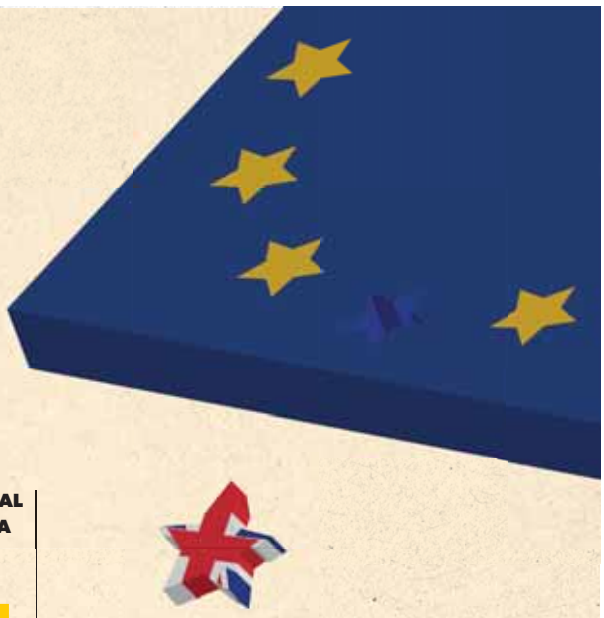
A PLACE OF CYBER SAFETY

Alan Calder assesses how Brexit is likely to affect cyber security in the UK



Notwithstanding our present government's position on Brexit and the widespread uncertainty about the exact nature of the UK's proposed "deep and special partnership" with the EU, there is at least something we can be sure of: if we are to continue doing business with EU organisations after Brexit, we will need to abide by EU cyber and data security laws. What might not be obvious, however, is that we will also need to do so in order to trade with much of the rest of the world, thanks to the scope of EU law.

When it comes to cyber security legislation, the EU leaves other blocs in the shade (eg, the US doesn't have a federal cyber security law). In recent years, the EU has proposed innovative laws to improve member states' cyber resilience, such as the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (which affects digital service providers and operators of essential services rather than accountants), both of which come into effect in May 2018. With the European Commission's September 2017 Cybersecurity Package – a programme that is likely to increase in ambition and scope in the coming years – the EU will effectively set global standards on cyber security.

The UK government has proposed a new Data Protection Bill to enact the GDPR and will implement the NIS Directive in March 2018, so we will be compliant with EU law at the point we formally leave the union in 2019. After that point – unless, that is, a deal on data transfers is included in our transition arrangements – we will be classed as a third country and the EU will need to determine that we afford data adequate protection in order for data transfers to continue. This is where we encounter major challenges.

ADEQUACY DECISION

To date, the European Commission has adopted 12 adequacy decisions, with Andorra, Argentina, Canada (for transfers to commercial organisations that are subject to the Personal Information Protection and Electronic Documents Act) the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (for certified companies).

THE INTERNATIONAL TRANSFER OF DATA IS VITAL TO THE UK'S PROSPERITY

£240bn
Value of the UK's data economy

11.5%
of the world's data flows through the UK

75%
of the UK's cross-border data flows are with the EU

Alan Calder, CEO, IT Governance

As the Confederation of British Industry's deputy director-general for policy and campaigns Josh Hardie told the confederation's September 2017 Cyber Security Conference in his keynote speech, the last third country to strike such a deal was New Zealand, and that took about four years. "I think we've got to be clear that we don't have four years," Hardie said. "With Brexit on the horizon there is a risk – I don't want to overstate it, but there is a risk – that we are facing a data cliff-edge."

If a deal is not reached, UK organisations will have to rely on binding corporate rules, standard contractual clauses or approved codes of conduct to transfer data to and from the European Economic Area until an adequacy decision is reached. To avoid this administrative burden, the UK government therefore "believes it would be in the interest of both the UK and EU to agree early in the process to mutually recognise each other's data protection frameworks as a basis for the continued free flows of data between the EU (and other EU adequate countries) and UK from the point of exit until such time as new and more permanent arrangements come into force".

Whatever your opinion of the EU, whatever your position on Brexit, it's an incontrovertible fact that international trade requires standards to be maintained, so it's in our interests to maintain a frictionless cross-border flow of personal data.

In terms of data protection, the EU is leading the way in setting those standards. If you want to supply that market, or even be in the supply chain of a company that does, then you need to conform with the likes of the GDPR – or risk being left behind. ●

BENJAMIN HARTE/IKON