General Data Protection Requirements (GDPR) – FAQ
Source: http://www.eugdpr.org/

When is the GDPR coming into effect?

The GDPR was approved and adopted by the EU Parliament in April 2016. The regulation will take effect after a two-year transition period and, unlike a Directive it does not require any enabling legislation to be passed by government; meaning it will be in force May 2018.

In light of an uncertain 'Brexit' - I represent a data controller in the UK and want to know if I should still continue with GDPR planning and preparation?

If you process data about individuals in the context of selling goods or services to citizens in other EU countries then you will need to comply with the GDPR, irrespective as to whether or not you the UK retains the GDPR post-Brexit. If your activities are limited to the UK, then the position (after the initial exit period) is much less clear. The UK Government has indicated it will implement an equivalent or alternative legal mechanisms. Our expectation is that any such legislation will largely follow the GDPR, given the support previously provided to the GDPR by the ICO and UK Government as an effective privacy standard, together with the fact that the GDPR provides a clear baseline against which UK business can seek continued access to the EU digital market. (Ref: http://www.lexology.com/library/detail.aspx?g=07a6d19f-19ae-4648-9f69-44ea289726a0)

Who does the GDPR affect?

The GDPR not only applies to organisations located within the EU but it will also apply to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

What are the penalties for non-compliance?

Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million. This is the maximum fine that can be imposed for the most serious infringements e.g.not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

What constitutes personal data?

Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

What is the difference between a data processor and a data controller?

A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.

Do data processors need 'explicit' or 'unambiguous' data subject consent - and what is the difference?

The conditions for consent have been strengthened, as companies will no longer be able to utilise long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent - meaning it must be unambiguous. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it. Explicit consent is required only for processing sensitive personal data - in this context, nothing short of "opt in" will suffice. However, for non-sensitive data, "unambiguous" consent will suffice.

What about Data Subjects under the age of 16?

Parental consent will be required to process the personal data of children under the age of 16 for online services; member states may legislate for a lower age of consent but this will not be below the age of 13.

What is the difference between a regulation and a directive?

A regulation is a binding legislative act. It must be applied in its entirety across the EU, while a directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how. It is important to note that the GDPR is a regulation, in contrast the the previous legislation, which is a directive.

Does my business need to appoint a Data Protection Officer (DPO)?

DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data (Art. 37). If your organization doesn't fall into one of these categories, then you do not need to appoint a DPO.

How does the GDPR affect policy surrounding data breaches?

Proposed regulations surrounding data breaches primarily relate to the notification policies of companies that have been breached. Data breaches which may pose a risk to individuals must be notified to the DPA within 72 hours and to affected individuals without undue delay.

Will the GDPR set up a one-stop-shop for data privacy regulation?

The discussions surrounding the one-stop-shop principle are among the most highly debated and are still unclear as the standing positions are highly varied. The Commission text has a fairly simple and concise ruling in favor of the principle, the Parliament also promotes a lead DPA and adds more involvement from other concerned DPAs, the Council's view waters down the ability of the lead DPA even further. A more in depth analysis of the one-stop-shop policy debate can be found here.