Brexit and EU data privacy

Regardless of UK exit, new rules are coming

January 2017

Mark Thompson

Mark is a director and the Global Lead for KPMG's Privacy Advisory Practice, which helps clients address their complex multi-jurisdictional privacy challenges.

mark.thompson@kpmg.co.uk

At a glance:

- Organisations can be fined up to 20 million euros – or 4% of global turnover – for breaching GDPR rules
- UK companies seem to be lagging behind their continental counterparts in preparation for GDPR
- GDPR will come into force in May 2018 – just 10 months before the earliest likely date for Brexit

Forget about Brexit for a second and think about all the things that will determine the success of your business in the next decade. Critical is likely to be your ability to access and use customers' personal information in order to predict, personalise and perfect your offering. That is the case whether the UK is in or out of the EU and whether the customer lives in Manchester or Madrid.

And that is why British companies need to do more to prepare for arguably the biggest change to rules governing data protection for more than 20 years. Data is no respecter of national borders, and companies who fail to grasp that are not only locking themselves out of a 440 million-strong market, but may find themselves breaking new rules – the EU's General Data Protection (GDPR) – from next spring. The GDPR's provisions are not only tougher; the sanctions are as well. Organisations can be fined up to 20 million euros or 4% of global annual turnover – whichever is higher.

How has this slipped off corporate radars? Part of the problem is the coincidental timing of Brexit and the implementation of the GDPR. It comes into force in May 2018 – just 10 months before the earliest likely date for the UK's exit from the EU.

Some companies might be tempted to 'chance it' given the short window in which they believe regulators have to act against them. However, that approach looks risky in the extreme. In my view companies that fail to collect, use, retain, disclose and transfer information on EU citizens correctly remain vulnerable, even after Brexit.

UK gets tough too

First, it looks likely, based on what the UK Government has already said, that it will comply with the GDPR while it negotiates Brexit. We already know

that the UK privacy regulator – the Information Commissioner's Office – is adamant the UK needs some sort of strong and equivalent privacy law in the UK. The direction of government thinking on data protection seems clear.

Second, if the government does implement the GDPR, a British version would remain UK law until the government chose to repeal it. (Theresa May has been clear her government will transpose the "acquis" – the whole body of EU law – onto British statute books). And it seems unlikely that government would seek to repeal it down the line, especially since the prime minister wants to sign a free trade agreement with the EU.

Finally, there is a risk that British based companies may still face action after the UK has left. The European Commission has shown on repeated occasions a willingness to launch cases against companies beyond its borders – just ask some of the United States' biggest tech companies. The GDPR reaches further than many realise. For example, say a British online events company sold tickets for a rugby match at the Stade de France to someone with an EU billing address, or emailed them to a customer living in the EU. In both instances it would probably be subject to the GDPR. Even if the company simply had a large proportion of customers in the EU, or allowed customers to pay in euros, the regulation would likely apply.

Think bigger

But quite apart from a narrow compliance issue is another about ambition. Even if the UK opted for a much lighter regulatory touch, businesses will need to take notice of the GDPR if they are serious about conducting business in Europe.

I can understand why the GDPR might have slipped off companies' agendas. Brexit has been all pervading and is sucking up an increasing proportion of management's time. The weaker pound, supply chain worries, staffing uncertainty, the prospect of tariffs and regulatory change: just maintaining the status quo is as much as many companies can handle right now. In this position, it is incredibly tempting to assume new EU regulations simply "don't apply to us".

That is perhaps one reason why, in my experience, British companies seem to be lagging their continental counterparts in prep for the GDPR.

Yet the stark truth is that we have little choice. Organisations – public and private – handling customer data need to ready themselves. That means understanding their level of maturity around privacy risks; developing a plan to safely handle information; and lastly starting to fix the parts of the system that need most urgent attention. With 15 months until the GDPR takes effect, the clock is running.

What do I do now?

The GDPR will require most organisations to significantly improve their privacy control environment and rethink the way they collect, store, use and disclose personal information. That is complex and takes time. Certainly, most organisations can't afford to wait and see what form Brexit takes since doing that would leave them too little time to get ready. There are some immediate steps organisations should take however:

1. Raise awareness at board level – executives need to understand the gravity of the situation and the task before them. Ultimately, most will need to put investment into a privacy improvement programme.

2. Understand your current state set against the GDPR in order to ascertain where your organisation is exposed to risk and analyse your desired state in order to determine what your risk appetite is.

3. Plan and implement a privacy improvement programme to fix gaps and reach that desired state.

What are some of the changes introduced by the GDPR?

The GDPR transforms a number of existing requirements and introduces a raft of new ones. These changes are complex and are likely to require significant enhancements in the way organisations process personal information.

	EU Data Protection Directive (previous)	GDPR
Fines	Fines vary by jurisdiction (e.g. UK £500,000)	A tiered fining structure depending on infringement Level 1 is 2% of global turnover or €10m (whichever is higher). Level 2 is 4% of global turnover or €20m (whichever is higher)
Data protection officer (DPO)	Generally no requirement to appoint a DPO	DPO required for 'government bodies' and organisations conducting mass surveillance or mass processing of Special Categories of data
Supervisory authorities (SA) enforcement powers	SAs have limited powers under national law	SAs will be given wide-ranging powers
Inventory	No reuirement to maintain a personal information inventory	Generally organisations will need a personal information inventory
Breach notifcation	Generally there are no obligations to report breaches	Requirment to preort Privacy breaches to the regulator within 72 hours and potentially to the Data Subject
Security	Vague requirements around security (i.e. 'adequate level')	Exploicit requirements around monitoring, encryption and anonymisation
Private Impact Assessments (PIAs)	There is no mandated requirement to perform PIAs	Companies should perform PIAs if the activity is considered 'high-risk'
Data subject's rights	Varioua rights, including right of access	Rights extended to include Data Portability and the Right to Ensure
Sensitive personal data	This includes religious beliefs, physical/mental health and thnic origin amongst others	Similar but extended to include biometric and genetic data
Consent	Potential to rely on 'implicit' consent depending on jurisdiction	Requirement to gain unambiguous consent (i.e. explicit)
Data Processors (DP)	Processors have limited regulator exposure or processing activities	Processors are also covered. Controllers must conduct due dilligence into processors suitability

kpmg.com/uk

CREATE | CRT075675 | January 2017