GDPR: THREE YEARS ON

Nicola Howell *explains why the General Data Protection Regulations are more important in 2021 than ever*

GDPR. Four letters that send shivers down the spine of businesses large and small. While 2018 feels like an age ago, the scramble to prepare for the General Data Protection Regulations feels like yesterday. The new processes, the HR meetings, the flurry of emails updating customers on the business' updated data policies – who could forget them?

Thankfully, things have calmed down in the last few years. Most businesses are 'over the hump' as it were, having successfully put in place policies and procedures that make them compliant. Indeed, many are discovering that GDPR compliance has more utility than simply avoiding a nasty fine. The regulations encourage best practise for maintaining data health, ensuring businesses have data that is accurate, up-to-date and fully secure. That's not to mention deeper bonds with customers who feel more confident that their data is being properly looked after.

And yet, 2018 was a long time ago. Times change – even without Brexit and a global pandemic. As the world moves inexorably on, so does businesses' relationship with GDPR as data becomes ever more integral to operations.

NOW THE DUST HAS SETTLED

In this article, I want to give a bit of a GDPR update. Now the dust from that initial scramble has settled, how are businesses faring? How has and will Brexit impact them? And as we emerge into a post-COVID-19 world, how will the rules evolve to account for a business landscape that, more than ever, has data at its very heart?

One of the strange dichotomies of 2018 was that, as businesses were shaping themselves to comply with GDPR, they were also acutely aware that the UK was leaving the EU. However, at the time the exact shape of that exit was uncertain to say the least, and questions were asked about whether the EU's shiny new regulations would be preserved in UK law.

We do now have some clarity on that. As you may know, GDPR has been transposed into UK law almost exactly, which of course is good news for those worrying about having to repivot their organisation to match a new set of regulations.

While there is no action to take immediately, businesses should be aware things will change in the future. The UK and the EU have set themselves on divergent tracks that will only become more pronounced over time. Inevitably, GDPR will be changed, moulded and evolved to suit the individual needs of the UK as it seeks its new place in the world. Eventually EU and UK GDPR regulations may indeed look very different – and businesses must be prepared to adapt accordingly.

On the subject of Brexit, there has been one very good piece of news: the UK data protection policies have been awarded 'adequate status' by the EU. This means that, from the EU's perspective, the UK is able to adequately handle the data of EU member states. UK businesses can therefore freely continue to receive and process EU data, making it much easier to do business in Europe. This is critical for those who actively depend on their European channels. It means they have a pre-existing data transfer mechanism in place and don't need to enter into a new contract to maintain data standards.

It is worth mentioning that, as good as having adequate status is, it does represent a significant reduction compared with what the UK had before. The UK will not be invited to the table when it comes to making amendments to the regulations. If the UK wishes to keep its adequacy status, it must continue to align to European regulations – which is of course counterintuitive to the UK forging its own path.

> THERE IS NO EXCUSE NOT TO BE COMPLIANT. IF YOU'RE NOT, YOU RISK A HEFTY FINANCIAL PENALTY.

Furthermore, having EU adequate status doesn't benefit UK organisations when it comes to dealing with businesses further afield. America and China for example – two countries the UK hopes to trade more with in the future – may have different conditions that UK businesses will need to satisfy. Overall, in the short term, businesses are in a good place and the status quo has been maintained. But from a long-term perspective, the future cannot be predicted – and businesses must be prepared.

Brexit is only one major event that has had an impact on GDPR. The more pressing concern is of course COVID-19. The first point to make is the most obvious one: now that many of us are working from home (and that working remotely is likely to be a major trend in the future), the way we physically stay compliant will change.

Organisations will need to update their policies to cover those small-but-important processes. Now there is no office shredder, how should employees dispose of sensitive documents? How should employees conduct meetings when there may be others within hearing distance? And when BYOD (bring your own device) is more common than ever, what measures should employees take to ensure a family member doesn't accidently access documents on a shared computer? These though are minor hurdles that can be overcome with training and a cultural shift. What is more important is ensuring infrastructure is up to scratch.

If businesses have relevant, accurate and up-to-date data, they will have keener insights and will be able to make smarter decisions

EMBRACING REMOTE WORKING

Data needs to be secure in order to be GDPR compliant. But the move to remote working is effectively widening businesses' security perimeter from a single building to potentially the entire globe. It's one thing to ensure only a certain type of computer in a single location can access data. But when a multitude of devices in multiple regions or even countries need to access it, keeping out bad actors while ensuring a smooth experience for employees is a big hurdle. This is of course not just a GDPR challenge. It falls into the wider bucket of security and is doubtlessly an issue businesses are grappling with now as they are forced to embrace remote working.

As technologies like the cloud become more commonplace and remote working becomes a staple of working life, questions about where data is stored and how it is kept secure will become even more important.

But remote working won't be the only lasting impact of COVID-19. The pandemic has turned the economy on its head: shop doors have been closed, high streets have been emptied and countless businesses have shut down. As it stands UK, 97 percent of businesses in the UK have already been disrupted as a result of the pandemic, as revealed by Dun & Bradstreet's COVID-19 Commerce Disruption Tracker.

The downtick in the economy could very well trigger a recession, which after a year of turmoil is exactly what businesses don't want. If this were to happen, it would be the second recession since the 2008 financial crash. Those in business back then will remember how during those hard times it was vital to migrate risk as much as possible. By having the right insights, businesses can make smarter decisions and weather hard times. And that brings us to data.

Data is crucial for providing these insights. If businesses have relevant, accurate and up-to-date data, they will have keener insights and will be able to make smarter decisions. For this reason, GDPR is vital. Failure to comply won't just result in fines, but will mean businesses won't have access to the best data possible – thus harming their decision making.

Another point to make is that many businesses, in the absence of having their own first-party data, will use a data supplier to get those market insights. This is a wise choice for many, but businesses must remember

to check the data suppliers' GDPR practises. If they buy data from a company that doesn't comply with GDPR, then vicariously they won't comply either.

And this is true from a wider partner perspective too. On the brink of hard economic times where businesses will be using data more than ever before, they must be sure to step back and do their due diligence. The need to make sure any data you process

GDPR WILL BE CHANGED, MOULDED AND EVOLVED IN THE FUTURE TO SUIT THE NEEDS OF THE UK

– which has been sourced by a supplier or partner – is fully compliant and won't land them in trouble.

GDPR is as relevant in 2021 as ever, and as we head into a data-driven future, it's vital organisations stay updated with the latest policies. The cost of not complying is starker than ever. That's partly because fines are so high. Whatever period of grace authorities gave when GDPR first came into force is now gone – in 2021, there is no excuse not to be compliant. If you're not, you risk a hefty financial penalty.

But the financial damage of a fine could pale in comparison to reputational damage. The public has never been more tuned into issues of the usage and mishandling of data. The collective consciousness has an innate suspicion of businesses using their data in nefarious ways. Being seen to not comply with GDPR could confirm their worst fears and make them hesitant to do with business with a company.

But I don't want to end this piece on such a negative note. While the motivation behind compliance is partly fear, I feel businesses are increasingly seeing GDPR as an opportunity. It's certainly true in the conversations with people I've been having. The questions customers ask me today are light years away from what I was being asked in 2018 as their data maturity has moved on. In my experience, businesses want to comply. They want to earn the trust of their customers. And importantly, they want to have healthy, clean data that's going to add real value to the business. This is the attitude we should all adopt. Particularly as that second recession looms on the horizon and the quality of our data is put in the spotlight.

Now isn't the time to do the bare minimum to simply avoid fines. Instead, businesses need to rethink how they gather, store and draw insights from data. They should be securing their infrastructure, shifting their work culture, putting in place new processes and ensuring they are working with established, credible data suppliers who are fully compliant. But most importantly, they need to ensure they are fully leveraging their data and are unlocking its true potential. And that can only happen by putting in place a robust, GDPR-compliant foundation on which to build ●

Nicola Howell,
Compliance & Privacy Attorney, leads Dun & Bradstreet's European privacy team which provides oversight and guidance on privacy issues to help ensure businesses are in compliance with privacy and data protection legislation.

Organisations need to update their policies to cover the issues caused by working from home