Unsplash © Dominik Schroder

Is 2022 the year that data residency takes off?

Businesses today are navigating an incredibly complex regulatory landscape. Recent data residency laws are now pushing companies toward residency as a service and I believe this is more than just a trend, but will soon become an obligation for many technology providers.

Data privacy has become a major priority for regulators across the globe in recent years. In 2018, the *EU* brought into effect “the most important change in data privacy in 20 years”, ensuring comprehensive data privacy rights to its citizens with the General Data Protection Regulation (GDPR). This sparked a wave of similar acts across the world, such as the California Consumer Privacy Act (CCPA), giving consumers more control over the personal information that businesses collect about them.

Five years on, *Gartner* has predicted that nearly two-thirds of the world’s population will have their personal data protected under new privacy regulations by next year. This comes as more than *60 jurisdictions* around the world have now enacted data laws, many inspired by GDPR, and all varying in terms of their priorities and levels of protection. This has created a diverse regulatory landscape, making compliance a complex challenge for enterprises and businesses operating internationally.

The era of borderless data is ending

The increasing diversity of regional privacy regulations has fundamentally shifted the way data is treated at a transnational level. Since the early days of the internet, data has flowed freely across the globe, acting as what *The New York Times* has called “a kind of borderless currency that underpins the digital economy.”

But this era of borderless data is slowly coming to an end, as more and more countries have accelerated efforts to control the digital information produced within their borders. For example, *India’s Supreme Court* is moving to pass a law which would limit which data can leave its jurisdiction. Meanwhile, last year the Chinese Government introduced its Personal Information Protection Law (PIPL), which guaranteed the protection of personal information and data of all ‘natural persons’ located in China.

In the pursuit of ensuring data privacy for citizens, regulators are creating a new, regionally fragmented digital landscape. But what does this mean for multinational organisations responsible for storing and managing customer data globally?

Now more than ever before, companies must prioritise partnering with technology providers that have data privacy at the core of their offering to ensure they are compliant in all their operational regions. This is already a major priority for many business decision makers; according to a recent poll conducted by *Capgemini Research Institute*, 69% of enterprise leaders have cited potential exposure to extraterritorial laws as a top concern when using the cloud.

As such, organisations must now take note of where their data resides, and partner with technology providers that prioritise customer privacy in their product offerings. Encryption, zero-trust controls, and threat detection are no longer nice-to-haves. They are necessities.

The future of compliance and privacy offerings

To ensure compliance in this increasingly complex global regulatory landscape, some *cloud companies* have introduced multi-region data centres. This allows customers to choose where their data physically resides, providing them with the capacity to meet regional data protection and privacy requirements. For instance, a French company with a US-based cloud provider can opt to have their data reside in the UK, which would enable them to comply with GDPR.

Moving forward, ‘data residency’ will become an integral part of organisations’ and cloud providers’ operational structure. The number of laws and policies that require digital information to be stored in a specific country has *more than doubled since 2017,* and with new data localisation regulations being proposed across the globe each month, there is little sign of this trend slowing down any time soon.

But this doesn’t come without its challenges. Cross-border data flow restriction has been *shown* to reduce trade and productivity. To combat this, cloud providers will focus on offering streamlined solutions that enable international collaboration that does not compromise security, privacy or compliance. Those who actively work with regulators, and weave compliance into the fabric of their offerings, will come out on top.

We are now transitioning into an era of post-globalisation, where citizens’ digital entities are intrinsically linked to the nation in which they reside. Data is no longer a borderless commodity – its residency *matters* – and 2022 will be the year that organisations take the geographical location of their data seriously.

Sébastien Marotte is President EMEA at *Box.*

Article by SÉBASTIEN MAROTTE