EUDPR – Will you be ready?

European Union Data Protection Regulation

October 2015

Q Associates Limited,

7-8 Langley Business Court,

Beedon, Newbury,

Berkshire

RG20 8RY

EUDPR – Will you be ready?

This June saw the biggest change in Data Protection Regulations since 1995 with all 28 States agreeing to the introduction of a Pan-European law (EUDPR) putting an end to each individual member being responsible for enforcing data protection solely within their own country.

It's a legislation that potentially changes the role of data protection almost beyond measure and it's coming very soon to a European Union near you.

It's also an immensely complex and detailed subject and with a little under 24 months to achieve compliance, we've decided to make your life a little easier by pulling together Q's brief guide to EUDPR.

Firstly, what is the role of EUDPR?

- The European Commission's proposals for a comprehensive reform of the EU's 1995 Data Protection Directive aim to strengthen privacy rights and boost Europe's digital economy.

- Who does it affect? – Any organisation (Globally) who handles/holds "personal" information of any EU Citizens

- The legislation is technologically neutral: this means that it will not go out of date, enabling innovation to continue to thrive under the new rules.

- It forms a cornerstone of the "One Digital Market" for EU

The terminology

- Personal Data - is any information which directly or indirectly identifies an individual. It may relate to a person's private, professional or public life. It may be a name, a photo, an email address, bank details, his/her posts on social networks, medical information or his/her computer's IP address.
- Data Controller (Owner) - decide on the conditions, purposes and manner in which personal data are processed. They may be individuals, firms or public authorities. Examples of individuals include doctors, pharmacists and politicians, who keep data on their patients, clients and constituents.
- Data Processor (Third Party) - process personal information under the authority of data controllers but do not take decisions on conditions, purposes and means of the processing (outsourcers). For example, payroll companies and market research companies may process personal information on behalf

of others (e.g. other companies or public authorities, which would be data controllers in such cases). However, if they decide on conditions, purposes or act beyond the instructions of the controllers, they become controllers for that specific processing activity.

- Data Subject - Personal data is used to identify a natural person. That person is the "data subject".
- Data Protection Officer (Responsible) – The designated responsible person within an organisation for the governance of the EUDPR.

What are the main benefits for Citizens?

- A right to be forgotten: You can request your data to be deleted, subject to there being no legitimate grounds to retain it, the data (all of it) must be deleted. It is not designed to "erase" history or limited the press.
- Easier access to your own data: Individuals will have more information on how their data is processed and this information should be available in a clear and understandable way. Moreover, a right to data portability will make it easier for you to transfer your personal data between service providers.
- The right to know when your data has been hacked: For example, companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible (if feasible within 24 hours) so that users can take appropriate measures.
- Data protection first, not an afterthought: 'Data protection by design' and 'Data protection by default' will also become essential principles in EU data protection rules – this means that data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm – for example on social networks or mobile apps.

What are the main benefits for Businesses?

Data is the currency of today's digital economy. According to some estimates, the value of European citizens' personal data has the potential to grow to nearly €1 trillion annually by 2020.

- One continent, one law: There will be a consolidation to one law from 28, companies will deal with one law. Estimated benefits are at €2.3 billion per year
- One-stop-shop: The Regulation will establish a 'one-stop-shop' for businesses: companies will only have to deal with one single supervisory authority, not 28, making it simpler and cheaper for companies to do business in the EU
- The same rules for all companies – regardless of where they are established: Today European companies have to adhere to stricter standards than companies established outside the EU but also doing business on our Single Market. With the reform, companies based outside of Europe will have to apply the same rules.
- European regulators will be equipped with strong enforcement powers: data protection authorities will be able to fine companies who do not comply with EU rules up to 2% of their global annual turnover. The European Parliament has even proposed to raise the possible sanctions to 5%.

How will it operate?

- Creation of a new European Data Protection Board – 28 Members sit on the board and the European Data Protection Supervisor. It will be responsible for the consistent application of the regulation
- To anyone who does not comply with the Regulation, the supervisory authority has the power to impose a fine of up to 100,000,000 EUR or up to 2% of the annual turnover in case of an enterprise, whichever is greater. It should be noted that the European Parliament has proposed to increase the fine to up to 5% of annual turnover.
- Companies to appoint a DPO to be responsible for the governance of the EUDPR

EUDPR has already entered its trial phase and in 2017/18 the law will become fully active. There will be a 2 year acclimatisation period and then the new legislation proposes fines of up to €100 million or 2% of an organisations turnover.

This is a country mile away from a hypothetical threat. Data Owners will be liable but so will the company or individuals that actually manage and process the data; this includes all cloud and digital service providers.

But what if all your servers are sitting outside the European Union? Well, cue major clashes between the giants of cloud services and EU legislators. Taking a leaf out of

the US' stance on what is or is not fair game, this EU legislation includes all data used by EU citizens and EU residents. After all, the whole point of data protection is to protect personal data and that has global implications. It also addresses an awful lot of organisations who previously, may have dodged a few bullets here and there. The legislation also includes reputational damage, which if you're a lawyer, means Christmas has just come early.

Adherence to EUDPR is now a critical component to the safety of all types of data, not to mention your exposure as an individual and as an organisation. The ICO has been banging this well-intended drum for years now, so if we're being honest, the introduction of this legislation is hardly a surprise but equally doesn't make it any simpler to address.

The derivatives of EUDPR are undoubtedly sound but the timeframes for adherence are tight and the path to compliance is likely to a big complex beast for most organisations to address; which means for many, the time to create a plan which puts you on the right side of the digital law will probably start from the time you've finished reading this post.

Q Associates can provide a Strategic IT Review service (QSR) that can help you understand where you are now and how to prepare & protect yourself and organisation.

If you'd like to understand more about EUDPR or chat to one of our specialists about the best way to manage and secure your data you can contact us on the details below.

Email: info@qassociates.co.uk

Tel: 01635 248181