BUSINESS FEATURE

Getting ready for GDPR

Changes to data-protection rules will have major implications for your business. Davey Winder explores the new requirements

The EU General Data Protection Regulation – GDPR for short – has become law. It's the biggest change to data legislation for years, and don't think for a moment that just because the UK has voted to leave the EU it's any less relevant to your company – as we'll discuss in depth later. The good news: you have until 25 May 2018 to comply with the legislation. The bad news: that may sound a long time but there's a lot to do, so start your preparations now.

If you're wondering exactly what GDPR is all about, the simple answer is data. It exists to protect the privacy and security of all the data collected by organisations, large and small, across the European Union. It replaces the old Data Protection Directive, which was brought into play back in 1995, and updates it to keep pace with the changing data-protection landscape of the modern online world.

So while some might see the GDPR as "yet another regulation from Brussels", it protects an important aspect of human rights, and improves information security for us all.

Why is GDPR necessary?

As individuals, we're expected to hand over personal data as part of some sort of online transaction. We do it when we book a flight online, access our bank accounts, or keep in touch with our social circles.

"Failure to comply with the GDPR could lead to financial penalties, so it isn't something that you can afford to ignore"

We accept this as part of living in the modern world. But that doesn't mean we shouldn't be concerned about what happens to that data once it's been handed over. Hopefully, we don't need to explain why it's important for individuals to know what personal data about them is stored by third parties, and what measures are in place to prevent a breach. The GDPR is designed to give EU citizens more transparency and control over just that.

If you're managing a business, you might be worrying about the cost of this latest layer of red tape. The GDPR simplifies the regulatory environment for most businesses, while at the same time bringing information security front and centre, which is never going to be a bad thing.

The principle at the heart of the GDPR is that personal data "can only be gathered legally, under strict conditions, for a legitimate purpose". It codifies such things as a right to be forgotten, as well as a data breach notification requirement. Failure to comply can lead to financial penalties, so it isn't something you can ignore.

ABOVE As part of GDPR, businesses must comply with "right to be forgotten" legislation

The Brexit (non)-issue

It matters not a jot that the UK voted to leave the EU: your business still needs to comply with GDPR.

Prior to the vote, we spoke to John Culkin, director at Crown Records Management, who warned: "It would be tempting for businesses to think that if the UK leaves the EU then the GDPR rules wouldn't apply to them. That isn't the case.

"Although an independent Britain wouldn't be a signatory of the regulation, it would be impossible for businesses to avoid its implications. Any company holding identifiable information of an EU citizen, no matter where it's based, needs to be aware."

At any rate, the General Data Protection Regulation merely reinforces certain aspects of good information governance, which all companies should already be embracing anyway.

"There's no point ignoring privacy by design, when that is good procedure" Culkin concludes. "The same is true of measures to protect a business from data breaches. These have reputational as well as financial implications – no matter who imposes the fine."

Data breach notifications

One consequence is that businesses, large and small, will find themselves required to report most data breaches that impact personal data. That means notifying both the Information Commissioner and the individuals whose data has gone walkabout.

"Loss of client data is a major risk to any business, and the stakes are only getting higher," said John Michael, CEO at iStorage. "The feedback from iStorage clients is that most data losses arise from human error, rather than any conscious contravention of the rules, or a lack of internal compliance effort." This implies that the shift in emphasis to pro-active self-review and analysis should cut mistakes and limit data losses.

"The increase in financial risk from the new penalties will also see greater investment in encryption technology and tools to reduce the risks arising from the human element," Michael suggested.

Five steps to mitigating data risks

Rick Orloff, chief security officer at Code42, shares his five-step recommendations regarding GDPR

1 Look to the front line
You can't keep your clients' data safe if your systems aren't secure. Make sure your antivirus and other internet security provisions are up to scratch. Consider switching to multifactor authentication for systems handling client data.

2 Get your backups in order
It's good business practice in all cases to ensure you're protected. It becomes all the more crucial when you're handling personal data, and keeping mandatory records of how you're processing it.

3 Understand your endpoints
Check your employees' workstations to ensure that sensitive information is available only to those who need access. Think of mobile access, too: in the age of BYOD, employees' personal devices can be a route to a data leak.

4 Communicate a clear data-security policy
Employees rarely break the data-protection rules on purpose. If everyone understands what's expected of them, it's more likely they'll recognise when potential concerns arise, and handle them appropriately.

5 Track movement of data
Draw up a data map to see if information is ending up in places it shouldn't – and use technical measures to track how and when personal data is being accessed, so you can immediately spot any suspicious or inappropriate activity.

"Although an independent Britain wouldn't be a signatory of the regulation, it would be impossible to avoid its implications"

The right to be forgotten

Perhaps the most written-about feature of the GDPR is the "right to be forgotten". This gives an individual the right to order a business to erase their personal data, as long as certain criteria are met.

To find out more, *PC Pro* spoke to Sarah Pearce, a partner in the Technology Transactions Group at law firm Cooley LLP. She told us that data

Your GDPR preparation timeline

One of the primary challenges for small businesses when facing GDPR compliance is budget. As Clearswift's Dr Guy Bunker points out, you have approximately two years to get compliant – so if you start allocating budget this year, you can split the cost down the middle by spreading it over the two-year period. However you arrange your budget, Dr Bunker advises small businesses to be ready six months ahead of the GDPR-compliance deadline, so there's a buffer in place to accommodate the hitches that will appear along the way. Here's what you need to be doing, and when.

First 6 months
If your organisation has more than 250 employees, then you'll need a data-protection officer (DPO). If you don't already have one then this post should be filled sooner rather than later, so that they can be involved in the journey towards compliance.

6 -12 months
Work out where new procedures need to be introduced, such as security and breach notification. You should aim to get this in place early, so you have plenty of time to disseminate new policies and test new processes around your business.

12 - 18 months
Start conversations with suppliers and data processors to discover how they'll protect your information and respond to requests for data deletion. Look at tools to help in discovery, especially for "right to be forgotten" requests, which need to be done in the next two years.

controllers will have to erase any and all copies or links to personal data where the data subject withdraws consent and there is no legal ground for processing it. The organisation must also take reasonable steps to inform others who are processing the data concerned.

Data must again be removed – pending investigation – if someone objects to the accuracy of their personal data, under a provision called the "right to restriction".

Pearce recommends that all businesses review their procedures for handling erasure requests, to ensure they can provide both for erasure and restriction. Determine how you'll identify other controllers and inform them of a request, and nominate someone within your business to be responsible for dealing with such requests.

Record keeping

This might sound like something of a record-keeping nightmare for smaller business, but the reverse could well be true. "For a smaller organisation, the ability to comply should actually be easier," reckoned Guy Bunker, senior VP at security company Clearswift.

"Under GDPR, organisations of less than 250 employees will not have to employ or train a data-protection officer (DPO)." Essentially, they won't have to change the structure of their organisation, whereas larger businesses probably will.

Smaller organisations will also benefit from no longer having to notify the ICO of data-processing activities. The GDPR instead requires businesses to keep detailed records on their own processing activity.

ABOVE Ignore GDPR and you could be hit with a fine up to 4% of your turnover

"The GDPR may sound like something of a record-keeping nightmare for smaller businesses, but the reverse could well be true"

"This includes info such as the reason for processing, the description of the categories of the data subjects and personal data, categories of recipients to whom personal data is disclosed, the time limits for erasure and a description of the security measures taken", explained David Barker, technical director at cloud hosting company 4D.

In fact, companies with fewer than 250 employees can be exempted from these bookkeeping requirements – but only if your data processing isn't "likely to result in a risk to the rights and freedoms of the subject"; doesn't relate to sensitive personal data; and isn't occasional in nature. If any of those do apply, then even the smallest business must comply with the full record-keeping requirement. We look forward to guidance from the ICO on how those criteria will be interpreted.

Getting it wrong

You can't ignore the GDPR, and you can't afford to get it wrong. If you do, your business may face a substantial fine. Indeed, some have questioned the scale of the penalties associated with non-compliance: "If a smaller business were hit with one of these fines," noted Guy Bunker, "it would be potentially catastrophic."

How catastrophic? Well, GDPR replaces the old warning system for SMEs with a two-tier fining regime. Tier 1 is for a "less serious" breach of the regulations, such as where an administrative failure in record-keeping is found. Even this can be up to 2% of turnover, or €10m.

Tier 2 is for failures categorised as "serious", such as a breach of basic data-protection principles – and the maximum penalty is doubled.

"This means that SMEs are exposed to the Tier-1 level of fines for non-compliance with record-keeping or procedure issues," warned David Barker. However, there are ways to reduce your exposure. "Fines will be set by the ICO, and they do take into account an SME's code of conduct and certifications such as ISO 27001. It may be worth small businesses perusing these to give them some protection from fines – as well as implementing best practice when it comes to information security."

That's the real point. It's not about the fines or laws, but about protecting your clients' data. ●

A risk-based approach to the rules

In the coming months and years, we can expect a lot of official guidance for SMEs to come from national bodies such as the Information Commissioners' Office. This will clarify and dictate the detail of what specific industry sectors must do to prepare for GDPR. But that doesn't mean businesses can't take the initiative and start their preparations now. We asked Christine Andrews (*right*), managing director of data governance, audit and consultancy firm DQM GRC for her advice.

"First, organisations need to evaluate the personal data they have," she told us. "Categorise the data so you're clear where the personal and sensitive data resides, and where other, less important data sits in the company. Usually, drafting a data map will help businesses to understand the pattern of data through the company, provide clarity on who has eyes on the data, indicate what skills these people have and, finally, highlight where the data ends up.

"Once organisations understand just what personal data they're holding, they should then ensure that regular risk assessments are completed, in order to understand the level of threat imposed on the company when processing data.

"The GDPR in fact demands a risk-based approach with the development of appropriate controls. This should, in a single stroke, ensure that management recognises the dangers associated with the loss, misuse, theft or any other compromise of customer data. For organisations that pass data onto others, there is a tendency to presume that third parties operate to high standards of data security and protection. The GDPR now requires controllers to obtain sufficient guarantees of this before engaging with processors.

"Basically, as the data owner, you must check that the organisations you're working with have effective technical and organisational measures in place to ensure the security of the processing."