Mr Paul Sexby, Global Security Manager & Data Protection Officer at Abertis Mobility Solutions – Written Evidence (DAT0002)

House of Lords

European Affairs Committee

Dated: 01 May 2024

Views on possible threats to EU-UK Adequacy

In 2017 the undersigned presented to circa one thousand five hundred (1500) peers at the Information Security Forum's Global Congress (Cannes) on the implementation of the EU GDPR.

I took the audience through the high-level requirements for implementing the GDPR from a risk, information security and governance perspective, emphasising how much of the Regulation should already be in place!

In the Q&A following the presentation a delegate asked: "*for my views of the possible impacts to the UK following the BREXIT referendum?*".

I responded: "*The UK needed to achieve and subsequently maintain adequacy with the EU or the impacts to IT Services and UK businesses in general could be more damaging than the impacts of BREXIT to the financial sector.*

I indicated I was also concerned that "*the UK would 'go-it alone' and diverge from the EU, potentially opening doors to third countries not deemed adequate by the EU and creating a potential "Back-door" that the EU would not like, further weakening our own adequacy chances.*" I ended by stating "*I hope to be proven wrong*!"

I stand by those statements today. I believe the UK is at an increased risk of attaining adequacy which will have a monumental impact to the UK economy, IT services and businesses in general as a high proportion of organisations interact with the EU in some way - if we are not seen as a trusted partner our business interests, and the National economy will be severely damaged. To reiterate "*I hope to be proven wrong*".

The UK's future adequacy with the EU is not solely linked to Data Protection Legislation but encompasses other important legislative instruments. Three such instruments being:

- The **Investigatory Powers Bill** - could hinder technological advancements aimed at improving consumer privacy, integrity and security.
- **Digital Operational Resilience Act** (DORA) - UK is introducing its own DORA equivalent (UK DORA), meaning that UK technology

businesses with Financial Services customers in the EU will need to navigate two regulatory regimes in parallel. The EU's DORA is significantly more progressed than UK DORA s from the UK's existing approach to operational resilience approach involves firms identifying "important business services" and determining their "impact tolerance," with detailed considerations of various factors affecting service disruption. EU DORA mandates the creation of an ICT risk management framework, including digital resilience strategy and governance, but is less granular in requiring businesses to set impact tolerances for each critical function or service.

- **Data Protection and Digital Information Bill** (DPDI Bill) - another UK legislation that diverges from the EU position and which will make our ability to attain adequacy more challenging.

The UK will face greater scrutiny and uncertainty in the run-up to the EU's renewed decision, unnerving the markets and deterring investors from the UK with the consequential impacts over time on employment not just for IT services but the organisations (and thereby people) that support them.

Conclusion

Failure to retain adequacy will have significant repercussions on the country and its economy for a long time.

Whilst we may forge partnerships, and 'Adequacy agreements', with other countries not being seen as 'Safe' or 'Adequate' by our nearest and most influential neighbours will have significant consequential effects. We will lose significant market share and future business opportunities which will impact the Treasury and the country forever.

And finally, "***I hope to be proven wrong!"***

Paul Sexby
Global Security Manager & Data Protection Officer
Abertis Mobility Services

Disclaimer. The views and opinions set out above are my own and have not been endorsed or sanctioned by my employer.

Received 1 May 2024