Gradient Consulting

White Paper

Introduction to GDRP in the EU

How is GDPR in the EU going to affect you?

As many of you are aware GDPR (General Data Protection Regulation) is being spoken and written about seemingly everywhere currently and we have been approached by many customers for assistance with this. To demystify some of the myths we have put together this short document to help.

The European Union GDRP is the first EU-wide legislation on the issue of data protection since 1995. It's made up of strict regulation that governs anyone who conducts business inside or with the EU. This document aims to simplify the Information Security related parts of the regulations and explain in simple terms what can be done to become compliant and what can assist in this area.

It's important to keep in mind that being 'compliant' with an act or regulation alone is not enough to say you are 'secure' — 'efficient and measurable' security falls at the intersection of secure practices (being security ideals or policies) and compliant practices or behaviours (*ensuring that minimum security measures are in place*).

Whilst the regulations within the UK will take some time to adopt for the many we cannot ignore the fact that fines for non-compliance will start to be seen and it's anyone's guess who will be audited first. At present, there is a two-tiered sanction regime. For breaches of some provisions by companies; which the government have deemed to be the most important for data protection; will lead to fines of up to €20M or 4% of global annual turnover or, for less serious breaches €10M or 2% of global annual turnover whichever is greater in both cases.

The regulations come into effect on the 25th May 2018 and the provisions of GDPR within the UK will be covered by a new Data Protection Bill. This has now been published by the government, for those who would like to read more about the bill, please click the following link:

https://www.gov.uk/government/collections/data-protection-bill-2017

Steps to becoming compliant

Know what you have and why you have it! – Data

It may seem obvious but how many of you really know what data you currently hold and why you are holding it?

The very first step towards compliance of the EU GDPR is to be mindful of the data you are collecting, the reasons you are collecting it, who is responsible for it and where and how it's stored.

Companies need to treat data as an asset and manage it in a structured way. You must know the type of data [e.g. personal, commercial, company, analysis...), source of the data, where it's kept, and have a good understanding of the levels of security and encryption that are being used to protect this asset.

Make it clear who, in your organisation, has responsibility for each type of data you hold. Keep in mind that this maybe different people for different types of data. With fines of up to 2% of global turnover for breaches of the regulation of a less serious nature, its highly advised that a clear hierarchy of responsibility is established.

Gradient Consulting

White Paper

Introduction to GDRP in the EU

Encrypt what you wouldn't want disclosed

Encryption is one of the best ways to keep you and your customers' data safe. if a data breach does occur and proper encryption standards have been used any encrypted data will, for the most part be useless to the attacker.

Moreover, the EU GDPR Regulation calls for "the pseudonymisation and encryption of personal data" and also makes numerous other references to the use of encryption being if not mandatory, highly advised. An interesting point on this is that if a Data Breach does occur, but the leaked data is encrypted, and you can prove this to the supervisory authority; you are not obliged to disclose details of the breach to the affected data subjects {the people who the data is referring to).

The use of SSL (secure data traffic) is required as the purpose of it is to keep sensitive information, sent across the internet, encrypted so that only the intended recipient can understand it.

When considering encryption, we all must use proven technologies; homebrew cryptography is not advised, seriously. The most secure direction to take is by using known encryption methods and algorithms like Triple DES, RSA, Blowfish, Towfish & AES as these are industry standards. For some, these terms will mean nothing, but industry specialists do, and we are well placed to offer advice and solutions to tick this box.

Design a security aware culture

All too often the weakest link in security is the human hand. Business can enforce the strictest of security protocols but, without a security-aware culture they mean very little.

Business will continue to experience data breaches through the hands of uninformed personnel. Studies show that 'human error' accounts for approximately 16% of all data breaches. Whilst 55% of all data breaches come from malicious attacks (which are relatively easy to resolve and prevent), designing a security aware culture within your organisation is another key component to becoming compliant.

So how do we build this culture? Traditionally security is pushed from the top down, that is to say, executive directors direct on what's required. They then pass it to 'experts' to implement which is mostly centred on installing hardware and software to defend against threats. *In reality however, the culture needs to be built from the bottom up.*

For security to be effective it needs to be from the ground up. This means that everything is built with a secure foundation as well as secure architecture to meet the demands of GDPR and internal policy. By building in this way a risk-aware culture emerges leading to a full security stack of well-informed employees being protected by a well-designed security setup.

Gradient Consulting

White Paper

Introduction to GDRP in the EU

Be prepared!

Simply put, expect the best but prepare for the worst. De-Risk.

It's extremely important to have a well thought-out and practiced set of contingency plans in place for the worst-case scenario. This is not only true of principles relating to GDPR but also disaster recovery in general. Just as with having a Disaster Recovery Plan in place to reduce your recovery time should the worst happen. An Incident Response Plan needs to be produced too as this will be key in recovering from a data breach and returning to the norm as fast and efficiently as possible.

An important note here is that it will soon be compulsory for all countries in the EU to have a system in place for dealing with Data Breaches.

Summary:

Becoming compliant is not as scary as you might think, but it's something we all need to consider. We have been educating staff on the issues so over the coming months assistance is available to those companies that wish it, in meeting the goals set by the government.

(We have trained people and will put on an awareness event, just an hour presentation for those who feel this a useful way to start the 'ground up' process. Watch this space.)