Achieving Compliance with India’s Personal Data Protection Bill
Since GDPR came into force in 2018 across EMEA, many countries around the world have followed suit and have either revamped or introduced new data protection and privacy regulation. India, too, is taking steps to enact a data protection framework which incorporates many elements of the GDPR. The new law, the Personal Data Protection Bill (PDP), is currently in front of parliament and was proposed in 2019 to bring about a comprehensive overhaul to India’s current data protection regime, which today is governed by the Information Technology Act, 2000.

Unfortunately, India is no different from other countries when it comes to cyber threats, and cybercriminals are carefully discovering new ways to obtain sensitive personal and business data. This is coupled with the fact that the pandemic has accelerated digital transformation and catapulted the ecosystem forward five years in a matter of months and remote working and the distributed workforce has created an expanded attack surface.

In this guide, we examine the evolving risk and data privacy landscape, particularly in light of changes in working patterns brought about by COVID-19. We lay out key steps to help organizations in India sensibly adopt a better data protection posture and with it, build a firm foundation towards onward compliance. This involves taking a layered approach to security with people, process and technology interwoven together. We outline why data classification is a robust start point and how organizations can go about detecting and preventing leaks, as well as securing and protecting sensitive data that is shared both inside and outside the organization with solutions such as Adaptive Data Loss Prevention (DLP), encryption and secure managed file transfer.

We summarize by explaining that organizations in India should not view data protection and compliance as an expense, but as a positive competitive differentiator and one that, over the long term, will prove to deliver efficiencies and benefits back to the business.
Introduction

Not long ago, organizations operated closed systems, with data processing only carried out on the inside, and the ability to communicate directly with the outside world was limited to email and telephone. The data protection laws in place were benign, with only repeat or very serious offenders receiving a fine. The rapid acceleration of digital data generation, combined with the dissolution of the corporate perimeter and creation of vast corporate ecosystems, suddenly created countless opportunities for personal data to go astray through theft or accident.

Additionally, COVID-19 introduced home working on a scale that we’ve never experienced before. This has created new opportunities which cybercriminals are now exploiting, and new threats are emerging – both inside and external to the organization.

India is no different from other countries and has certainly seen an increasing level of threat as cybercriminals have taken advantage of the speed that organizations are digitizing their businesses and the expanded threat surface that a distributed workforce creates.

Today, India is a vibrant economic powerhouse, an attractive country for outsourcing and it has many well-educated technology workers which attracts US technology vendors and global call centers to the country. Likewise, it has a huge domestic economy and a thriving financial services sector.

Already familiar with, and adhering to, regulations such as GDPR and CCPA when servicing overseas customers in the US and Europe, India is now starting to look seriously at privacy and data protection frameworks and ensuring that such frameworks are enforced, not just because it enables the nation to trade with overseas customers but because it is good business practice to protect data and have the customers’ best interests at heart.

However, today India doesn't have any dedicated laws on cybersecurity, so the detailed nuances around legal cybersecurity frameworks are currently missing. The only provision is the Indian Cyber Law in the Information Technology Act, 2000 which has a given definition of the term “cybersecurity” - however, many say that this merely pays lip service to legal cybersecurity frameworks.

The data protection landscape and its associated compliance environment changed fundamentally with the implementation of the European-wide GDPR in May 2018, with many other privacy regulations following suit around the globe. This has made data privacy a boardroom issue and today many boards understand their responsibility around this area.
Breaches are driving regulatory change across India

Serious data breaches and incidents of cyber-intrusion have a powerful effect on driving regulatory focus and change. To date India has experienced its fair share of incidents, from the well-publicized international Facebook hack, whereby more than 500 million Facebook users were found available on a website for hackers including those of Indian consumers, to a massive database breach that occurred in MobiKwik servers, whereby Indian card holder data was leaked and hundreds of thousands of its users’ details surfaced on the dark web.

Likewise Indian telecommunications company, Tata Communications, suffered a data breach and the cybercriminals claimed they had sold access to Tata’s servers to hackers. Another example is BigBasket, the popular Indian online grocery vendor, which faced a data breach that affected the data of over 20 million customers. Personal information such as email, IDs, full names, and IP addresses were compromised and offered for sale on the dark web.

In fact, according to India publication, THE WEEK, India saw a 37% increase in cyber-attacks in the first quarter of 2020 compared to 2019. India has also been featuring in the top countries that have been falling prey to data breaches over the years with no substantial action being taken to effect major change. Additionally, Indian companies allowing employees to work from home have not sufficiently prepared them to deal with protecting themselves from unauthorized access or usage. These companies have become an easy target for cybercriminals, causing cybersecurity breaches to massively increase.

So, as you can see, data breaches in India are happening frequently, but often these are not reported, which can lead to a sense of complacency. However, organizations who don’t act and act fast, could face the huge financial and reputational damages that a breach can cause and the longtail ramifications such as a loss in customer trust. It is therefore timely that the India Personal Data Protection Bill is being introduced, which will supersede the Information Technology Act, 2000 and this Bill is currently being ratified by Parliament.
What does the India Personal Data Protection Bill (PDP) include?

The India Personal Data Protection (PDP) Bill includes requirements for notice and prior consent for the use of individual data, limitations on the purposes for which data can be processed by companies, and restrictions to ensure that only data necessary for providing a service to the individual in question is collected. In addition, it includes data localization requirements and the appointment of data protection officers within organizations.

India has not yet enacted this specific legislation on data protection. However, the Indian legislature did amend the Information Technology Act (2000) to include Section 43A and Section 72A, which give a right to compensation for improper disclosure of personal information.

The Indian central government subsequently issued the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules under Section 43A of the IT Act. The Rules have imposed additional requirements on commercial and business entities in India relating to the collection and disclosure of sensitive personal data or information which have some similarities with the GDPR and the Data Protection Directive.

Companies in regulated sectors such as financial services and telecoms are subject to obligations of confidentiality under sectoral laws which require them to keep customer personal information confidential and use them for prescribed purposes, or only in the manner agreed with the customer.

The government of India and a joint Parliamentary Committee has proposed the draft PDP Bill on data protection which will be India’s first law on the protection of personal data and will repeal 43A of the IT Act. However, even after enactment, the law is likely to be implemented in a phased manner. Currently, there is no information about that implementation timeline.

Additionally, India does not have a national regulatory authority for protection of personal data. The Ministry of Electronics and Information Technology is responsible for administering the IT Act and issuing the rules and other clarifications under the IT Act. The PDP Bill proposes creating a Data Protection Authority of India that will be responsible for protecting the interests of data principals, preventing misuse of personal data, and ensuring compliance with the new law.

The PDP Bill proposes the concepts of a ‘data fiduciary’ and a ‘data processor’. A ‘data fiduciary’ and a ‘data processor’ are equivalent to the concept of controller and processor under the GDPR. The PDP Bill will not only apply to persons in India but also to persons outside India in relation to business conducted in India, the offering of goods or services to individuals in India, or the profiling of individuals in India.
The internal threat environment: Insider data breaches are catching organizations out

It is worth noting that not all breaches are a result of external malicious activity; one area that is still causing considerable concern from a compliance perspective is the threat of an insider data breach. In fact, according to a recent Forrester report by analyst Heidi Shey entitled: “The State of Data Security and Privacy, 2020”, among breaches in the past 12 months, 46% involved insiders like employees and third-party partners - the majority of which were simple errors.

This is consistent with what Forrester witnessed in 2018: “News headlines of insiders stealing trade secrets from companies like Hershey, Philips, and Tesla lead us to assume that insider threats are based on malicious intent, but the reality is that inadvertent misuse of data and lost devices cause a concerning proportion of incidents and breaches. From a compliance perspective, insider breaches are perhaps even more damaging, as organizations have more control here than with external threats.”

Personally Identifiable Information (PII) remains the top type of data that global security decision makers most often say has been compromised or breached. IP is also high on the list along with sensitive corporate data.
What approach should Indian organizations take to achieve robust compliance?

Today every investment an organization makes in cybersecurity and privacy technology has to be about protecting data, with the goal of improving security performance and boosting its ability to demonstrate a compliance position in this increasingly regulated environment.

In its report, Forrester defines data security and privacy technology as technologies that directly touch the data itself and that help organizations:

1) understand where their data is located and identify what data is sensitive;  
2) control data movement as well as introduce data-centric controls that protect the data no matter where it is; and,  
3) enable least-privilege access and use.

The report went on to highlight that among global security decision makers, 49% indicated that they had invested in privacy management software to comply with data protection regulations. They reported investing in data discovery and classification (45%) and other data security controls (44%) to help fulfil their compliance obligations. This highlights that, while some businesses recognize that technology investment is critical to meeting regulatory requirements, more than half of those surveyed haven't invested in privacy management technology, which is concerning and demonstrates a level of apathy or uncertainty over the most effective approach to take.

India's national airline Air India announced a cyber-attack on its data processor’s data servers has affected about 4.5 million customers around the world.

The breach involved personal data registered between August 2011 and February 2021. Details including name, date of birth, contact information, passport and ticket information as well as credit-card data were compromised.

In a statement Air India said: “The protection of our customers’ personal data is of highest importance to us and we deeply regret the inconvenience caused and appreciate the continued support and trust of our passengers.”
Layering your data security solutions

Organizations must therefore implement the appropriate measures to prevent unauthorized access to sensitive, and confidential information, and to prevent malicious cyber-attacks, accidental loss, or the deletion of any confidential data. This involves putting in place a robust data security strategy that centers on people, process, and technology. Organizations need to ensure that employees are trained and understand the importance of securing sensitive and confidential information. Therefore, security should be embedded into the culture of the business and processes put in place to support this. This also involves implementing the right technology to guard against both the malicious and accidental loss of data. Here data security is only as robust as the various elements that support it, therefore, layering proven solutions to ensure your sensitive and confidential data remains secure from start to finish should begin with the following steps:

1. Understanding and classifying your data
   The basis of a solid data security strategy begins by identifying and classifying what type of information you have and need to protect, including critical unstructured data such as intellectual property. By taking this step, you lock down the base control and management parameters needed to help ensure compliance. Whether you need to protect public, financial, personally identifiable information (PII) information, or more, establishing and classifying data to be protected sets the foundation for the additional security layers needed to continue protecting data along its journey.

2. Detecting and preventing data leaks
   Inevitably, an employee will accidentally send sensitive data to the wrong person, or perhaps transfer an otherwise “safe” document that contains hidden metadata that could compromise your compliance or privacy standards. Any number of scenarios can put a barrier to your organization at risk unless you have a solution in place to detect and sanitize data in real time, before it is sent to the cloud or to third parties, before a breach occurs.

   Therefore, organizations need to ensure that documents uploaded and downloaded from the web are thoroughly analyzed, even if they are coming from a trusted source. To do this effectively, they need a solution that can remove risks from email, web, and endpoints, yet still allows the transfer of information to occur. Adaptive DLP allows the flow of information to continue while removing threats, protecting critical data, and ensuring compliance. It doesn’t become a barrier to business or impose a heavy management burden. This is important because traditional DLP ‘stop and block’ approaches have often resulted in too many delays to legitimate business communications and high management overheads associated with false positives.

3. Securing and protecting your data
   After the organization has ensured that data is identified and classified, scrubbed of potentially sensitive data, and approved for sending by authorized users, that data now needs to be protected as it is sent or transferred for true end-to-end data security. This can be achieved by email encryption or, where there are large volumes of data sent on a regular basis, through a managed file transfer (MFT) solution. MFT locks down your data at the point it is most vulnerable – when it is being used by others and while traveling to its destination into unmanaged domains, devices, or applications. This secure channel provides a central platform for information exchanges and offers audit trails, user access controls, and other file transfer protections.
Privacy will reign as the top compliance regime

The Indian PDP Bill and numerous other regulatory regimes will continue to be developed and privacy will reign moving forward.

While compliance with data protection regulations is non-negotiable and the penalties for failure are severe, it is a mistake to see compliance solely as an inevitable burden. With a comprehensive and proactive approach, that involves a combination of people, process and technology, organizations can pivot from viewing compliance as an expense and turn it into a positive competitive differentiator and one that, over the long term, will prove to deliver business benefits.

Here are a few pointers to keep top of mind when looking at your data security and compliance strategy:

• There should be a combined approach to IT security and operations when it comes to business data, one that involves people, process and technology and is embedded into the company culture.

• Therefore, CISOs should identify and engage stakeholders right across the business, including risk, legal, and compliance. This is critical to the success of your compliance program.

• Organizations must educate users about the sensitivity of data and ensure the appropriate controls are in place around confidential and sensitive information.

• Ongoing education programs should be embarked upon and security should be embedded into the culture of the company so that these programs are not viewed as a one-off.

• Users should be alerted when data is leaving the organization to warn them before sending messages that contain sensitive information.

• Look to classify data as a foundational step and enforce security controls to stop unauthorized distribution of data.

• Layer data security tools so that data is protected throughout its lifecycle. Security software tools should work together to enhance overall data protection.

• Provide critical audit information to enable remediation activity and demonstrate the organization’s compliance position to the regulatory authorities.

• Have a plan for if or when things go wrong so that employees can act quickly and decisively.
SUMMARY

Ultimately, in today’s highly regulated data environment, organizations in India need to embrace and build an effective compliance strategy, as those that do will experience positive business benefits and undoubtedly reap the rewards. Those with low levels of data privacy protection and data governance software adoption need to change – and change quickly. But, more broadly, companies need to obtain better visibility of their data before they can consider themselves compliant with relevant data protection regulations. By taking a layered approach to data security and adopting a people, process and technology centric approach, organizations in India can confidently embrace the new PDP Bill and, once compliant, should view this as a competitive advantage.

Recommended Links

international/facebook-data-on-more-than-500-million-accounts-found-online/available-data/slideshow/81896603.cms


More about HelpSystems Data Security

Our comprehensive data security suite includes:

**Data Classification**
- Identify, label, and control your sensitive or valuable data
- Helps determine data value and build a security-focused culture

**Managed File Transfer (MFT)**
- MFT provides a secure and compliant way to share data outside the organization
- Automate workflows and integrate with third-party applications
- Large file acceleration helps move data quickly and securely

**Integrated Data Loss Prevention (DLP)**
- Minimize the risk of a data breach by automatically removing sensitive data from emails and documents as they are sent, received, or transferred to the cloud
- The solution applies an additional layer of sanitization to protect from phishing emails, ransomware, and other Advanced Persistent Threats

**Digital Rights Management**
- Security that stays with your data wherever it travels
- Track, audit, and revoke access at any time

For more information, visit: [https://www.helpsystems.com/solutions/cybersecurity/data-security](https://www.helpsystems.com/solutions/cybersecurity/data-security)
About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.