

GDPR is an evolution in data protection, not a burdensome revolution

By Steve Wood, ICO Deputy Commissioner (Policy)

Our new series of blogs aiming to bust some of the myths that have developed around the General Data Protection Regulation (GDPR) are proving incredibly popular and we are pleased that so many of you are finding them useful.

Here at the ICO, we took the view that it was time to sort the fact from the fiction before the new law comes into effect on 25 May 2018, given some of the misinformation and outright scaremongering out there – some of which, it must be said, seems commercially driven.

Our first two blogs covered the myths surrounding new fining powers and the issue of consent, and this week we want to talk about another widely held misconception – that the new regime is an onerous imposition of unnecessary and costly red tape.

Myth #4

GDPR is an unnecessary burden on organisations.

Fact

The new regime is an evolution in data protection, not a revolution.

Let's start off by being totally up front here. Any regulation has some sort of impact on an organisation's resources. That's unavoidable and GDPR is no different to any other new legislation in that respect. But thinking about burden indicates the wrong mindset to preparing for GDPR compliance.

What must be recognised is that GDPR is an evolution in data protection, not a total revolution. It demands more of organisations in terms of accountability for their use of personal data and enhances the existing rights of individuals. GDPR is building on foundations already in place for the last 20 years.

If you are already complying with the terms of the Data Protection Act, and have an effective data governance programme in place, then you are already well on the way to being ready for GDPR. Our GDPR overview and 12 steps to take now documents explain where there is continuity, what's new and how to plan.

Many of the fundamentals remain the same and have been known about for a long time. Fairness, transparency, accuracy, security, minimisation and respect for the rights of the individual whose data you want to process – these are all things you should already be doing with data and GDPR seeks only to build on those principles.

That doesn't mean there's any room for complacency. There are new provisions to comply with and organisations should start making preparations now, if they haven't done so already. But by and large, the new GDPR regime represents a step change, rather than a leap into the unknown.

Much of the criticism about GDPR seems to have focused on the perceived burdens it will place on SMEs and smaller organisations. We have long recognised that SMEs may have limited time and resources for compliance and have acknowledged this in our regulatory approach. But many of these criticisms fail to recognise the flexibility that the key principles in the DPA and GDPR provide – they scale the task of compliance to the risk. Many of the principles reinforce tasks businesses will already to undertake in relation to record keeping – e.g. the principle on data minimisation.

The principles are essentially the same whether you are a small business or a multinational corporation. Many of the actions SMEs should take are practical and straight forward – our updated toolkit is a good starting point.

It is not the size of the organisation that's relevant so much as the risk that particular businesses and types of data processing pose. Those handling particularly sensitive data, or processing personal data in potentially intrusive ways, for example.

Information management is key to compliance. Under GDPR, people will have strengthened subject access rights to the data you hold about them. This could well lead to more requests being received. So that's a real burden, right?

Whatever the size of your organisation, GDPR is essentially about trust. Building trusted

relationships with the public will enable you to sustainably build your use of data and gain more value. Through changing their data handling culture, organisations can derive new value from customer relationships.

Failing to get data protection right is likely to damage your reputation, your customer relationships and, ultimately, your finances. That goes way beyond increased fines – think brand damage and a subsequent loss of custom.

The ICO's annual research on privacy and data protection consistently shows that levels of public trust remain low. Conversely, it also shows that they would be more willing to provide their data, and for different uses, if they felt they could trust organisations to handle it fairly, securely and responsibly. And that provides a major opportunity and competitive advantage for those who can demonstrate that they get data protection right.

<https://iconewsblog.org.uk/2017/08/25/gdpr-is-an-evolution-in-data-protection-not-a-burdensome-revolution/>