). This is likely to apply to some of the larger scale Marketing Service Providers and Research Organisations – but needs further clarification.

Although an early draft of the GDPR limited mandatory data protection officer appointment to organisations with more than 250 employees, the final version has no such restriction.

The regulation requires that they have "expert knowledge of data protection law and practices." The level of which "should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor."

The data protection officer's tasks are also delineated in the regulation to include:

- Informing and advising the controller or processor and its employees of their obligations to comply with the GDPR and other data protection laws.
- Monitoring compliance including managing internal data protection activities, training data processing staff, and conducting internal audits.
- Advising with regard to data protection impact assessments when required under Article 33.
- Working and cooperating with the controller's or processor's designated supervisory authority and serving as the contact point for the supervisory authority on issues relating to the processing of personal data.
- Being available for inquiries from data subjects on issues relating to data protection practices, withdrawal of consent, the right to be forgotten, and related rights.

Data Protection Officers may insist upon company resources to fulfill their job functions and for their own ongoing training.

They must have access to the company's data processing personnel and operations, significant independence in the performance of their roles, and a direct reporting line "to the highest management level" of the company.

Data Protection Officers are expressly granted significant independence in their job functions and may perform other tasks and duties provided they do not create conflicts of interest.

The regulation expressly prevents dismissal or penalty of the data protection officer for performance of her tasks and places no limitation on the length of this tenure.

A company with multiple subsidiaries (a "group of undertakings") may appoint a single data protection officer so long as they are "easily accessible from each establishment."

The GDPR also allows the data protection officer functions to be performed by either an employee of the controller or processor or by a third party service provider.

Privacy Management

Organisations will have to think harder about privacy.

The regulation mandates a "Risk Based Approach:" where appropriate organisation's controls must be developed according to the degree of risk associated with the processing activities.

Where appropriate, privacy impact assessments must be made – with the focus on protecting data subject rights.

Data protection safeguards must be designed into products and services from the earliest stage of development – Privacy by Design.

Privacy-friendly techniques such as Pseudonymisation will be encouraged to reap the benefits of big data innovation while protecting privacy.

There is an increased emphasis on record keeping for controllers – all designed to help demonstrate and meet compliance with the regulation and improve the capabilities of organisations to manage privacy and data effectively. There is exclusion for small businesses (less than 250 staff) where data processing is not a significant risk.

Consent

Consent is a basis for legal processing (along with legitimate interests, necessary execution of a contract and others). For marketers in particular there has been much debate about the type of consent that might be required under this new regulation.

According to the Regulation consent means "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;"

The purpose for which the consent is gained does need to be "collected for **specified, explicit and legitimate purposes**"

In other words it needs to be obvious to the data subject what their data is going to be used for at the point of data collection.

Consent should be **demonstrable** – in other words organisations need to be able to show clearly how consent was gained and when.

Consent must be freely given – a controller cannot insist on data that's not required for the performance of a contract as a pre-requisite for that contract.

Withdrawing consent should always be possible – and should be as easy as giving it.

Information Provided at Data Collection

The information that must be made available to a Data Subject when data is collected has been strongly defined and includes;

- the identity and the contact details of the controller and DPO
- the purposes of the processing for which the personal data are intended
- the legal basis of the processing.
- where applicable the legitimate interests pursued by the controller or by a third party;
- where applicable, the recipients or categories of recipients of the personal data;
- where applicable, that the controller intends to transfer personal data internationally
- the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;
- the existence of the right to access, rectify or erase the personal data;
- the right to data portability;
- the right to withdraw consent at any time;
- and the right to lodge a complaint to a supervisory authority;

Importantly where the data has not been obtained directly from the data subject – perhaps using a 3rd party list – the list varies and includes:

- From which source the personal data originate.
- The existence of any profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

There are some exceptions – notably where the effort would be disproportionate (although this is unlikely be a good justification in day to day circumstances) and, importantly, where the information has already been provided to the data subject.

This is likely to cause many headaches to marketers using multiple sources of third party data – and to those building such data products.

Profiling

The regulation defines profiling as any automated processing of personal data to determine certain criteria about a person. "In particular to analyse or predict aspects concerning that natural person' s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

This will certainly impact some marketing processes and services – although the extent of this impact is yet to be understood – where does profiling finish and selection start? Full personalisation and other ad serving techniques for example rely on a degree of selection normally built on profiles of behaviour or purchase – is explicit consent for this now required? It looks this way.

Individuals have the right not to be subject to the results of automated decision making, including profiling, which produces legal effects on him/her or otherwise significantly affects them. So, individuals can opt out of profiling.

Automated decision making will be legal where individuals have **explicitly** consented to it, or if profiling is necessary under a contract between an organisation and an individual, or if profiling is authorised by EU or Member State Law.

Legitimate Interests & Direct Marketing

The regulation specifically recognises that the processing of data for "direct marketing purposes" can be considered as a legitimate interest.

Legitimate interest is one of the grounds, like consent, that an organisation can use in order to process data and satisfy the principle that data has been fairly and lawfully processed.

The act says that processing is lawful if "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."

It's worthy of note that "Direct Marketing" has not been defined – so consideration should be given to the precise nature of the marketing activity proposed to be covered by this grounds for processing.

It may, for example, mean that a simple mailing of similar goods and services to existing customers and prospects is completely legitimate without direct consent – but it certainly doesn't include "Profiling" for marketing purposes which does require consent.

Breach & Notification

According to the regulation a "personal data breach" is "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"

It's important to note that the wilful destruction or alteration of data is as much a breach as theft.

In the event of a personal data breach data controllers must notify the appropriate supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it." If notification is not made within 72 hours, the controller must provide a "reasoned justification" for the delay.

Notice is not required if "the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals," How this translates into real-world action is not clear – something the legal profession will debate I'm sure.

Importantly when a data processor experiences a personal data breach, it must notify the controller but otherwise has no other notification or reporting obligation.

Should the controller determine that the personal data breach "is likely to result in a high risk to the rights and freedoms of individuals," it must also communicate information regarding the personal data breach to the affected data subjects. Under Article 32, this must be done "without undue delay." – Again we will have to wait to see how this applies to real-world situations.

The GDPR provides exceptions to this additional requirement to notify data subjects in the following circumstances:

1. The controller has "implemented appropriate technical and organisational protection measures" that "render the data unintelligible to any person who is not authorised to access it, such as encryption"
2. The controller takes actions subsequent to the personal data breach to "ensure that the high risk for the rights and freedoms of data subjects" is unlikely to materialise.
3. When notification to each data subject would "involve disproportionate effort," in which case alternative communication measures may be used.

Data Subject Access Requests

Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way.

Where requests to access data are manifestly unfounded or excessive, SMEs will be able to charge a fee for providing access.

DSAR's must be executed "without undue delay and at the latest within one month of receipt of the request."

Subject access requests must also give all the information relating to purposes that should have been provided upon collection.

The Right to Data Portability

Clearly focussed on helping drive competition between service providers this part of the regulation seeks to drive automated transfers of data (using a common format yet to be defined) between services which primarily process customers automatically – so for example these could include utilities, banks, telecoms and ISP's.

Retention & The Right to be Forgotten

As has already been noted controllers must inform subjects of the period of time (or reasons why) data will be retained on collection.

Should the data subject subsequently wish to have their data removed and the data is no longer required for the reasons for which it was collected then it must be erased.

Note that there is a "downstream" responsibility for controllers to take "reasonable steps" to notify processors and other downstream data recipients of such requests.

This area of the regulation is likely to need further clarification – for example it doesn't seem to allow for the retention of suppression or do-not-contact lists.

A brief introduction to the E-Privacy Regulation and why GDPR needs this.

Known confusingly by many names including ePrivacy, ePrivacy2, PECR2 and ePR this regulation will replaces the existing EU Directive and is designed to harmonise and enhance the GDPR. Like the GDPR it has global reach and similarly significant penalties for non-compliance. In the UK this regulation will replace the exiting PECR laws.

This legislation is designed to regulate the use of personal information across all **electronic communications** including telephony.

At the time of writing this legislation is still in draft with the latest version issued on the 9th September 2017, the law going live simultaneously with GDPR becoming enforceable on the 25th May 2018.

This regulation is particularly important for digital marketing activity as it overrides the GDPR's allowance for legitimate interests and enforces consent on all digital communications for marketing purposes. there will still be an allowance for the so called "soft opt-in" where customers can be communicated to about similar goods and services with an opt-out only, but it should be noted that the wording here has been tightened restricting the use to customers only.

Cookies and similar tracking technologies, when used for non-essential processes (like profiling and advertising) will require prior consent. Browser and interface manufacturers are set to bear the burden of responsibility here by providing new mechanisms to allow individuals to manage their consent more easily. These mechanisms are yet to be defined...This is set to revolutionise (and potentially harm) the ad-tech industry which relies

on such techniques (third party cookie synching, the use of device ID's etc) for increasing ad relevancy.

This regulation should lead to much more open dialogue between advertisers and data subjects - with advertisers needing to make much clearer the "value exchange".