

6 reasons why data protection is probably here to stay

The UK's decision in a referendum in June to leave the European Union has implications for privacy there, but this still means UK and other organisations will have to adopt the EU's General Data Protection Regulation, says data specialist **Peter Galdies**. This is why



OPINION
Peter Galdies
development director
DQM GRC

REASON 1:

The 2+ year negotiation phase

Formal negotiations for exit won't start until after Article 50 is invoked – which gives the UK's official notice to leave the European Union (EU) – and this now looks to be September 2016 at the earliest. During this mandatory two-year period all existing legislation – including the General Data Protection Regulation (GDPR) – continues as before.

Many forecast this might take much longer, with many estimates between three and six years. The GDPR is already law, and although organisations have two years in which to meet compliance, it would be unwise for businesses to assume that after this period there will no longer be a need to comply.

REASON 2:

Trading with the EU

The GDPR applies to and can be enforced against organisations which process data on EU citizens regardless of nationality or location. It doesn't matter if you are in France, Germany, the US or India, the GDPR law – and its penalties – can be applied. Therefore, organisations attempting to do business with EU citizens in Europe must comply with the rule. Failure to do so presents the risk of substantial fines – up to 4% of global turnover.

REASON 3:

We just trade in the UK so we're OK – right? Maybe not

With over three million EU citizens resident in the UK – and at least two million of these in employment – chances are UK-based businesses may have data relating to EU citizens.

The GDPR is mainly concerned with

processing personal information about those who reside in the EU – although the European Parliament seems to consider residence irrelevant – and offering goods and services to these individuals or monitoring behaviour. However, who determines whether someone is a resident or not? Does a two-month holiday in London by an EU citizen mean they are a non-resident? Does the individual need to be granted residency status within the UK to be excluded from the terms of the GDPR?

REASON 4:

The Information Commissioner thinks so

According to a statement on 26 June from the UK Information Commissioner, "If the UK is not part of the EU, then upcoming EU reforms to data protection law would not directly apply. But if the UK wants to trade with the [European] Single Market on equal terms we would have to prove 'adequacy'.

"In other words, UK data protection standards would have to be equivalent to the EU's General Data Protection Regulation framework starting in 2018.

"Having clear laws with safeguards in place is more important than ever given the growing digital economy, and we will be speaking to government to present our view that reform of the UK law remains necessary."

This implies that new Commissioner, Elizabeth Denham, who has a proven history of backing consumer rights while encouraging transparency within business, is likely to push legislation that mirrors the GDPR requirements. It's also worth noting that UK privacy experts were key in shaping this legislation in the first place – and that the view of what constitutes

good privacy doesn't change simply because the UK exits the EU.

REASON 5

Trade negotiations, an easy win

Over the next few years the pressure to negotiate a strong trade deal with the EU will also drive the adoption of supporting mirror legislation, designed to minimise barriers to continue trade. Measures such as open borders will be highly contentious.

But it's unlikely that improved privacy protection would be seen as such – in fact it's an issue that many could openly support and encourage as an easy win, which would provide increased compatibility and security for UK-EU trade and improved protection for both groups of citizens.

REASON 6:

It needs doing anyway

Most current UK data protection law was written before the widespread adoption of the internet and the consequent globalisation of trade, and the collection of vast amounts of new data about data subjects.

Social media services such as Facebook and Twitter didn't exist and current laws on data protection were not created to accommodate them.

It's easier than ever before to build and infer much about people from the data they generate, often unknowingly, on a daily basis. We're all entitled to a free and private life, so we need laws that help protect us – and the legal framework prior to GDPR doesn't cut it.

The GDPR, while far from perfect, does offer an improved model for data protection – and it is, perhaps arguably, the right and pragmatic approach for the UK to adopt similar legislation. 