miracle

white paper

What does GDPR mean for you and your business?

About the GDPR

So what does this mean for organisations?

Steps for the implementation of a GDPR security framework for your organisation

Examples of poor data handling and why GDPR will be a good thing:

GDPR and the opportunities for sales and marketing

Consent Management

What does GDPR mean for you and your business?

Reference to the General Data Protection Regulation (GDPR) seems to be making a lot of noise right now to the extent that in some circles, technology and marketing mostly, it's the new buzzword. The reason GDPR is such a hot topic of conversation is that this new piece of legislation will impact data security and data privacy in a big, big way. GDPR is on the way, bringing with it new requirements for your organisation.

The new EU personal data regulations come into force on 25 May 2018. All companies must be preparing and ready to meet compliance by this date.

What is GDPR?
After 4 years of preparation and debate the GDPR was approved by EU parliament. The GDPR is extremely complex totalling eleven chapters divided into 99 articles. All companies must be compliant when the GDPR becomes enforceable from 25 May 2018. Those organisations found not to be fully compliant will face hefty fines.

The GDPR gives EU citizens control of their digital data by empowering them with the right to know what data is being collected, when it is collected, what it is going to be used for and to have access to that data. It also gives them the capability to withdraw it upon request.

Specifically, implementing the GDPR will protect your organisation from data, information and knowledge theft. Ultimately you should treat digital data in the same way as protecting sensitive paper documents stored in a safe. By not taking the appropriate measures, this data can be easily copied and sold. Experts agree that protecting sensitive company data is a worthwhile endeavour necessary to safeguard your organisation's unique competitive advantage.

About the GDPR
GDPR is a new EU regulation which has been designed to update the existing Data Protection Directive. GDPR applies to data collection that impacts any EU citizen, even if your business is located outside the EU, the reach of GDPR will affect you.

The new data protection framework with broader punishments for compliance failure brings new rules surrounding the storage and handling of personal data. GDPR is a new and improved form of 'consent management' and will provide individuals with trust in companies they choose to be in contact with. It will enable them to have greater control over their own data and what is done with their data.

Irrespective of the UK's imminent uncoupling from the EU, the law still very much applies to all businesses, particularly those which handle the data of individuals within the EU.

If your company processes the data of any individuals, whether that be your customers or potential customers the GDPR regulation will stipulate that new levels of consent will need to be acquired in order for your company to handle that data or use it in any way.

Enacted in 1995, the existing directive was established before the days of widespread internet use, which has significantly changed the way we create, use, share, and store information. Alongside the aim of updating data protection, GDPR is also levelled at unifying approaches to data privacy and security. Being a directive, the existing framework had, by its nature, the flexibility to be implemented by EU member states as they saw fit, resulting in quite different approaches to data protection across Europe. GDPR is a regulation and as such must be followed much more rigidly. At the core of GDPR is the aim to simplify, unify and update the protection of personal data.

At its core the GDPR mandate is to protect personal data. On the one hand, it focuses on the protection of consumers, but it is also invaluable in setting standards for the protection of public and private corporations.

So what does this mean for organisations?
Changes under GDPR are aimed at moving companies away from a tick-box compliance attitude to the security and privacy of personal information, and towards a company-wide approach to managing the lifecycle of personal data. With the GDPR compliance date looming, here are some key points to consider in ensuring your organisation is ready.

The top ten key points are:

1. GDPR has a wider geographic scope. You do not have to be based in Europe for it to apply. Any company that does business with EU residents will be subject to GDPR. Even if you are offering a free service, such as a website that people in the EU access, you may be subject to GDPR if you collect IP addresses or track cookies.

2. Data Protection Authorities (DPAs) will have the power to enforce much more severe penalties for breaches of personal data. There is a tiered approach to fines under GDPR. The maximum fine that can be imposed for the most serious infringements, such as not having sufficient customer consent to process data, is 4% of annual global

turnover or €20 million (whichever is greater). For less serious infringements, such as failure to notify about a breach, a fine of up to 2% of global annual turnover would apply. This is a much greater scope for fines than we currently have in place; for example, in the UK, the maximum penalty for breaching the Data Protection Act is £500,000, and the largest fine so far imposed was £400,000, which was issued to TalkTalk in 2016 for security failings that allowed a cyber attacker to access customer data easily. However under GDPR this would have cost a massive £54m!

3. Personal data is characterised by a connection between a person and another person, thing, or event. Constitutive for personal data is the possibility of connecting the data to a specific person. Examples of personal data include car license plates, account numbers, social security insurance numbers, registration numbers, online identifiers such as email and IP addresses and mobile device identity. The determining factor in applying these regulations is not the location of the company but rather the physical location of the individual whose data was collected.

4. Organisations will need to attain explicit consent from individuals regarding the processing of their data, and companies will no longer be able to use long, illegible terms and conditions. Individuals will also have more rights regarding the processing of their data, for example relating to data erasure (often referred to as the 'right to be forgotten') and data portability, which is the right to transmit their data to another controller.

5. Technical and organisational measures regarding the protection of personal data are to become mandatory, with the GDPR outlining examples of the measures expected. These relate to the hashing and encryption of personal data, the ability to ensure confidentiality, integrity, and availability, and processes to test the effectiveness of security measures.

6. Data processing registries will become mandatory. This means organisations will need to keep a written (electronic) record of personal data processing activities, capturing the lifecycle of the data and the name and contact details of the data controller.

7. Data protection impact assessments will be required for technology or processes that are likely to be high risk to the individuals, for example data profiling.

8. The reporting of personal data breaches will become mandatory. Under Article 33 of the GDPR, organisations must report breaches of personal data to the DPA within 72 hours of becoming aware of them. If a breach poses a high risk to individuals, for example relating to personal data that has not been encrypted, those individuals must be informed **without delay**.

9. If your organisation monitors individuals on a large scale or processes special categories of data (particularly sensitive personal data), you will be required to have a Data Protection Officer (DPO). The DPO monitors organisational compliance with the regulation and must report directly to the highest management level of the organisation, must perform their tasks in an independent manner, and cannot be dismissed or penalised for performing their tasks.

10. The legislation is focused on attaining data protection by design and by default. Privacy by design is a concept that has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

The legal and technical changes required to comply with GDPR are huge and will require changes deep within the organisation. Becoming compliant with GDPR is not something the legal and information security teams of organisations can achieve alone. Senior level support is key to embrace these changes and provide the necessary financing and resourcing to achieve compliance.

Steps for the implementation of a GDPR security framework for your organisation

Data owners
Nominate data owners and assign resources to them. To improve IT security for personal data, you must firmly put in place the required measures and policies. The goal is to decentralise the security competence in your organisation. Do this by nominating a data owner for the areas where personal data is used and processed. Typically these include purchasing, finance, payroll, sales, marketing and HR.

CEOs assign the responsibility of data ownership to department managers. They know which data in their department is worth protecting and who should have access to it. The data owner is the first line of defence reporting to the data security officer, who in turn provides advice on rights and responsibilities regarding the handling of sensitive data (second line defence). The third line of defence is typically an internal or external audit. Both data security officers as well as internal auditors should be regularly informed about the current access rights situation.

Locating and centralising files containing personal data
Every data owner takes inventory of their assigned resources, locating all files containing personal data.

Reducing access rights to files containing personal data
Create a security group and use it to provide access to all users requiring access to a security critical directory. Then identify any multiple access paths and remove these so the only remaining access is provided by membership in the previously created security group. Next remove any permissions of people who do not require access to personal data to perform their role. In this instance access to security relevant data should only be granted on a need to know basis.

Remove directory access rights when employees move departments or leave the company
As soon as an employee moves to a different department immediate removal of department specific access rights must be removed. When an employee leaves the company access rights to security critical directories should be removed immediately.

How GDPR can present organisations with opportunities

However the route to GDPR compliance shouldn't be viewed as a negative. Companies can use this as an opportunity to get ahead of the competition. Acquiring clear consent from your contacts and website visitors who agree for you to send them your marketing collateral will mean the data you hold will become a far more valuable commercial asset.

In removing those individuals who don't want to be marketed to, you will be left with a honed list of contacts who have given full consent for you to contact them. Even if your Customer management system is reduced from a 30,000 strong database to 8,000 who agree to you handling their data, this will be 8,000 high quality contacts open to nurturing and ongoing communications from you.

The vital 4 questions to ask

- What contact data have I got?
- Where is it stored?
- How are we using it?
- Do we have consent to use it?

If you cannot answer these questions fully and know that you have explicit or implied permission to use the data you are holding, in the way that you are using it with a 'yes' then you shouldn't have the data at all. And as of 25th May 2018, you will NOT be able to use it.

Recently pub chain JD Wetherspoons purposefully deleted their entire database of customers because they couldn't justify how they came to have this data. The company couldn't guarantee that marketing to the ad-hoc list wouldn't pose problems in the future so they deleted all these records. The number of contacts were not reported but when they suffered a security breach in 2015 it compromised 656,723 email addresses.

Examples of poor data handling and why GDPR will be a good thing:

In March this year, Flybe was fined £70,000 by the Information Commissioner's Office (ICO) after sending over 3.3 million emails with 'Are your details correct' in the subject line. In the same month, Honda was fined £13,000 after sending over 289,000 emails enquiring if these contacts wanted to receive marketing materials. In June, Morrisons supermarket was fined £10,500 for sending 131,000 emails to people who had opted out of marketing related info from its loyalty card.

When TalkTalk suffered its security breach it lost over a million customers. These customers didn't stop using these services they went to one of their competitors.

GDPR and the opportunities for sales and marketing

Use this time to capitalise on GDPR to get ahead of your competitors in becoming compliant so that when the new regulation comes into play, you will legitimately be able to market to your database without the threat of fines, losing customers to the competition or having to put your marketing activities on hold.

The GDPR will mean a complete shift in the way we market or at least, the people that we market to. It will also have a huge impact on those that

handle the data of individuals within the EU. What kind of data does your company hold? Do you collate customers, newsletter subscribers, data you have bought in, details gained via competitions you may have run, social media campaigns you have run, business cards at events you have gathered, IP addresses from website visitors? The GDPR will have an impact on how your company can use any this data from 25th May 2018 including all of your historical data.

Different rules will apply to different groups of stakeholders. For example, if you are working with a customer and there is a contract in place and you provide them with a service, you won't necessarily need their consent to store their data if there is an ongoing relationship. The lines become blurred when you start looking at prospects or leads and how you acquired them, or previous customers who bought your products or services in the past.
In the move to compliance, under the new regulation, companies will need to be able to demonstrate how it gained the data that it holds. If a comprehensive list of consents has been granted in order for you to market to an individual in the way that you currently are, where is your proof of this?

If your company has a customer management system bursting with 'potential' customers and there have been momentary touchpoints over the years, each department within the company will need to be extremely careful about how they continue to correspond with them.

Between now and May, there will be a process of education and the need for behavioural change and staff training to bring everyone up to speed on what they can and can't do with the data you have on record.

Consent Management

There are two areas to focus on. Adapt your current processes for the new data to be collected in accordance with GDPR, with consent. Manage your historical data –if you don't know how you gained these details do you ditch the data or contact everyone to gain consent under the new GDPR stipulations? Regulators of GDPR will ask one thing when they walk through the door 'Show me your consent management database.' Can you provide evidence of this now?

The Information Commissioner's Office (ICO) have produced a handy guide 'Preparing for the General Data Protection Regulation (GDPR)' which explains what your company needs to do in order to become GDPR compliant.

Useful Resources

www.eugdpr.org
www.ico.org.uk
www.itgovernance.co.uk
/blog/list-of-free-gdpr-
resources/

www.miracle-dynamics.com
0845 634 5015

/miracle-dynamics

/MiracleDynamics

/miracledynamics