SYSTEMAGIC

DOING IT DIFFERENTLY

SYSTEMAGIC WHITE PAPER

Quick guide to GDPR: Is your business ready?

THE REGULATION

You've probably seen the term "GDPR" doing the rounds on blog posts, in the news and on social media and if you're like most business owners (according to a national survey in May 2017) you probably haven't paid much attention to it.

Big changes to the laws, regulations and associated penalties around how businesses handle and store data are coming in the Spring of 2018, all as part of new General Data Protection Regulations or GDPR. These aren't just new guidelines on data protection – they're actual laws which will be enforced and spot-checked by government bodies with fines of 4% of turnover or £20million handed out to businesses large and small who don't comply. Rumour has it that SMEs will be specifically targeted by these spot-checks because they often ignore this type of legislation. Any business that has customers is affected so it's really not something that we, as business owners, should be ignoring or putting off until 2018 arrives.

It seems to have fallen in the main to IT companies to make businesses aware of GDPR and to educate them about what they need to do to prepare for 25th May 2018 when the law changes. Don't get me wrong - I love helping our clients and making sure they're aware of important changes, but the very real danger is that GDPR will be seen as another attempt for IT service providers to sell firewalls, security software and security audits and with IT budgets are already stretched in most SMEs the whole thing will be ignored.

Never one to shy away from our assumed responsibility though, we at Systemagic are starting early(ish) and trying to make GDPR less confusing and easier to implement in to your business. We're running a series of breakfast events for our customers where, armed with croissants and decent coffee, we can work together to figure out what steps need to be taken to become compliant. We're making sure GDPR is on the agenda in our client review meetings and catch-ups and that all our team are up to speed with it all.

We've also produced this white paper which we hope will demystify some of the spin around GDPR at the moment. I hope you find it useful, informative and that you go away with a better understanding of your obligations after May 2018 and whether there's anything you need to do before then to become compliant.

James Eades

james@systemagic.co.uk | @systemagic | www.systemagic.co.uk

KNOW YOUR STUFF

The regulation is almost upon us and companies should be well on their way to finalising a GDPR plan. Businesses are expected to be fully compliant from the 25th of May 2018. The regulation is intended to give people more say and better control over what companies can do with their personal data. It will also establish one single set of data protection rules across Europe, which ultimately should make it easier for EU citizens to understand how their data is being used, and also raise any complaints, even if they are not in the country where its located.

HOW DO I KNOW IF GDPR APPLIES TO MY BUSINESS?

To put it simply GDPR applies to all companies worldwide that process or have control of the personal data of European Union (EU) citizens. This means any business that works with information / data referring to an EU citizen will need to comply with the regulations on time.

Despite the regulation not being enforced until 2018 it's imperative companies have a complete overview of the personal data entering, leaving and being stored within the business. One of the first things you can do in your organisation is ensure all the decision makers are fully aware of what personal data actually is.

'Personal data" is any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data etc.

This policy applies to the data of employees, customers and individuals you do business with. It also applies to individuals you market to so by having that initial awareness of the personal data your business currently holds you're already taking a step in the right direction to easing yourself into preperations for compliance.

Essentially then, any business that has customers or employees or even an email list of people they've met needs to have a think about where they store details about those people and how secure access to the data is.

WILL GDPR MATTER POST BREXIT?

Regardless of Brexit the UK government has confirmed that the GDPR will be fully enforced from May 2018. This means that just like businesses in any other EU Member State, UK businesses will need to be compliant by this time, or face enforcement action.

WHAT IF I'M NOT PREPARED IN TIME?

Almost 50% of global companies say they will struggle to meet the rules set out by Europe unless they make significant changes to how they operate! The clock is ticking and businesses should be using the next 11 months as a transitional period to apply the GDPR provisions. In the event of a personal data breach, companies must notify the appropriate supervisory authority immediately.

THE CONSEQUENCES

Depending on the severity of the breach Article 79 outlines the penalties for GDPR non-compliance, which can be up to 4% of the violating company's global annual revenue depending on the nature of the violation. So if you're thinking can you afford to ignore the regulations.. think again!

While IT and system security is only part of the GDPR regulation, it's often the area that is most important. Your IT service provider or network manager will be able to help you to run system audits, scans and reports and then prepare a plan of steps you need to take before May next year.

> ***Many of the elements included in GDPR are just good practice.***
>
> **Oz Alashe MBE**
> **CEO & Founder, Cybsafe**

KEY CONSIDERATIONS

The GDPR has been a long time in the making and yet the execution appears to have been rather rushed. The European Commission first proposed its legislation in 2012 and yet as of writing the final guidelines for the implementation of the GDPR are as yet unpublished. That said the following provides some key points of the GDPR for businesses:

EXPANDED REACH

GDPR covers any business offering goods or services (potentially even if they're for free) or the monitoring of data subjects (tracking them on websites with a view to marketing to them) within the EU. This is a major change as previously companies operating outside the EU were not necessarily subject to regulation.

ACCOUNTABILITY AND PRIVACY BY DESIGN

The GDPR places onerous obligations on data controllers requiring them to maintain certain documentations, undertake data protection impact assessments for risky data processing and perhaps most significantly implementing data protection by design or in other words ensuring that businesses do not keep more data than is necessary.

Furthermore, in certain circumstances a business will have to designate a Data Protection Officer ("DPO") depending on the nature of their operation (effectively if they core activities involve the use or monitoring of data subjects).

DATA BREACH NOTIFICATIONS

Data controllers must notify of most breaches to the DPA and this must be done without undue delay and, where feasible, within 72 hours of awareness or to provide a reasoned justification if this time frame is not met. More guidance on this area is expected later in 2017 but will include cases where data subjects must also be notified and what is considered to be a "serious" breach.

FINES

As mentioned previously the GDPR changes the way in which fines are approached and includes a tiered approach which enables infringements to be up to the higher of 4% of worldwide turnover and €20m for those in relation to international data transfer or other specified infringements of the higher of 2% of worldwide turnover and €10m which is obviously significant and has definitely raised the GDPR to being a serious board level consideration.

RIGHTS OF DATA SUBJECTS

One of the main aims of the GDPR was to raise the rights of individuals. This can clearly be seen in the strengthened rights of data subjects such as the right to be able to access data stored on them, ability to correct data, restrict its use and object to its processing for direct marketing purposes as well as the much talked about data transfer mechanisms.

The above is by no means a comprehensive list. The GDPR contains fairly comprehensive provisions and is especially burdensome on those companies involved in the processing of data on behalf of other data controllers but we have tried to pick out the key points that we think will affect our clients and which we think will be most relevant but it is a guide only and each business must consider the data they control and the issues and implications in relation to the new legislation.

> ***The most important thing from a businesses' internal governance perspective is to be prepared all the time and to put it on the agenda before it becomes the agenda***
>
> **Sandy Gilchrist**
> **Director, Priviness**

INDIVIDUALS RIGHTS

According to the GDPR guidelines it's required of businesses to "implement appropriate technical and organisational measures" in terms of the nature, scope, context and purposes of both handling and processing personal data. Ensuring your business has the correct procedures in place to detect, report and investigate a personal data breach is vital to managing and protecting your data.

At this stage you really need to be making yourself fully aware of the key areas surrounding GDPR. One of the most important elements to consider being individuals rights. The GDPR has created new rights for individuals and strengthened some of the existing rights under the old Data Protection Act.

One of the largest changes and an area of huge interest has been the changes surrounding a data subject's consent to the processing of their personal data. Under the GDPR consent must be freely given, specific, informed, unambiguous and separated from other terms in a clear and understandable language. Furthermore, a data subject's consent must be as easy to withdraw as it is to give and for "sensitive" data must be "explicit".

This is one of the most important areas to businesses that use data to market to their customers and whilst existing consents may work business owners would be strongly advised to consider if they meet the new conditions especially when used for direct marketing purposes as the data subject now has a right to object which is to be specifically brought to their attention. Data controllers should consider whether their notices to data subjects are compliant as the GDPR requires a much more detailed notice (including for example the right to withdraw consent).

As well as the right to consent GDPR has strengthened a number of existing rights, they are as follows:

THE RIGHT TO BE INFORMED

If you collect an individual's data, you must tell them who you are; why you are collecting their data; what data you are collecting; who you will be sharing it with and why; how long you will retain it and what their rights are.

THE RIGHT TO ACCESS

Once you have an individual's data, they have a right to ask what data of theirs you have and how you are processing it.

THE RIGHT TO CHANGE THE RECORD

An individual can ask you to update or rectify his/her information and you must comply. If you do not, you will need to explain why and inform them of their right to complain. You must also tell them who else you disclosed their data to so they can update them.

THE RIGHT TO BE FORGOTTEN

In certain circumstances, an individual has a right to have their personal data erased. You need to know in what circumstances you will have to comply with their request. Similarly, an individual also has the right to ask you to stop processing his data.

THE RIGHT TO DATA PORTABILITY

Individuals should be able to obtain and reuse their personal data as they wish across different services. If the individual requests it, you may be required to transmit the data directly to another organisation if this is technically feasible. If you refuse, you must be able to explain why.

If IT is taken care of by your service provider, it's still down to you to document the data policies your business abides by and the recommendation is to nominate a Data Protection Officer internally who has responsibility for reviewing procedures and maintaining an eye on data security.

WHERE TO BEGIN..

At Systemagic we believe that despite the regulation not being enforced until May 2018 it's imperative you act now. It might seem a long way away but being prepared and proactively managing the impact will make it a lot more manageable and less likely that the GDPR will be impact your business.

To assist with this we have produced the following 6 step guide which we believe will assist in getting you started with the process and ensure that it goes smoothly, and could actually be a positive for you in interacting with your customers.

Step 1 – Assign Responsibility

For us this is key. As identified above for many large businesses the GDPR has become a board level issue and we think SME's should approach it in the same way. Assign someone in your business with sufficient ability to make necessary changes to head up the implementation of compliant policies and provide them with sufficient relevant support from relevant external advisors.

Step 2 – Discover your data

Begin the process by understanding, identifying and categorising the data that you have entering, leaving and being stored within your business and what you use it for. You need to classify it and determine if it falls within the GDPR, that is, does it relate to customers / consumers and are they therefore data subjects within the definition of the GDPR.

We also suggest that at this point you consider whether you actually need the data at all, in whole or in part, as many businesses these days collect all sorts of data which may or may not be relevant and this might be an appropriate point to consider some (carefully managed of course) data cleansing.

Step 3 – Establish a Framework

Don't panic, we aren't going to come over all management consultancy here but the GDPR effectively requires you to put in place a documented procedure for how you will capture, manage and process data on applicable data subjects. We believe therefore that as you put the policies and procedures in place that the best thing to do is start with a compliant framework which works. Our recommended framework covers the following areas: Discover, manage, project and report.

WHERE TO BEGIN..

Step 4 – Embrace the Change

We believe that for those businesses that deal directly with customers / consumers and that are going to be most affected by the GDPR the best thing to do is embrace the changes and try to become best in class as there is an opportunity to use the GDPR to engage with your customers. Consider:

- Incorporating privacy by design into your system so that data subjects are aware of their rights, the options available and are comfortable with you holding data on them.
- Ensuring that the data you hold is legitimate (have you even considered the legal basis on which you hold data) and build the systems so that it can be easily portable should data subjects wish to use their new rights.
- Ensure all data notices are clear and in plain language and easily accessible.
- Build a response mechanism which is ready to respond to individual requests for data in a timely manner. General consensus is that early adopters will request this and may have unreal expectations so again be prepared.

Step 5 – Determine if you are a supplier to others

One of the key changes in the GDPR concerns the direct obligations placed on those businesses which process information for other data controllers. In that case you need to build in compliance to all aspects of your operations from policies, procedures to contracts which will now need to cover areas such as rights and responsibilities and also establishing who bears the costs of compliance.

For those businesses that use data processing services from third parties the reverse is true and they must consider documenting responsibilities and establish the costs of management and also indemnification for breaches.

Step 6 – Training, review, improve, repeat

It is key to note that the GDPR is not a one hit wonder and compliance will mean more than a one-off audit. After all you could be reviewed at any time by the regulatory authorities so we believe it is key to train all of your staff to be aware of the rules as well as build a system for constant review and improvement. Be that in terms of the data you are collecting, the reasons for collecting it and legal basis through to ensuring you actively manage the data you hold, respond to individual's requests and keep improving your notices and security. The key is to keep reviewing and actively managing you're your policies and procedures to ensure ongoing compliance and prevent potentially triggering one of those large fines.

WHAT STAGE IS YOUR BUSINESS AT WITH GDPR

18%

Have began training awareness programmes across the business.

14%

Have a data classification policy in place

TECHNICAL MEASURES

By now you hopefully have a greater understanding of how GDPR will impact your business, what key areas you should be focussing your attention on and what the consequences will be if your organisation isn't implementing those practices in time.

Data security plays a prominent role in the new GDPR regulation. In comparison to the current Data Protection Act the new regulations follow a stricter set of rules for businesses in relation to security. The requirements from an IT perspective are fairly simple, we are focussing on the following five key areas:

FIREWALLS

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. The main purpose of a firewall is to separate a secure area from a less secure area and to control communications between the two.

SECURE CONFIGURATION

Secure configuration refers to security measures that are put in place when building and installing computers and network devices. Implementing secure configuration allows a reduction of unnecessary cyber vulnerabilities.

USER ACCESS CONTROL

User Access Control is a security restriction that's implemented to control who or what can view or use resources online.

MALWARE PROTECTION

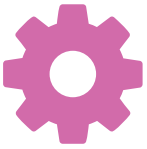
Malware is short for 'malicious spyware' and is designed to infiltrate and damage computers without the users consent. Malware protection is a kind of security software that's specifically designed to protect a computer and stop malware infecting a device.

PATCH MANAGEMENT

Patch management is an area of systems management. Tasks include: maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems and ensuring that patches are installed properly. Security vulnerabilities can be easily avoided by applying patches.

The good news is that the majority of businesses should have all of these key elements put in place as part of general good business practice, so it's just a case of reviewing what measures are in place, documenting them and reviewing regularly to ensure that they're working and running efficently.

WHAT STAGE IS YOUR BUSINESS AT WITH GDPR



8%

Have implemented a data classification tool

13%

Have done nothing, placing themselves at risk of non-compliance

SYSTEMAGIC'S TOP TIPS

While this list is nowehere near exhaustive, we have come up with the following tips which will bring most companies significantly closer to being fully GDPR compliant:

Make a list of what personal data you store about employees, customers, sales prospects and contacts. This includes any information you keep about name, address, next of kin details, work address, date of birth and even technical information like IP addresses and if your website uses cookies to collect information.

Conduct a risk assessment. How might this information get in to the wrong hands? Is data storage protected from certain employees? Does your IT system have an appropriate firewall? Do you make sure that employees who connect from home have adequate AntiVirus and IT security on their home computer? How often are passwords change? Do your staff understand when they can and can't share information with third parties?

Set user passwords to expire regularly and make sure they have to choose a 'complex' password - i.e. one that includes numbers and symbols

Make sure your internet connection has a firewall which is properly configured and kept up to date with firmware updates

Install encryption software on any device that is taken outside of the office so that it can't be accessed if it's lost or stolen

Benchmark your IT systems against the government's Cyber Essentials assessment.

Set up a process of regular review and reassessment. The GDPR regulation is a bit like ISO standards in that they expect a continual process of review and ongoing improvement. This should include a regular IT security assessment.

If you're concerned about your compliance plans or want to learn more about the measures your organisation should be putting in place before the regulation is enforced then please get in touch!

info@systemagic.co.uk www.systemagic.co.uk 01225 426800

SYSTEMAGIC

DOING IT DIFFERENTLY

Head Office: Systemagic Ltd The Old Gas Warehouse Frome Road Bradford on Avon Wiltshire BA15 1HA

Bath Office: Systemagic Ltd Waterhouse Waterhouse Lane Bath BA2 7JB

SYSTEMAGIC

DOING IT DIFFERENTLY