GDPR - So What Does It Actually Mean?

We've all been bombarded with GDPR for quite a while now, but what does it all mean?

When is it happening?

The General Data Protection Regulation (GDPR) goes live on 25th May 2018.

What's new in GDPR?

- GDPR applies to everyone: It is enforceable internationally if data is held on an EU resident.
- GDPR widens the definition of personal data: Essentially anything that could be used to identify an individual.
- Tightens rules for "valid consent" of personal data: This will affect those that collect the data more than those that keep it safe, e.g. your marketing department!
- A Data Protection Officer becomes mandatory in some circumstances, if you:
    - Are a public authority (except for courts acting in their judicial capacity).
    - Carry out large scale systematic monitoring of individuals (For example, online behaviour tracking).
    - Carry out large scale processing of special categories of data or data relating to criminal convictions and offences.
- Privacy Impact Assessments become mandatory.
- New breach notification requirement.
- Individuals have the right to be "forgotten" and removed from all records.
- Data Controllers are not solely responsible for data. GDPR applies to organisations that provides data processing services to the data controller, so service providers that work with personal data will need to comply with rules such as data minimisation.
- A level playing field, local rules no longer apply, GDPR can be enforced globally.
- Privacy by design must be a consideration: This is a big one for infrastructure, IT security and development teams. Security must be part of the design right at the outset of project, not at "near completion" as is often the case. Network, infrastructure and security teams should be working closely with developers and project stake holders to ensure a secure architecture for services at the outset. This applies to data systems, as well as IT infrastructure in general.

What about Brexit?

The UK will still be in the EU in May next year, regardless of how the negotiations go, it's even possible we may be "in" for a while longer if everyone involved agrees more time is needed. Even after Brexit is finalised (probably 730 days from the end of March 2017) we will still be bound by the GDPR if holding any personal information on a resident of any of the remaining 27 member states.

In addition, UK data protection laws are contained in the Data Protection Act 1998, which may or may not end up encompassing more of the GDPR in due course to facilitate trade deals with the EU. The Data Protection Act covers broadly similar ground but the penalties are less severe, with a maximum of £500,000. It's also a distinct possibility the GDPR will replace the DPA wholesale post Brexit.

> “The new EU General Data Protection Regulation is a broad framework describing responsibilities for personal data, what constitutes personal data and the approach you should take to ensure it remains safe.”

What are the penalties for a breach?

Fines up to 20m Euro, or 4% of annual group turnover.

What’s Personal Data?

The GDPR defines any data that can be used to identify an individual. Names, addresses, phone numbers, account information, email addresses, cultural and social information, economic or financial data and health & mental data… it’s all included!

So what does this mean from an infrastructure and IT security point of view?

To an extent business as usual, however that depends a lot on what that means to your organisation and the current state of your data protection systems and controls.

If you are holding any “personal data” ALL your systems must be compliant, this doesn’t mean deploying a new product to meet GDPR, but instead applying a best practice security, following the 4 pillars of IT security:

- Confidentiality
- Integrity
- Availability
- Non-repudiation

Technology can be used to mitigate risk where it is identified, it can be used to help prevent a breach, but it is not the answer to all the issues. Correct design, development, process, policy, user training, security awareness and fostering a secure culture in business are all key.

That’s where ANSecurity can help, ensuring your security is as good as can be:

- Ensuring the confidential personal data stays that way.
- Making the best use of the infrastructure and technology you have today, helping with design of new services at the outset to ensure “Privacy by Design”.
- Authentication solutions to prevent theft of credentials.
- Network breach prevention using a variety of technologies to protect your exposed attack surface areas.
- Evaluation and testing, ensuring everything is configured as it should be.
- Logging, archiving & audit trail, ensuring activities are recorded and reported upon.
- Building resilient infrastructure, virtualisation and utilising public and private cloud resources.

The list is long and the answer varies based on your business model and industry...