protiviti®
Global Business Consulting

Mastering Data Dilemmas: Navigating Privacy, Localisation and Sovereignty

In today's digital age, data privacy management is paramount for businesses and individuals alike. With the ever-changing regulatory landscape surrounding data protection, organisations must adapt swiftly to ensure compliance and maintain trust with their customers and stakeholders. However, both data sovereignty and localisation play an important role in privacy, as discussed in a previous post "How data sovereignty and data localisation impact your privacy programs." With that in mind, businesses and individuals must also know why it is crucial to manage data privacy under a dynamic regulatory environment:

- **Upholding Individual Rights and Safeguarding Personal Integrity:** Adhering to data privacy regulations upholds the privacy rights of individuals and protects individuals' sensitive information, ensuring their personal integrity.
- **Legal Compliance:** Compliance with evolving data privacy laws and regulations, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and others, mitigates legal risks and potential penalties.
- **Building Trust and Reputation:** Implementing robust data privacy measures fosters trust in consumer digital interactions, enhancing the reputation of businesses and organisations and deepening customer relationships.
- **Safeguarding Personal Integrity:** Data privacy protects individuals' sensitive information, ensuring their personal integrity.
- **Staying Competitive:** Demonstrating commitment to data privacy sets businesses apart from competitors and attracts customers who prioritise their privacy.
- **Adapting to Changes:** With the regulatory landscape continually evolving, proactive management of data privacy enables organisations to adapt swiftly to new requirements, maintain compliance and meet evolving consumer expectations.

As such, prioritising the management of data privacy under changing regulatory conditions is not just a legal obligation but also a strategic imperative for businesses aiming to thrive in the digital ecosystem.

The impact of privacy regulations on the transmission of data

Data privacy regulations have significant implications for the transmission of data, affecting how organisations handle and transfer sensitive information. Here's how these regulations impact data transmission:

- **Encryption Requirements:** Many data privacy laws and regulations mandate the use of encryption and other privacy enhancing technologies (PETs) when transmitting sensitive or personal data over networks. Encryption ensures that data remains secure and unreadable to unauthorised parties during transmission.
- **Data Localisation:** Some regulations, like the GDPR in the European Union, require organisations to ensure that personal data is transmitted only to countries with adequate data protection standards. This may necessitate implementing mechanisms to verify the legal basis for data transfers and assessing the need for appropriate safeguards to ensure compliance with cross-border data transfer regulations. Localisation requirements can also force organisations to reconfigure their IT architecture and reevaluate the use of cloud-based solutions, potentially leading to less efficient operating environments.
- **Consent and Transparency:** Data privacy laws and regulations often require organisations to obtain explicit consent from individuals before transmitting their data and retain evidence of that consent. Additionally, organisations must be clear and transparent about how data will be transmitted, including the purpose of the transmission and any third parties involved.
- **Impact on Information Management:** Compliance with data privacy laws and regulations may require organisations to implement robust information management practices to track and audit data transmissions. This includes documenting data flows, maintaining records of consent, ensuring that data security measures are applied during transmission and applying clear retention periods.

Data privacy laws and regulations fundamentally influence how organisations transmit and access data, emphasising the importance of secure and compliant practices to protect individuals' privacy rights and maintain regulatory compliance.

The international regulatory landscape

A myriad of international laws and regulations restrict cross-border data transfers, and the landscape continues to change, with governments and consumers leading the way. The list below is illustrative and does not encompass all laws and regulations. It is intended to provide a view of regulatory activity across the globe.

Strict Transfer Requirements

- **European Union (EU):** The GDPR is a comprehensive data protection regulation that applies to all EU member states and companies that are also bound by EU extra territoriality provisions. It imposes strict rules on the processing of personal data collected from its data subjects, including requirements for data storage, security and transfer.

- **Brazil:** The General Data Protection Law (LGPD) is Brazil's data protection law. While it doesn't explicitly mandate data localisation, it imposes strict security and privacy requirements for the transfer of personal data outside its jurisdiction.
- **South Korea:** The Personal Information Protection Act (PIPA) in South Korea governs the processing of personal data. While there are no explicit requirements for data localisation, cross-border data transfers must have either consent with specific notice requirements or data protection adequacy with the receiving jurisdiction.
- **United States:** Executive order 14117 prevents or limits access to Americans' bulk sensitive data and US government data by countries or jurisdictions of concern, such as China, Hong Kong and Russia.

Localisation Required

- **Russia:** The Federal Law on Personal Data (PLPD) governs the processing of personal data in Russia. It imposes specific data protection obligations on organisations handling such data and requires personal data of its citizens to be stored within Russian databases.
- **China:** China's personal information protection framework imposes data localisation requirements, mandating that certain types of data collected by "critical information infrastructure operators" must be stored on servers within China and can be transferred only after passing a security assessment.
- **India:** India has sector specific regulations for data localisation. The Reserve Bank of India (RBI) has made it mandatory for all entities in the payment ecosystem to ensure that all data relating to payment systems are stored in local systems.
- **Australia:** Australia's My Health Records Act imposes restrictions on the processing and handling of health data within its territory.

Common Denominators Across Privacy Regulations

Despite the plethora of privacy regulations, there are similarities that can help ease the process of building a compliance framework. These common denominators span numerous privacy regulations and prove to be foundational elements for organisations developing comprehensive compliance strategies.

Here are the primary common denominators observed across various privacy regulations:

- **Data Protection Principles:** Most privacy regulations are based on common data protection principles, such as transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. These principles serve as the foundation for ensuring the lawful and fair processing of personal data.
- **Individual Rights:** Privacy laws and regulations aim to protect the rights of individuals concerning their personal data. These rights typically include the right to access, rectify and erase data, as well as restrict its processing, transfer it easily (data portability) and object to its processing.

- **Security Measures:** Ensuring the security of personal data is a fundamental aspect of privacy regulations. Organisations are required to implement appropriate technical, contractual and organisational measures to safeguard personal data from unauthorised access, disclosure, alteration or destruction.
- **Consent Requirements:** Many privacy laws and regulations mandate obtaining valid consent from individuals before processing their personal data. Consent must be freely given, specific, informed and unambiguous, empowering individuals to have control over their data. This is especially relevant for sensitive or personally identifiable data.
- **Accountability and Governance:** Privacy laws and regulations emphasise the importance of accountability by requiring organisations to demonstrate compliance through documentation, record-keeping, risk assessments and regular audits. Implementing effective governance structures is crucial for ensuring ongoing compliance and mitigating privacy risks.

Organisations can establish robust privacy programs by adhering to these common denominators that address the core principles and requirements across various privacy laws and regulations.

Adhering to privacy obligations through data discovery

Data privacy laws and regulations are increasingly stringent, requiring organisations to implement robust practices for managing data throughout its lifecycle. Two key areas of focus concerning data localisation and sovereignty are data mapping and assessing cross-border transfers.

- **Data Inventory and Data Mapping:** Data Inventory and data mapping involves identifying all the sources of data and categorising and documenting the flow of data within an organisation to gain a comprehensive understanding of the types of data collected, where it resides and how it moves across systems. By conducting thorough data inventory and data mapping exercises, organisations can comply with privacy laws and regulations by accurately identifying personal data and implementing appropriate measures to protect that data.
- **Assessing Cross-Border Transfers:** Identifying transfers of data across jurisdictions is crucial due to the varying requirements and restrictions regarding data protection. Organisations must assess the legal framework governing cross-border data transfers, implement appropriate safeguards such as standard contractual clauses or binding corporate rules, or align with inter-governmental agreements via adequacy determinations, and ensure that individuals are adequately informed about the transfer of their data. Regular reviews of data transfers help mitigate the risk of unauthorised disclosures and ensure adherence to regulatory requirements.

The importance of impact assessments

As organisations continue to be responsible for vast amounts of data, it becomes imperative to adhere to robust data assessment principles to ensure compliance and mitigate risks associated with cross-border data transfers, third-party vendors and contractual agreements.

- **Assessing Data Transfers for High Risk:** Data transfers, especially across borders, pose inherent risks to data privacy and security. Regulatory frameworks such as the GDPR require organisations to assess data transfers for high risk and implement appropriate safeguards to protect individuals' rights. This involves conducting thorough assessments of the data being transferred to identify potential risks and implementing measures such as encryption, anonymisation or obtaining explicit consent from individuals.
- **Assessing Risks by Third-Party Vendors:** Data privacy laws and regulations mandate that organisations assess the risks posed by third-party vendors and ensure that adequate controls are in place to mitigate these risks. This includes conducting due diligence on vendors' security practices and assessing their compliance with relevant laws and regulations. Organisations must monitor vendors' activities regularly to ensure ongoing compliance and mitigate emerging risks.
- **Assessing Third-Party Vendor Contracts:** Vendor contracts play a crucial role in governing the relationship between organisations and their service providers. These contracts should clearly define responsibilities and expectations with appropriate provisions for confidentiality, commitments to assist the organisation with related GDPR regulatory obligations, data security measures, data breach notification requirements, indemnification, compliance with applicable laws and regulations, and rights to perform audits to ensure that vendors meet their contractual obligations. By incorporating robust data protection clauses into vendor contracts, organisations can mitigate legal and financial risks associated with noncompliance.

Data transfer mechanisms explained

Data transfer mechanisms are methods to ensure the secure and compliant movement of data across borders. These mechanisms are important in maintaining data protection standards when personal data is transferred into jurisdictions with more stringent privacy laws. These include the following:

- **Execution of SCCs and BCRs:** In cases where data is transferred across borders or shared with third-party service providers, organisations may need to execute standard contractual clauses (SCCs) or binding corporate rules (BCRs) to ensure compliance with data protection laws and regulations. SCCs and BCRs establish the terms and conditions for data processing activities and outline the respective responsibilities of the parties concerned.
- **Data Privacy Framework:** The EU-U.S. Data Privacy Framework (DPF), developed by the U.S. Department of Commerce, the European Commission, the United Kingdom and the Swiss federal administration enables the transfers of personal data. Organisations that have

self-certified and comply with the DPF Principles (notice; choice; accountability for onward transfer; security; data integrity and purpose limitation; access; and recourse, enforcement and liability) are deemed adequate without the need for SCCs or BCRs. The DPF subjects participating organisations to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

It is crucial for organisations that deal with cross-border transfers of personal data to understand these mechanisms and use them appropriately based on their specific circumstances and legal obligations under applicable privacy laws and regulations. Regular reviews and updates should be conducted in line with changes to laws or guidance from relevant authorities.

Final thoughts on building data privacy frameworks

Implementing a robust framework is vital for addressing privacy concerns and combating cyber threats. However, the business units responsible for managing risks associated with privacy, data governance and cybersecurity often prioritise their own activities, resulting in inconsistent practices that lead to gaps in customer data protection efforts.

To manage the risks of customer data loss effectively, it is crucial to adopt a collaborative approach that encompasses privacy, data governance, cybersecurity and consumer trust. This approach should consider the distinct challenges and priorities of each function.

Privacy

Given the rapid expansions in privacy regulations, organisations are placing more emphasis on data privacy to ensure compliance and build consumer trust. Privacy risk poses a unique challenge due to the volume and nature of data that organisations collect and retain. The changing regulatory environment and advancements in business and technology further complicate this risk.

A robust privacy framework is essential in managing a data subject's personal data, which may include any information relating to an identified or identifiable natural person. Examples of that information can consist of any identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person and other forms of protected information regulated by different bodies and jurisdictions.

Therefore, it is important for discussions to take place among the company's cyber, privacy, legal and data management professionals, as well as executive management and the board of directors, regarding data governance and cybersecurity matters as regulatory scrutiny, the risk of data exposure or leakage, and consumer demands for privacy protections continue to escalate.

Data Governance

Data governance is a crucial and ongoing effort that needs to be integrated into every aspect of a business. It encompasses the policies, processes and systems that ensure that data is readily available, consistent, defined, accurate and of high quality. In recent years, organisations have recognised the importance of enhancing data availability to improve offerings, reduce costs and develop new business models. When effectively managed, data can provide valuable insights and aid in decision-making.

One effective method to foster collaboration between functions responsible for managing risks associated with customer data loss is to establish a working group consisting of representatives from cyber security, privacy, legal, data governance and risk management.

Cybersecurity

Protiviti's recent Top Risks Survey reveals that data privacy and cybersecurity are among the top risks impacting organisations today and in the future. Cybersecurity attacks remain a highly relevant and ongoing challenge, with a focus on protecting valuable information and systems, understanding the evolving threat landscape, and developing effective incident-response plans. The cyber function must align with privacy and data governance functions to manage priorities and protect customer data collaboratively.

For additional information, examples and insights, visit Protiviti's Data Privacy web page. Protiviti is not a law firm, and nothing within this paper should be relied on for legal purposes. Clients should always seek legal advice from inside or outside counsel.

Contacts

Sameer Ansari
Managing Director
sameer.ansari@protiviti.com

Joel Wuesthoff
Managing Director
joel.wuesthoff@protiviti.com

Arnold Park
Senior Manager
arnold.park@protiviti.com

Joseph Emerson
Managing Director
joseph.emerson@protiviti.com

Nicholas You
Associate Director
nicholas.you@protiviti.com

Hanneke Catts
Director
hanneke.catts@protiviti.com.au

Philip Greaves
Managing Director
philip.greaves@protiviti.co.uk

Michael Pang
Managing Director
michael.pang@protiviti.com

Kai-Uwe Ruhse
Managing Director
kai-uwe.ruhse@protiviti.de

Tjakko de Boer
Managing Director
tjakko.deboer@protiviti.nl

Enrico Ferretti
Managing Director
enrico.ferretti@protiviti.it

Tom Moore
Senior Managing Director
tom.moore@protiviti.com