GDPR, Brexit & SMEs

What you need to know now to stay compliant

entrustIT Europe

CONTENTS

INTRODUCTION

GDPR is big news right now and whilst many of the organisations we work with are aware it's on the way; others are still very much in the dark. In short, the major shift, with the implementation of GDPR, will be in giving people greater control over their data. The regulatory landscape is rapidly changing due to the explosion in digital and the ever changing ways in which we share information. GDPR strives to protect yours and your customer's personal information in this new digital age.

This white paper aims to cut through the noise, explain the regulation and pull out the salient points for SMEs.

What is GDPR?

GDPR stands for the General Data Protection Regulation. It is the result of four years of work by the European Union to bring the data protection regulation of all member states into line with one another, as well as ensuring that existing legislation is updated and 'future-proofed'. In the UK, we rely on the Data Protection Act 1998, which no longer keeps up with the pace of technological change.

When it comes into force on 25th May 2018, it will supersede the existing legislation, as well as introduce vastly tougher fines for non-compliance – but we'll get onto that later.

The General Data Protection Regulation

Why bother with GDPR?

All EU member states have their own data protection regulation, so why bother making a new one?

Current legislation was enacted before the cloud, before internet advances, and before social media such as Facebook became so big in our lives. GDPR aims to give people more control over how their personal data is used. It seeks to strengthen data protection and provides tougher enforcement measures.

In addition, GDPR will provide a standard across the entire single market. The intention is that this will make it easier for companies across member states to do business. The EU estimates this will save businesses €2.3bn annually (collectively).

Gives individuals more control over their personal data

When will GDPR come into effect?

Whilst the legislation was approved on 24th May 2016, it comes into effect on 25th May 2018. Once GDPR officially comes into effect, it applies to all businesses that handle the personal data of EU citizens, regardless of whether they are based in the EU or not.

It is the responsibility of every business to ensure that they comply with GDPR once it comes into effect.

GDPR Deadline:
25th May 2018

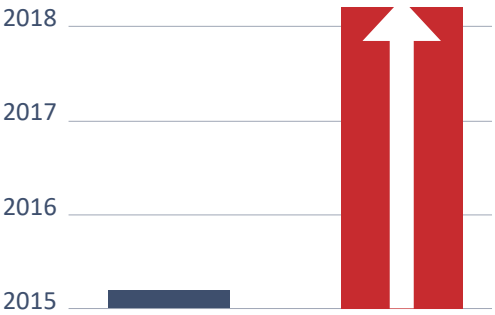
BREXIT & NON COMPLIANCE

But the UK is leaving the EU, do we still need to comply with the regulation?

First, the UK is expected to leave the EU in March 2019. Until that date, we must still comply with EU law. GDPR comes into effect in May 2018, so all UK businesses will have to comply with the law, at least until the UK leaves the EU.

However, as mentioned previously, GDPR applies to all businesses that handle the personal data of EU citizens. It is also likely that GDPR will be incorporated into UK law after Brexit, since that will be the easiest way of ensuring that UK businesses comply with EU data protection law and will make it easier for the UK to get an adequate trade deal with the EU – although of course nobody really knows what life outside the EU will be like for the UK. Therefore, UK businesses cannot use Brexit as an excuse not to comply with GDPR.

What are the penalties for non-compliance?



The short answer is that the penalties are very harsh. Larger organisations may find them easier to swallow but for small to mid-sized organisations they are stomach churning.

Failure to comply adequately with GDPR can result in a fine of up to 4% of your company's global annual turnover or 20M EUR, whichever is higher. This is damaging enough, but when brand damage is added, non-compliance with GDPR could be extremely destabilising for your business.

These penalties come into effect if a data breach occurs in your business, which is defined as a breach of security, resulting in the destruction, loss, alteration, unauthorised disclosure of or access to personal data. In the event of a data breach, it is your responsibility to report it to a data protection authority (the UK authority is the Information Commissioner's Office) within 72 hours of your organisation becoming aware of it. You are expected to notify the authority of the nature of the data that has been breached, and the approximate number of people affected, as well as estimating the consequences for those people and outlining the measures you are taking to protect their data. You should also inform the people affected.

To put these fines into perspective, the current maximum fine for a data breach under the Data Protection Act is £500,000. This means that if data breaches remain at 2015 levels, the fines paid to EU regulators could increase 90-fold , from £1.4bn in 2015 to an estimated £122bn.

72-hour deadline

Up to 4% of global turnover or 20M EUR, whichever is higher.

For large organisations, the effect could be even greater, with **fines potentially soaring to £70bn,** more than a 130-fold increase.

DATA BREACH & YOUR BUSINESS

But my business isn't likely to be hacked, so why do I need to be worried?

It's a common misconception that small or medium sized businesses don't suffer from data breaches. Whilst SMEs are perhaps not such a lucrative target as a large business, they are just as at risk of breaches as a large company.

Ponder the fact that 74% of UK SMEs had a data breach in 2015. Furthermore, the IBM "2014 Cyber Security Intelligence Index" found that 95% of all security incidents involve human error. This could possibly be something as simple as sending an email with sensitive data to the wrong person by accident.

No company is completely immune to human error. It is therefore naïve to think that your business is somehow sheltered from data breaches.

What should I do to make sure my business is compliant?

Since it is roughly a year until GDPR comes into effect, it is important that you begin preparing now. Make sure everyone in your business is familiar with the regulation, from the top to the bottom. If everyone is on the same page, it will make implementation smoother, particularly if it has support from the board and management.

From 25th May 2018, your business must:

1. Keep a record of data operations and activities and consider whether you have the correct data processing agreements in place
2. Carry out privacy impact assessments (PIAs) on products and systems
3. Designate a data protection officer, if applicable
4. Review processes for the collection of personal data
5. Be aware of your duty to notify your data protection authority, particularly who that authority is and what their contact details are
6. When implementing new products and services, why not ensure that data security is built in?

THE EFFECTS OF A DATA BREACH

Some real-life examples of data breaches and the effects

Talk Talk

Breach date: October 2015

TalkTalk, the telecoms company, was hit by a cyber-attack in October 2015. The result was 157,000 customers having their personal details stolen – 15,656 of these customers had bank account numbers and sort codes stolen.

The hack was widely publicised in the media and TalkTalk lost around 100,000 customers in the months immediately following the hack.

The hack is estimated to have cost TalkTalk £35m in one-off costs (such as calls into call centres and additional IT and technology costs), when you factor in the costs of lost revenue the damage is closer to £80m.

Damage: 157,000 personal records stolen

Cost: est. £35 million

Ashley Madison

Breach date: July 2015

Then there's the well-known story of Ashley Madison. A group of hackers acting as internet vigilantes hacked the website and stole the personal details of 32 million account holders.

What made this hack all the more troubling is that Ashley Madison offered to fully remove user data from their servers for a one-time payment. It became clear that this was a lie when the email addresses of people who had paid to be removed turned up in the hack.

Users whose details were leaked are filing a $567 million class-action lawsuit against the parent company of Ashley Madison. The brand of Ashley Madison is now irreparably damaged. Sadly, there have also been reports of a number of suicides linked to the hack.

Damage: 23 million users personal detials stolen

Cost: est. $567 million

Tesco Bank

Breach date: November 2016

In November 2016 cyber-thieves stole £2.5m from 9,000 Tesco Bank customers.

A number of theories have circulated about the cause of the issue including one that it was an internal security breach. The attack described as 'unprecedented' saw the loss of £2.5m, from the 9,000 customer accounts affected.

The bank who have over 7 million customer accounts alerted customers to the breach via text message after observing suspicious activity across multiple accounts and customer's reporting sums of up to £600 stolen from their accounts. The bank faced criticism over its handling of the hack with customers complaining about the difficulty of contacting the bank to report suspicious activity.

There is speculation that the bank would face fines of over £1.9bn for the hack if it occurred under the EU's forthcoming General Data Protection Regulation (GDPR).

Damage: 9000 customer accounts affected

Cost: est. £2.5 million

WHY CONSENT MATTERS

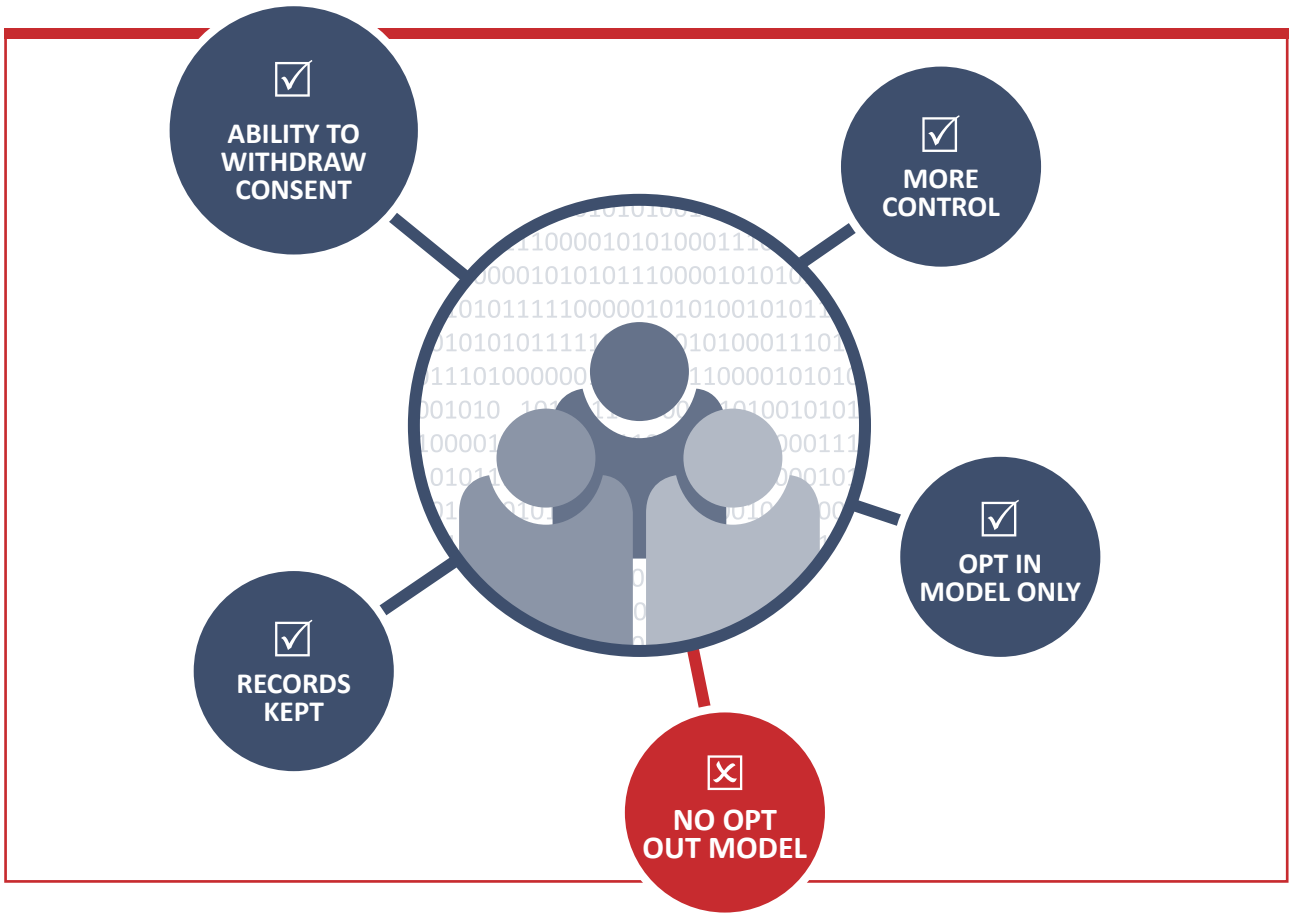
Consent: What is different and why does it matter?

GDPR will bring in new directives on consent, giving individuals more control over their personal data. It will make it crucial for data controllers to ask for consent from customers to store their data.

This means active, affirmative action by the customer. Passive acceptance, or an "opt-out" model is unacceptable under GDPR. Without consent, processing personal data is unlawful. Your business MUST be able to keep a record of when an individual gave consent, and that individual can withdraw consent at any time.

If your current model does not keep a record of when and how an individual gave you consent, you MUST update it before the May 2018 deadline. Any business found misusing personal data will be fined to the highest level – up to 20 Million EUR.

Under the data protection act, passive consent is allowed. Many businesses process personal data until a customer opts out. This will not be legal under GDPR.



THE ePRIVACY REGULATION

The ePrivacy Regulation: What is it and what do I need to know?

The ePrivacy regulation is separate to, but will work alongside, GDPR. It is a regulation that covers what data controllers and processors should be doing to protect individuals' communications, electronic or otherwise. Like GDPR, the regulation will come into effect on 25th May 2018.

Here are some of the important parts of the regulation:

1

Extra-territoriality and 4% fines

This proposed regulation applies to businesses anywhere in the world who provide publically available "electronic communication services" that gather data from the devices of EU citizens. Remember, this applies across the world, as long as you acquire data of EU citizens. The fines imposed for non-compliance match the GDPR fines, so up to 4% of annual turnover.

2

Wider reaching application

Not only does this regulation apply to ISPs, but also providers of messaging apps, email platforms, VoIP services etc. It also includes anyone using tracking technologies, such as IP tracking.

3

New rules for communication data

New rules ensure that data regarding conversations such as who said what, and when, are confidential.

4

E-Marketing rules

E-Marketing requires opt in, unless the contact details have been obtained in the context of a sale – in which case opt-out is possible.

5

Exemption analytics cookies

Businesses will now be exempt from the cookie consent requirement for analytics. However, websites using third party analytics such as Google Analytics will require consent.

CONCLUSION

entrustIT, a safe pair of hands for your data.

GDPR is a vast regulation. This whitepaper covers most of the important points you need to know. However, you could be forgiven for thinking that GDPR compliancy is extremely daunting.

Since burying your head in the sand is not a valid option, you may feel that the best course of action for your business is to find a trustworthy partner to look after your business data.

At entrustIT, we have been working for over 10 years providing cloud computer solutions to businesses. You only need to look at our name to see that trust is at the heart of our business. It's what makes us tick. We are passionate about providing industry leading security to our business clients. That is why we are ISO 27001 security certified.

All our cloud solutions have disaster recovery and failover options built in and we constantly monitor our datacentres against threats. As a managed cloud services provider, it is absolutely crucial for us to be on top of all data protection legislation. If we didn't we would be out of a job.

Why worry about whether your sensitive data is open to breaches?

By finding a specialist partner for your data management, you can rest assured that your data is safe, your organisation complies with GDPR and, perhaps most importantly, you won't chance upon a 20,000,000 EUR fine in the near future!

entrustIT
Europe

entrustIT Limited
UK Head Office: Units 1-3, The Doughty Building, Crow Arch Lane, Ringwood, Hants BH24 1NZ
t: 0330 002 0045
e: enquiries@entrustit.co.uk

References:

http://privacylawblog.fieldfisher.com/2017/the-new-e-privacy-regulation-what-you-need-to-know/
http://www.telegraph.co.uk/business/british-standards-institution/cyber-security-for-smes/
http://www.computerweekly.com/news/450401190/UK-firms-could-face-122bn-in-data-breach-fines-in-2018
https://en.wikipedia.org/wiki/General_Data_Protection_Regulation#Sanctions
https://www.bonddickinson.com/insights/publications-and-briefings/brexit-great-repeal-bill-and-data-protection-law

DESIGNED BY bite IT MARKETING