DATA PROTECTION FRAMEWORK

**What is DATA PROTECTION?**

Data protection is about safeguarding our fundamental right to privacy, which is enshrined in international and regional laws and conventions.

**Introduction/ Context**

The world has progressed from the Industrial Revolution, which came about with the advent of rapid industrialisation, to the age of the Information Revolution, which is distinguished by an economy based on information, computerisation and digitalisation.

However, increasing globalisation and digitalisation have brought a lot of challenges. There has been an alarming rise in cybercrimes on a global scale. With India also moving towards a digital economy with the adoption of Aadhaar and an ever-increasing dependency on information, the concerns over cyber security, data protection and privacy are justified. Further, in the wake of the Supreme Court ruling that privacy is a fundamental right, there is a growing sense of urgency in India to have in place a proper legislative framework to address the concerns over cyber security, data protection and privacy.

The data protection framework must be built on the following principles:

- **Technology agnosticism**: The law must be technology agnostic. It must be flexible enough to take into account changing technologies and standards of compliance.
Holistic application: The law must apply to both private sector entities and the government.

Informed consent: Consent is an expression of human autonomy. For such expression to be genuine, it must be informed and meaningful.

Data minimisation: Data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject.

Controller accountability: The data controller shall be held accountable for any processing of data, whether by itself or by entities with whom it may have shared the data for processing.

Structured enforcement: Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity.

Deterrent penalties: Penalties on wrongful processing of data must be adequate to ensure deterrence.

The framework (data protection framework) defines personal data as follows:

‘Data from which an individual is identified or identifiable/reasonably identifiable may be considered to be personal data. The identifiability can be direct or indirect.’
speculates that data in this context ought to include any kind of information, including opinions or assessments, irrespective of their accuracy.

Accountability in data protection.

To translate data protection norms into action, a widely used method is to identify the party accountable for compliance with these norms. For this purpose, the concept of control over data is used. In such systems, control over data refers to the competence to take decisions about the contents and use of data.

An organisation that collects and processes personal data for its business transactions can fall under two broad categories—data controller and data processor. The framework recognises the concept of a ‘data controller’ to ensure accountability. However, the need to define ‘data processors’, ‘third parties’ or ‘recipients’ is currently under discussion in order to define the level of detail with which the law must allocate responsibility.

Globalisation vs localisation

Under data localisation, entities are required to store and process personal data on servers physically present within their national boundaries. Although this approach helps address concerns over data privacy, security, surveillance and law enforcement, it increases the burden on businesses by way of increased cost of compliance, and may also impact the building blocks of the economy, which rely on data exchange.

Conclusion

Given the proposed regulations in the white paper on ensuring the data privacy of individuals, it is very important that organizations start aligning their processes and IT investments in such a way that the regulation, once enacted, does not affect them. Although the paper does not clearly outline anything on past processing activities or retrospective action, CIOs/CISOs are advised to see how capable their existing IT infrastructure is and what it requires to handle the changing data privacy landscape in India.
Introduction

The bill is in line with most of the leading global privacy laws and regulations that are currently prevalent, such as the GDPR and Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA). It touches upon almost all the domains of data privacy such as collection limitation, fair and lawful processing, notices/consents, data subject rights, privacy by design, security safeguards, transfer of personal data, penalties, data quality, privacy incidents or breaches and children’s privacy. The bill has also identified the supporting regulatory and administrative framework for enabling the enforcement of its roll-out.

The proposed bill is fairly comprehensive in terms of addressing the key facets of privacy:-

- **Anonymisation**: The proposed bill explicitly states that it will not apply to the processing of anonymised data. However, organisations are required to apply the
standards specified by the Data Protection Authority (DPA) for anonymisation. The exclusion of anonymised data will considerably bring down the obligations on entities (both in the private and public sector). In order to prevent harm to specific groups of individuals, the limitation of processing and publishing analysis of anonymised data should be evolved.

- **Data localisation:** The draft bill also proposes that data fiduciaries save a local copy of all personal data that is stored outside the boundaries of India. Although this move could have some negative consequences, as discussed here, it would ensure effective enforcement of the law, reduce bottlenecks in dealing with foreign jurisdictions, and protect national security and interests. Further, in a move focused on protecting national interests and containing the risk of surveillance from foreign states on critical data, the draft bill prevents data fiduciaries from sending ‘critical’ personal data outside the territory of India.

- **Data processor:** The draft bill calls out the data protection obligations, with fair and reasonable processing considered as the core principle. The data fiduciary/entity is identified as the party responsible for compliance with the Personal Data Protection Act, 2018, and bears the onus of ensuring that data processors fulfil their contractual obligations. However, with no direct regulatory obligation on the data processor, the level of expected compliance will only be as strong as the contract.

### The right to privacy

The right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of information privacy. The power of exercising this right should rest with the individual. The aim is also to protect the privacy of individuals by allowing them determine how their personal data is collected, shared with or used by any entity, public or private.

The bill enforces the right to confirmation and access, right to correction of inaccurate personal data, completion of incomplete personal data, update of out-of-date personal data, right to data portability, right to be forgotten and the right to withdrawal of consent for data subjects.

### Data breaches

The bill proposes a layered approach for levying penalties for non-compliance on organisations. In order to avoid significant business ramifications due to data breaches, organisations need to outline a well-defined testing mechanism to assess readiness to address any eventualities. Further, they must nominate a competent person, preferably a
Chief Data Officer, to communicate with the Data Protection Authority (DPA). The bill proposes a penalty of up to 5 crore INR or 2% of an organisation’s total worldwide turnover for the preceding financial year, whichever is higher, in case the organisation fails to meet its obligation to take prompt and appropriate action in response to a data security breach.

**Data Protection Impact Assessment (DPIA)**

The proposed bill makes it mandatory for organisations, especially SFDs, to conduct a DPIA for processing activities that may carry a risk of significant harm to data principals. Additionally, SFDs are required to submit their DPIA to the authority, who may either require the organisation to cease processing or implement additional measures. The requirement provides an effective tool for organisations to ensure business interests involved in processing activities are aligned with the privacy interests of data principals.

**Conclusion**

With India going digital and the potential that this move unleashes, the Personal Data Protection Bill is the need of the hour. This is in line with the global trend of increased focus on protecting the rights of citizens with respect to their data. India is moving towards developing a strong regulatory framework to address the challenges of the digital age.

There is traction in various data-intensive sectors such as banking, healthcare and telecom, where the Supreme Court and the respective regulatory authorities (namely the RBI, Ministry of Health and TRAI) are taking a strong stance when it comes to ownership and control of data belonging to individuals. What this essentially means is that organisations need to shift gears in the way they collect, process, store and share personal data. Having said that, business should see privacy regulation as an opportunity to align themselves for future success and strategic risk management, and not merely to ensure compliance.
Introduction

India is the fastest growing trillion-dollar economy in the world. The long-term growth prospects of the Indian economy are largely due to its young population, technological progress, and increasing urbanisation. The country is in the midst of a massive wave of urbanisation as millions of people move into towns and cities each year. Enormous investments are being made to meet soaring aspirations and to make towns and cities more liveable.

Smart cities

The smart cities leverage technology and utilise existing and planned infrastructure investments to provide a higher quality of living to residents. Smart cities are powered by advanced technologies such as the Internet of things (IoT) and sensors along with the traditional information technology (IT) and operational technology (OT) systems and devices. These advanced and traditional technologies, distributed across the smart city, work in an integrated manner to generate intelligent and actionable information to help in providing services to residents in an efficient and sustainable manner.

Characteristics

- **Intelligent traffic management system (ITMS):** The ITMS includes automating the process of traffic management by optimally configuring traffic junction signals on real-time basis.
- **E-governance:** E-governance is the use of information and communication technology (ICT) to provide public services to citizens, by re-engineering internal business processes and increasing the transparency and accountability of government schemes.
Closed circuit TV (CCTV) surveillance: The city surveillance system comprises video and audio surveillance that converge onto possible crime vectors and their prevention.

Smart water management: The smart water management system gathers meaningful and actionable data about the flow, pressure and distribution of a city’s water and streamlines the processes.

Automatic fare collection system: This system includes an automatic gate machine, ticket vending machine and ticket checking, along with analysis of passenger flow.

Enterprise GIS application: It is an integrated cross-sectoral platform to collect, manage, compile, analyse and visualise spatio-temporal information for sustainable urban planning, development and management.

India’s efforts to protect its smart cities

Ministry of Housing and Urban Affairs (MoHUA) Guidelines:
MoHUA, the Government of India, released a model framework for cyber security in smart cities on 20 May, 2016. It covers the security of smart cities across different layers, namely sensor layer, communication layer, data layer and application layer. The major guidelines include

- Designing a secure network architecture based on the National Institute of Standards & Technology (NIST) reference IT architecture.
- Security solutions that needs to be considered while developing a smart city.
Secure storage and transmission of data between different systems and devices implemented in the smart city.

- **The National Critical Information Infrastructure Protection Centre (NCIIPC), 2014:**
  NCIIPC has been identified as the nodal agency under the National Technical Research Organisation for the protection of critical information infrastructure. The formal roles and responsibilities of the NCIIPC include cooperation strategies, issuing guidelines, advisories and coordination with CERT-In. The NCIIPC has defined controls for the critical infrastructure sectors to enhance security.

- **National Cyber Security Policy, 2013:**
  The policy aims to create a secure cyber ecosystem in the country and strengthen the regulatory framework.

- **Aadhaar Act, 2016, and its regulations:**
  The Aadhaar Act, 2016, defines how Aadhaar-related data is to be captured, stored and processed. Aadhaar data includes not only biometric information (fingerprints, iris and photo) but also the demographic details of the resident. The Aadhaar Act, 2016, forms the basis of various e-governance initiatives such as distribution of services and benefits to residents of India.

- **Draft Personal Data Protection Bill:**
  The Personal Data Protection Bill includes provisions to protect personal data as an essential facet of information privacy. The bill provides guidelines on the data processing grounds, rights of the data principal, penalties and exemptions, amongst other areas. The bill aims to protect the autonomy of individuals from data privacy violations by the state and private entities. Once enforced, the bill will impact how the smart city information systems store and process personal/sensitive data.

**Conclusion**

*The Smart Cities Mission* is expected to drive economic growth and improve the quality of life of people by enabling local development and harnessing technology to create smart outcomes for citizens. Though the beginning has been excellent, the Smart Cities Mission is still very much a work in progress. There are various economic, technical, and managerial challenges to overcome in mission implementation. One of the most prominent challenges is definitely the cyber security of the smart cities. Considering the ever-expanding risk landscape, India’s developing smart cities could be the target for various adversarial interests.
The smart cities leverage technology and utilise existing and planned infrastructure investments to provide a higher quality of living to residents. Smart cities are powered by advanced technologies such as the Internet of things (IoT) and sensors along with the traditional information technology (IT) and operational technology (OT) systems and devices. These advanced and traditional technologies, distributed across the smart city, work in an integrated manner to generate intelligent and actionable information to help in providing services to residents in an efficient and sustainable manner.

**Security risk landscape for Indian smart cities**

The Indian Smart City technology architecture can be understood through the four logical layers: sensor, communication, data and application layers. The technology across these four layers works in an integrated manner to deliver Smart City services.
Challenges specific to the Indian context weaken the efforts towards cyber security implementation in smart cities. The major challenges have been 1

✓ Cyber security not figuring amongst top priorities.
✓ Limited stakeholder awareness on cyber security.

While security should be a prerequisite, in the Indian context, it is often an afterthought. As cities throw their weight behind timelines to implement services, security takes a backseat.

Challenges in creating cyber secure smart cities

✓ Security governance:
  There is no security organisation responsible for ensuring cyber security within smart cities. Additionally, there is no or limited consideration of cyber security during the various phases of smart city development.

✓ Budget Allocation:
  Limited budget is allocated for cyber security in the overall smart city budget. Even when a budget is allocated, it does not match the risk profile of smart cities, thereby making the process of setting up adequate defences a difficult proposition.

✓ Cyber security capability and awareness:
  Smart city stakeholders have low awareness of cyber security risks and vulnerabilities. Further, the stakeholders responsible for securing the smart cities, have limited cyber security capabilities.

✓ Security products selection and implementation:
  Business-driven risk assessments are not conducted to identify appropriate security products based on the risk profile of the smart city. Additionally, there are no baseline security guidelines for implementation and configuration of security products.

✓ Review and monitoring mechanism:
  There is no mechanism in place to regularly perform security assessments of the smart city set-up in order to identify and mitigate security risks on a continual basis.

Way forward

✓ Appoint a security organisation led by CISO to ensure cyber security in the smart city. Perform a business-driven risk assessment to appropriately consider cyber security requirements.
ACHIEVERS IAS ACADEMY

- Design a security and privacy framework including policy, procedures and minimum baseline security guidelines covering systems, network devices, and edge devices including IoT, sensors, etc.
- Establish a governance mechanism to periodically review and enhance cyber security for the smart city.
- Plan for cyber security awareness and capacity building within the smart city.
- Maintain contact with various security agencies such as CERT-In and NCIPC and other security experts for cyber threat advisory and incident reporting.
- Conduct security operations in line with the security procedures—change management, incident management, etc.
- Design, implement and operate a security operations centre (SOC) with advanced analytical capabilities and integrate with all the systems and edge devices, wherever possible.
- Operate the SOC on a 24x7 basis to detect, identify and respond to security incidents.
- Enforce a comprehensive patch management process including regular and timely updates of all firmware and operating systems.

**Conclusion**

Today, there are more people living in cities than in the countryside. Vehicles and energy consumption in cities are skyrocketing. The domestic and international mobility of citizens is significantly improved and tourists are travelling extensively from one city to another. Under such circumstances, many metropolitan cities are dealing with challenges such as overpopulation, waste management, massive energy consumption and pollution as a result of dramatic increase of migrants and travellers.

Traditional access control systems, therefore, can no longer effectively deal with such multidimensional challenges, traffic jams and long queue waiting times should not be accepted as the norm. Cities have to innovate themselves with better and smarter access control systems to track and manage their populations, vehicles, buildings and touristic sites.
CROSS BORDER DATA FLOW

Introduction

Most governments recognize that innovations powered by cloud computing offer huge potential benefits connecting their countries to the global digital economy. Governments also understand that cloud computing, applications and data processing require that data has free flowing movement across international borders. However, some governments are considering imposing data localization policies and restrictions which could significantly impact the growth of the digital economy.

The Importance of Cross Border Data Flow

The flow of data across borders now drives global economic growth more than the flow of goods. If all businesses, small, medium or large, can access inexpensive storage, then any company can compete on a global stage. If one company is forced to store data locally as opposed to a competitor in a neighbouring country, their costs will be higher and this will affect how they compete in today's global marketplace.

Requiring companies to store data in their own country hurts micro, small and medium sized enterprises (MSMEs) the most as it prevents them from leveraging lower cost global cloud platforms that are available today. In addition, larger companies are more likely to have the funds to build datacentres whereas smaller firms can be shut out of the domestic and international digital marketplace completely if they cannot access affordable computing and data services. Data localization also hurts consumers resulting in less choice of services and increased prices, making local companies less competitive because local storage increases costs and complexity of doing business.

Challenges

- Some governments currently promote data localization as a method of keeping their data more secure and within their own borders. Data localization policies aimed at keeping data within a nation’s borders have a negative impact on both the privacy and security of data and it is argued that storing information in one physical location could actually increase vulnerability. In fact, local storage in a
single place can create an attractive target for cybercriminals and incremental surveillance.

- **Localized datacentres are also more vulnerable to natural disasters** that may strike in a country.
- **Any economic gains that were realized by data localization policies were not significant enough to offset the losses in the general welfare and output** in the economy.

**Scope of data flow**

Access to cloud computing creates opportunities for businesses of all sizes to drive innovation and efficiency in their operations. In a recently published article in the Harvard Business Review, Michael Porter and James Heppelmann argue that data-fuelled technologies have the potential to drive a sharp increase in innovation, productivity gains, and economic growth. The McKinsey Global Institute estimates that the international flow of data contributed US$2.8 trillion to the global economy in 2014 and is expected to contribute up to US$11 trillion in 2025.

**Way forward / Policy recommendations**

- **Promote an Open Internet**: An open internet is essential for recognizing the Internet’s true potential as it boosts international trade, supports internet-enabled innovation and increases productivity and growth.
Establish Trade Rules that protect cross border data flows: When developing multinational trade agreements such as the Regional Comprehensive Economic Partnership (RCEP), one should provide opportunities to make requirements for cross border data flow and restrict forced localization of computing facilities while also permitting exceptions to the extent necessary to protect the privacy of personal data and achieve other legitimate policy goals.

Permit Data Flows in Domestic Legislation: Today, many if not most companies utilize a variety cloud services which involves the flow of data across borders. Governments should avoid making policies that prohibit such transfers or that require the data to remain within borders (data localization). Such policies will have a negative economic impact on MSMEs and limit their participation in the global digital economy.

Establish Compatible Rules: The cost of compliance can be significant and can eradicate any profit a small to medium size business can make. Governments are therefore encouraged to establish compatible rules through trade agreements to reduce the compliance burden.

Promote E-Commerce: E-commerce has enormous potential, even more so in emerging markets, to increase GDP, create jobs and promote growth. Governments should do all they can to encourage and promote the use of ecommerce to allow MSMEs to access the global market. Customs procedures should also be simplified where possible and customs duties or other taxes on cross border trade carefully considered, especially on low value shipments which typically are sold by MSMEs.

Conclusion

Data localization policies can stunt economic growth that is taking place in an increasingly digital world. These policies usually tend to hurt the MSMEs the most by restricting access to the global digital economy. While security, data and privacy concerns are normally cited when developing such policies, it has been argued that such localization policies actually do not improve security, data and privacy standards.
Previous Year Questions


2. Religious indoctrination via social media has resulted in Indian youth joining the ISIS. What is ISIS and its mission? How can ISIS be dangerous to the internal security of our country?

3. India’s Traditional Knowledge Digital Library (TKDL) which has a database containing formatted information on more than 2 million medicinal formulations is proving a powerful weapon in country’s fight against erroneous patents. Discuss the pro and cons of making the database available publicly available under open source licensing.

4. Discuss the advantage and security implication of cloud hosting of servers vis-a-vis in house machine based hosting for government business.

5. Use of Internet and social media by non-state actors for subversive activities is a major concern. How these have misused in the recent past? Suggest effective guidelines to curb the above threat.

6. Discuss the potential threats of Cyber-attack and the security framework to prevent it.