DATA SOVEREIGNTY

Digital Data and the Promise of Sovereignty

Data Sovereignty

With data breaches occurring daily to the world's largest brands, including high profile tech companies, c-suites of every organisation need urgently to recognise that cyber security it not just about IT, it is about data governance. And the responsibility for data governance falls firmly – and heavily – at the feet of management.

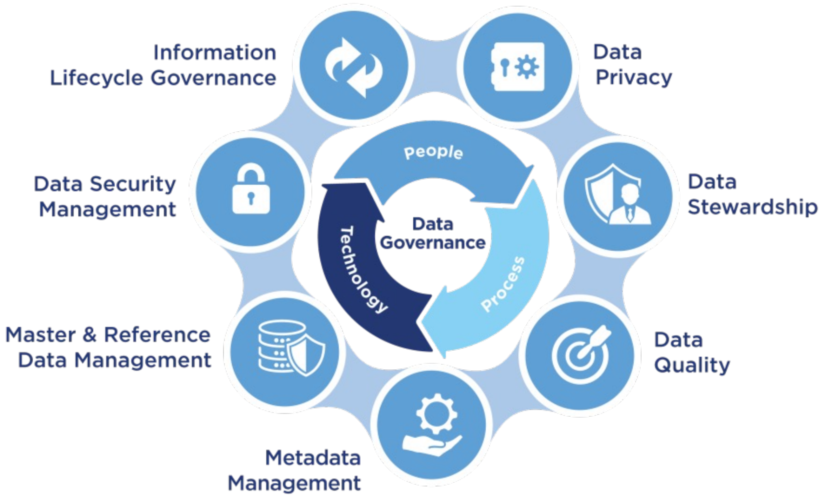
With the increasing inclusion and application of punitive laws for data breach, it is vital for the c-suite to take ownership of key data protection issues, such as data sovereignty. Does the board understand the current requirements for transferring data between the EU and US – or is it at risk of incurring a fine, such as the record 1.2 billion fine imposed on Meta, not for experiencing a network breach but for violating EU data protection rules? With Managed Service Providers (MSPs) increasingly concerned about their data liability in the light of rising breach and punitive regulations, is the c-suite aware of the complex, time consuming and expensive contractual negotiations now required?

Simon Pamplin, CTO at Certes Networks, explains why those organisations still taking a tech-first approach to cyber security are fundamentally misunderstanding the objectives of global data protection regulation – and leaving both individuals and the business dangerously exposed as a result.

Data Ownership

With the increase in global data protection regulation, the concept of data sovereignty has become a prime concern for every business. Essentially, data is subject to the laws and regulations of the country where it is stored or processed. However, with the latest data protection regulation from the Kingdom of Saudi Arabia, the country has extended the concept of data sovereignty to include the use of data relating to Saudi citizens and businesses anywhere in the world. And the penalties for breaching this regulation include a prison sentence.

Companies need, potentially, to comply with an array of local data protection laws when managing, storing and transferring data across borders – something that has become ever more challenging as more data is stored in the cloud and processed in more than one country. For companies using Managed Services Providers (MSPs) to deliver some or all of the infrastructure, the burden of responsibility can be confusing.



Is the data controller (the data owner) or the data processor (the infrastructure owner) liable in the face of data breach?

In fact, the liability in the event of a breach is down to whoever had control over protecting that data. That could be the data owner but it also could be the service provider if they provide the 'secure links' over which the data travels.

Endemic Confusion

Yet this issue of responsibility and data ownership continues to cause confusion and significant costs to both MSPs and businesses. Recent research from Certes Networks confirms that far too many businesses are simply handing over responsibility to an MSP – and expecting the provider to pick up the financial cost should a data breach occur. Companies employing third party organisations to deliver security policies expect MSPs to cover 48% of the costs in the event of a data breach. Astonishingly, 73% of MSPs also consider themselves responsible for paying fines and damages and believe they should pay 51% of the costs.

With incidence of breaches continuing to rise, this is clearly not a sustainable situation. Indeed, there is growing evidence that MSPs are turning away business due to the level of risk associated with the prospective client's data. This trend should be raising large red flags for businesses: if a top ranked MSP refuses the business, a company will have no option but to turn to another MSP who will either hike up the price to cover the risk or, more worryingly, have a far less robust and rigorous approach to risk assessment and, potentially, risk management.

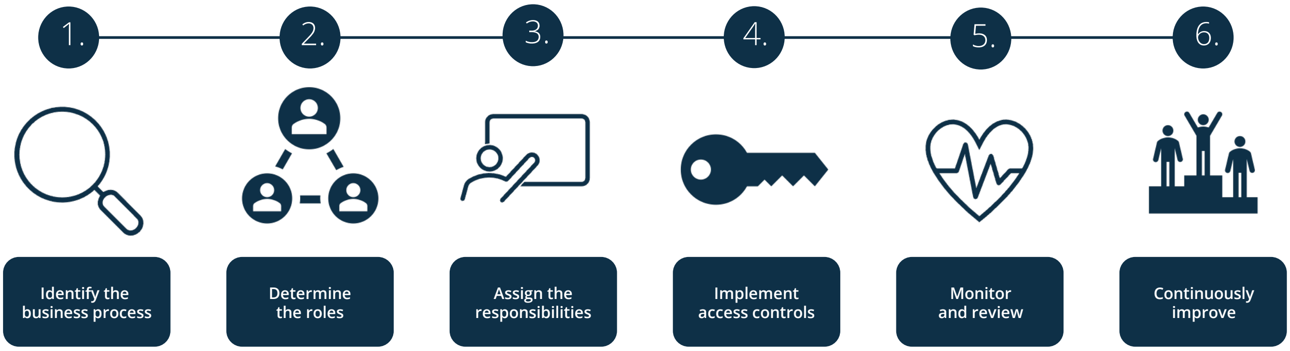
> Creating a clear line of responsibility in this way immediately overcomes the expensive and resource consuming contract negotiation that defines every MSP relationship today. It removes the burden – and cost – for an MSP attempting to safeguard the data over which it has no control and no knowledge.
>
> *Paul German – CEO, Certes Networks*

Separation of Duties

The issue of data sovereignty needs to be managed in a very different way to safeguard not only the data but also commercial relationships. This can only be achieved if these organisations both embrace a separation of duties and recognise the importance of wrapping security around the data, rather than relying on perimeter security. By using encryption to ensure that any PII is only visible by the intended recipient, an organization removes any constraints or concerns regarding geographic location. It is also important to note that the technical guidelines produced by the EU suggest that it is the data controller that should own and manage the encryption keys, reinforcing the regulatory push towards a separation of duties.

With this approach, a business accepts its obligations as data owner (controller) to protect its own data; the MSP or any other part of the infrastructure then accepts its role to deliver an optimal performance as a transport mechanism.

Creating a clear line of responsibility in this way immediately overcomes the expensive and resource consuming contract negotiation that defines every MSP relationship today. It removes the burden – and cost – for an MSP attempting to safeguard the data over which it has no control and no knowledge. Instead, the business can use encryption to wrap vulnerable data or PII in an additional layer of security. The result is risk mitigation for MSPs and data protection for data owner of the assets.



1. Identify the business process
2. Determine the roles
3. Assign the responsibilities
4. Implement access controls
5. Monitor and review
6. Continuously improve

Schrems ii Compliance

This separation of duties also enables organisations to overcome some of the data sovereignty issues currently plaguing global data protection regulations. This is particularly key within Europe where the transfer of data to the US for processing and storage continues to create confusion under the General Data Protection Regulation (GDPR). Since 16 July 2020, when the European Court of Justice issued the Schrems ii judgement, companies have been aware of the potential concerns regarding the transfer of data from the EU to the US. The decision in May 2023 to not only fine Meta 1.2 billion euros ($1.3 billion) but also order the company to stop transferring data collected from Facebook users in Europe to the United States, has raised very serious issues for c-suites globally. Meta did not experience a hack or network breach. The company was fined because it was deemed to be transferring PII from the EU to the US in a way that could be read by US surveillance programmes and hence interfered with the requirements for the fundamental rights to privacy, data protection and effective judicial protection as defined by Max Schrems.

Companies cannot rely on network monitoring or analytics tools to highlight such an issue because the network was performing as expected, efficiently transferring data from one place to another. This is not a network problem, it's a data problem. The breach of GDPR and the Schrems ii judgement could only have been avoided if the company had taken a data-first approach and used policy-based encryption to either block or encrypt any data sent overseas.

By wrapping security around the data and using encryption to ensure that any PII is only visible by the intended recipient, an organisation can deliver virtual data sovereignty and remove any constraints or concerns regarding geographic location.

Conclusion

By achieving data sovereignty through the protection of the data, rather than relying on any physical or geographic constraints, a business effectively addresses the problems created by Schrems ii and ensures GDPR compliance. It enables organisations to embark upon MSP negotiations based on the quality and performance of infrastructure rather than being derailed by expensive data liability debates. And, critically, it provides the c-suite with protection against the escalating personal and corporate risk associated with data breach.

> **Companies cannot rely on network monitoring or analytics tools to highlight such an issue because the network was performing as expected, efficiently transferring data from one place to another. This is not a network problem, it's a data problem.**
>
> *Simon Pamplin – CTO, Certes Networks*

Contact Certes Networks
300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1 (888) 833-1142
sales@certesnetworks.com
www.certesnetworks.com