Views sought to boost the security of UK data centres and cloud services

- UK's essential services and wider economy are becoming ever more reliant on large-scale data storage and processing services to operate

- Call for evidence launched to seek views on strengthening industry's cyber and physical security systems

The UK's data infrastructure should improve its protections from cyber threats and disruption. The Government announced today it is seeking views on how to boost the security and resilience of the UK's data centres and online cloud platforms.

Views are sought on tools currently used in other regulated sectors, such as having an incident management plan in place, notifying a regulator when an incident impacts their services, and a requirement for a person board or committee to be held accountable for security and resilience.

The UK's data storage and processing infrastructure includes physical buildings housing large computer systems, which store and process huge volumes of data, as well as cloud platforms which provide remote, shareable computing services via the internet.

New protections would build on existing safeguards for data infrastructure, including the Networks and Information Systems (NIS) Regulations 2018 which cover cloud computing services. The National Cyber Security Centre and Centre for the Protection of National Infrastructure also regularly update guidance for data centres and their online assets.

The plans will give greater confidence to the millions of people who rely on these digital services every day to make calls, and send photos and messages. Proposals will also help small businesses who use cloud platforms as a cheaper, more efficient way to access essential IT services and as the UK's reliance on digital services grows, shielding this infrastructure against disruption will protect the economy.

Data minister Julia Lopez said:

> Data centres and cloud platforms are a core part of our national infrastructure. They power the technology which makes our everyday lives easier and delivers essential services like banking and energy.
>
> We legislated to better protect our telecoms networks and the internet-connected devices in our homes from cyber attacks and we

> are now looking at new ways to boost the security of our data infrastructure to prevent sensitive data ending up in the wrong hands.

Research from the Office for National Statistics shows that from 2013 to 2019 the number of businesses purchasing 'cloud computing services' to store their data has more than doubled, with more than half (53 per cent) of businesses now relying on cloud platforms.

The UK government is today launching a call for views and inviting contributions from data centre operators, cloud platform providers, data centre customers, security and equipment suppliers and cyber security experts to understand the risks data storage and processing services face. It wants to know what steps they are already taking to address any security and resilience vulnerabilities.

The call for views will also ask companies which run, purchase or rent any element of a data centre to provide details of the types of customers they serve.

Based on the evidence, the Department for Digital, Culture, Media and Sport (DCMS) will decide whether any additional government support or management is needed to minimise the risks that data storage and processing infrastructure face.

The work is part of the government's National Data Strategy to ensure the security and resilience of the infrastructure on which data relies.

Julian David, CEO, techUK said:

> The UK's data infrastructure – through cloud platforms and data centres – underpins the digital technologies and services upon which all citizens and organisations increasingly rely.
>
> The technology sector already plays an important role in strengthening resilience across the UK economy and techUK welcomes the opportunity to engage with Government on these significant issues. One particular focus will be how these proposals will align with wider efforts to strengthen resilience across sectors as well as the wider ambitions outlined in the UK's National Cyber Strategy – which is a continuation of UK Government's longstanding leadership in cyber security.

Ends

Notes to Editors:

- The eight-week call for views will run until 23:59 on Sunday 24 July.

- Following the call for views, the government will review the feedback provided and will publish a response.