A Hitchhiker's Guide to

CROSS-BORDER DATA PROTECTION

PROTEGRITY

IMAGINE DOING BUSINESS IN A BUBBLE.

You are an international company only allowed to make decisions using data collected within your country and by your business unit (BU). You also cannot share data with subsidiaries or third parties. It would be challenging to conduct day-to-day business, let alone innovate and grow.

Fortunately, this isn't the state of business today. Organizations transfer trillions of data points across borders daily. The term "Cross Border" refers to movement and transactions across boundaries, including geographic, legal, and departmental.

As data transactions are shared, maintaining data privacy becomes of utmost importance. The impact of cross-border data transfers goes beyond the individual company level. The Software Alliance emphasizes its importance by stating that **"Cross-border data transfers allow software companies to provide new and innovative services to every sector of the economy – driving growth, enabling the technologies of the future, improving health and safety, and promoting social good."**

When GDPR went into effect in 2018, protecting cross-border data transfers became a higher priority for many international organizations doing business in or with customers in the EU. But cross border doesn't only refer to geographical borders such as between countries; logical borders exist within organizations across which data is also transferred. Therefore, businesses must ensure data separation is preserved and protected across all types of borders.

Geographical Cross-Border Transfers

Cross-border data transfer applies to data movement outside of its original jurisdiction. A geographical cross-border data transfer could consist of a data export from a country within the EU to one outside the EU. For example, if a French company outsources IT support to India, access by the support company to the data collected in France means it must travel across borders. When such a transfer is made, data sovereignty is of particular concern.

Data Sovereignty

Data sovereignty is the idea that data is subject to the laws and regulations of the country in which it was collected. Currently, more than 100 countries have some form of data sovereignty law in place, including the Personal Information and Protection Documents Act (PIPEDA) in Canada, the Act on Protection of Personal Information (APPI) in Japan, and The Data Protection Act in Kenya. While adopting these data laws goes a long way to protect the individual, organizations still need help to balance the restrictions against their business needs.

The World Economic Forum explains,
We are witnessing a proliferation of policies around the world that restrict the movement of data across borders, which is posing a serious threat to the global digital economy, and to the ability of nations to maximize the economic and social benefits of data-reliant technologies.

Data covered by data sovereignty laws cannot leave its original jurisdiction; it needs to be protected so that only the jurisdiction in which it was collected can authorize and control the reidentification of the data back to plain text. Companies must comply with these laws or face harsh penalties and fines. For example, Meta, Facebook's parent company, has been fined more than $1 billion for several breaches of GDPR. Amazon also received a single $888 million fine for breaching GDPR compliance.

Data sovereignty is a significant component of data compliance, adherence to laws, regulations, policies, and standards regarding the use and management of data. Data compliance includes not only regulations on data transfer but also regulations on storing and protecting data and standards for cybersecurity (like FISMA for government agencies), cloud computing, and even financial reporting. (Remember Enron? They helped spur this requirement).

Although keeping up with so many data sovereignty laws might feel overwhelming, a robust IT infrastructure with the right data de-identification technology can ensure you maintain data compliance and prevent breaches regardless of where the data needs to travel.

Logical Cross-Border Transfers

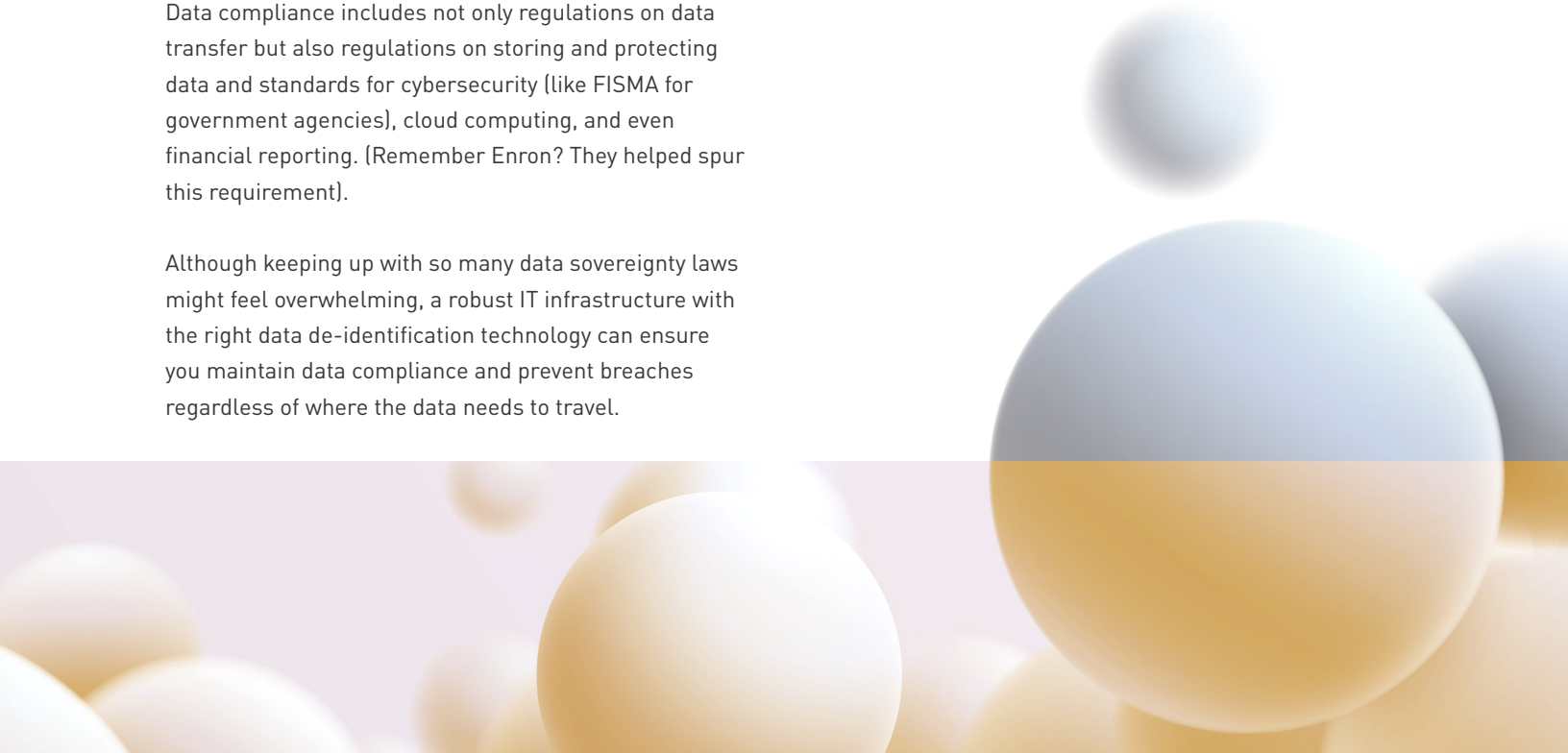
Logical borders also exist. These include within a company between BUs, such as when one BU is privy to personally identifiable information that another is not (think HIPAA) or within a company from on-premises to the cloud. For example, medical providers can access PHI within companies that handle private health information (PHI), but billing is denied access. Conversely, medical providers don't have access to the payment card industry (PCI) data that the billing department uses to process customer payments via credit card.

Another type of logical boundary is a logical legal boundary. This type of boundary is between a company and its subsidiaries. For instance, Johnson and Johnson may do market research on women ages 25-34, which is a demographic applicable to their subsidiary Neutrogena. The sharing of this research constitutes a cross-border transfer, even if they are located in the same city.

Data Protection

Data protection is a primary concern when cross-border data transfers occur, whether logical or geographical. Data must be protected in accordance with all applicable laws and regulations so only people allowed to access sensitive data can view it unencrypted in cleartext.

Existing regulations are ever evolving, and new ones are quickly surfacing, so your data protection must also evolve to ensure consistent data compliance.



Solutions for Data Protection

As confirmed by the Organisation for Economic Co-operation and Development (OECD), organizations are "increasingly reliant on data transfers in support of their business activities," but regulations can prevent them from moving data outside their original jurisdiction.

Businesses should be aware that:

- Data sovereignty requires a different set of security tools
- Privacy regulations limit data flows
- Massive labor shortages in privacy and security slow data access and usage
- Compliance remains and obligation with real-world consequences

The sensitive data usage that built your business could destroy it. Turn the threat of sensitive data privacy usage into an opportunity.

PROTEGRITY

With the Protegrity Data Protection Platform, companies can execute cross-border data transfers while protecting their data so that only the original jurisdiction controls the ability to re-identify it back to cleartext. With data movement enabled by Protegrity, organizations see global data compliance, improved efficiencies, and increased revenue.

Contact Protegrity today to learn how you can better protect your cross-border data.

Protegrity USA, Inc.
1.203.326.7200