Below is a GDPR Facts Guide that can be used as an introduction to all staff at to what GDPR is and can be used as an initial GDPR induction training document.

What does GDPR stand for ?

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It replaces the current Data Protection Act.

When does GDPR come into effect ?

GDPR is the most significant change to data protection law in almost 20 years and by 25th May 2018 your organisation must be fully compliant. The UK's decision to leave the EU will not affect the enforcement date.

Why is GDPR coming into effect ?

It was introduced to bring things up to date particularly with regard to storage of personal information. It questions where do you keep and back up the data to in terms of servers, or "The Cloud". In which country is your "cloud" located ? Rather than preventing you from doing things, GDPR compliance aims to improve standards by encouraging you to review existing processes and procedures, making them more effective where possible. It seeks to give consistency across the European Union.

Who does this apply to ?

The Regulation only applies to data kept about individuals and not companies. It is designed to give them the right to privacy and to protect them from unwanted marketing and to ensure personal information is not being held by organisations without their consent.

What are the potential penalties for companies ?

If they don't comply, they can potentially face very large fines, greatly increased from the ones currently being imposed. The new law will require significant preparatory work and with the financial penalties for non-compliance likely to be substantial, it is absolutely vital that your organisation begins its preparations now. Don't give the job of managing data to a junior member of staff.

What do you have to do to become GDPR compliant ?

You have to make sure that the process by which an individual gives consent for their data to be held and used is separate from any contract they were entering into and that it was not a condition of any transaction and you need to understand that they have the right to withdraw that consent at any time with immediate effect.

You need to make sure your electronic data is encrypted and password protected and that your paper records are held securely in a locked filing cabinet that only authorised people have access to.

Do I have to appoint a data protection officer ?

One of the least understood aspects of GDPR is the mandatory requirement for many organisations to appoint a Data Protection Office (DPO). There are very specific rules regarding the role and the requirement will apply to many more organisations than originally thought. Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

The GDPR calls for the mandatory appointment of a DPO for any organization that has over 250 employees or one that processes or digitally stores ***large amounts*** of personal data, whether for employees, individuals outside the organization, or both.

Look at the volume, velocity and variety of the data you are holding and it is highly likely that this does not constitute "large amounts of personal data" and therefore you do not need to appoint a DPO.

What is Encryption ?

GDPR legislation is driving companies to ensure that any personal data that is held or transferred is encrypted. These days you'll find encryption in most things that run using an internet connection, from messaging apps and personal banking apps to websites and online payment methods. It is also possible to source encrypted back up drives and USB sticks.

In its simplest terms encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text ; encrypted data is referred to as cipher text.

What are the individuals rights ?

Individuals will have the right to see any data organisations hold about them, free of charge and to have records changed or deleted. You need to make sure that all your paper and electronic systems are robust enough to deal with this. This applies to both customers and staff alike.

Dealing With Data Breaches ?

Do you have a processes in place to detect, report and investigate any data breaches ? The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible, to The Information Commissioner's Office.
If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay. You must also keep a record of any personal data breaches, regardless of whether you are required to notify the authorities or not. What constitutes a Data breach

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

Do You Have A Data Retention Policy ?

This will set out what data should be retained and when it should be deleted. In addition you should be able to quickly amend data records to ensure that they remain accurate and updated. Can customer communication preferences be easily adjusted in support of a customers right to be forgotten.

Why Should We Bother With GDPR ?

A lot of the talk surrounding GDPR is to do with the increased fines being talked about following its introduction. GDPR will make all responsible owners and managers take note of how important it is to increase due diligence in all areas relating to information security and make most realise how vulnerable their current operation is.

Below are four examples that may focus the mind a little more as to why we cannot ignore GDPR

Money Shop : Lost 2 old unencrypted servers that were not being used and the info wasnt needed & fined £180,000. Under GDPR this fine could be potentially £6.1 million

British Heart Foundation : Sharing customer records without consent. Fined £18,000 but this fine was reduced by 90% as it was found to be happening across the charity sector. Under GDPR this fine could potentially be £619,000

Whitehead Nursing Group : Had an unecrypted laptop stolen with information of less than 100 clients on it. They were fined £15,000. Under GDPR this fine could potentially be £515,000. This example could easily be applicable to any small to medium size business.

Talk Talk : When bought another company they didnt do due diligence on their compliance systems and had 160,000 customer records hacked. They were fined £400,000 as the software could and should have been rectified. Under GDPR this fine could potentially be £50 million.

What Is The Next Step ?

All companies must act and be able to demonstrate the actions they have taken towards moving their business to becoming GDPR compliant. The next guide to digest is a "20 Point GDPR implementation plan" that Simply Shredding has put together. This will help take you from where you are today to achieving GDPR compliance.