CERTES NETWORKS

NAVIGATING DATA SOVEREIGNTY

Lessons from the Meta Breach

Meta hit with the largest GDPR breach to date

Earlier this year, Meta was issued the largest fine ever by the European Union for a GDPR breach at a whopping $1.3 billion. The fine came into place as Meta violated EU privacy laws by transferring the personal data of Facebook users to servers in the United States.

This monumental penalty serves as a powerful reminder of the imperative to safeguard personal data and underscores the unwavering resolve of regulatory bodies when it comes to enforcing corporate compliance.

Meta's substantial fine sets a precedent, sending a clear message to other businesses that stringent measures must be taken to protect user data, else they face similarly substantial consequences.

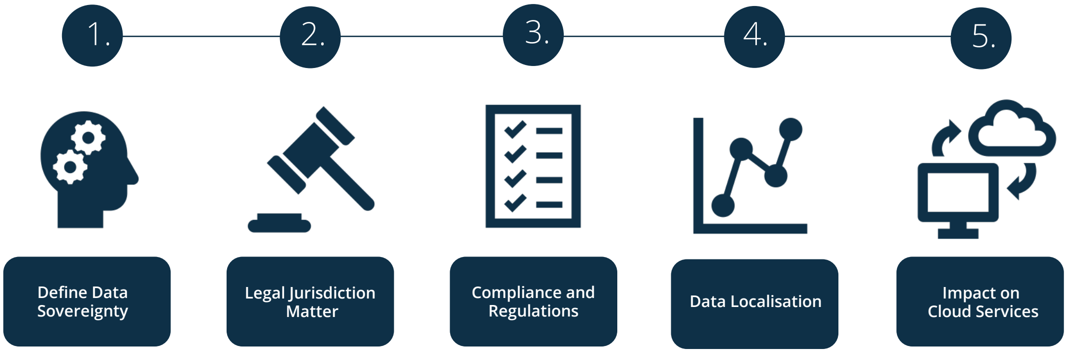
Simon Pamplin, CTO at Certes, delves further into the concept of data sovereignty and the challenges faced by companies like Meta in protecting user data. Pamplin below discusses the shift from traditional network security to securing the actual data itself as a means to prevent potential breaches and regulatory fines.

Understanding Data Sovereignty and GDPR

With the heightened enforcement of global data protection rules which we have seen with Meta, the notion of data sovereignty has evolved into a pressing issue. In essence, data is beholden to the rules and regulations of the nation in which it's held or processed. Some countries have stretched this idea to encompass data associated with their citizens and businesses across the globe. Violating these regulations can even lead to imprisonment.

Navigating the landscape of handling, preserving, and transferring data across borders has grown more intricate as cloud storage and cross-national data handling become standard practices. This intricacy is further heightened for organisations that rely on Managed Service Providers (MSPs) for their infrastructure requirements. In cases where an MSP is implicated in a data breach, accountability is shared between the data proprietor and the data handler (MSP).

Understanding Data Sovereignty



1. Define Data Sovereignty
2. Legal Jurisdiction Matter
3. Compliance and Regulations
4. Data Localisation
5. Impact on Cloud Services

Challenges Faced by Companies like Meta

The significance of our personal data has grown substantially over recent years, owing to the widespread use of platforms like social media and the increasing reliance on online activities such as banking. Our data, once perhaps undervalued, has now become a highly valuable asset. This shift is evident considering how deeply integrated it is within our lives and the potential risks associated with its misuse, including identity theft and cloning.

The escalating value of personal data prompts individuals to expect rigorous safeguards from the businesses they engage with. As the world becomes more interconnected and data-driven, the responsibility to secure this invaluable resource becomes even more critical so the organisations that are collecting and handling personal data must recognise their responsibility to protect the data, no matter where it’s located or processed - as GDPR regulations hold data owners accountable.

> **Meta's record-breaking GDPR fine is a stark reminder that data protection is paramount. We must safeguard user data at all costs. Compliance is not optional; it's a core responsibility for every organisation and a data centric approach to data security is a must in today’s world.**
>
> *Paul German – CEO, Certes Networks*

Shifting the Focus: Data-centric Security

Traditional network security has leaned heavily on perimeter protection, often at the cost of overlooking vulnerabilities. However, the constant stream of breaches and growing regulatory pressure casts doubt on this approach.

The Meta breach serves as a poignant reminder that companies cannot depend solely on network monitoring or analytics tools to detect such issues. Despite the network functioning as intended - facilitating seamless data transfers - this breach underscores the root cause as a data-related challenge, not a network glitch.

GDPR violation and the Schrems II ruling could have been averted had Meta adopted a data-centric approach, employing policy-based encryption to either prevent or secure overseas data transmission.

Adopting an approach like the Certes Layer 4 Solution, where data security is woven around the core, and implementing encryption mechanisms to ensure Personally Identifiable Information (PII) remains visible solely to the intended recipients, organisations can achieve a form of virtual data sovereignty. This approach eliminates concerns tied to geographic boundaries, giving organisations greater freedom and control.

Costs of a Data Breach

Reputational damage

Financial losses

Operational challenges

Legal ramifications

Lessons Learnt and Recommendations for Ensuring GDPR Compliance

So, what can companies learn from incidents like the Meta breach? The key takeaway is a shift in perspective. Companies must broaden their focus and understand that as data owners, they hold responsibility for the data entirety, regardless of where it resides. Designating the responsibility to service providers or the cloud doesn't hold up in the eyes of regulators. Data ownership matters, and any entity collecting personal, sensitive or intellectual data must embrace that responsibility throughout its lifecycle.

The significance of adhering to these principles cannot be overstated. While GDPR rules might have seemed like a minor annoyance, they underscore a larger responsibility that organisations must embrace seriously. As the landscape of data protection evolves, this understanding will become increasingly pivotal.

Amidst the evolving landscape of data sovereignty, the breach accentuates the complex challenge of handling data across borders and reliance on Managed Service Providers. Meta's breach amplifies the need for organisations to recognise the escalating value of personal data and their responsibility to safeguard it, regardless of its location. Data protection isn't just a regulation to meet but a core responsibility to embrace. As regulations get stricter and data risks continue, this awareness guides us through the complex world of data security and privacy.

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.

> **The primary focus in the network industry has been to safeguard the network perimeter to keep unauthorised individuals out. However, what we truly need to prioritise protection for is the most valuable asset at stake – our data. This is something that has been overlooked.**
>
> *Simon Pamplin – CTO, Certes Networks*

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

CERTES NETWORKS

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