rainmaker
creating ethical workplaces

The Rainmaker Manual:
A Toolkit for Indian Companies

Navigating Data Protection and Privacy Compliance

TABLE OF CONTENT S

Disclaimer: The views expressed in this handbook are those of the authors and do not necessarily reflect the views and policies of Rainmaker Online Training Solutions Private Limited.

ABOUT THE ORGANIZATION

Rainmaker is a leading provider of ethics and compliance training programs for corporates in India. Our focus is on delivering engaging and interactive training solutions that help create ethical and compliant workplaces for employees.

We believe in transforming the future of online learning by integrating training with the power of storytelling and movies. This approach creates memorable and interactive training experiences that are effective in promoting best corporate governance practices and codes of conduct within organizations.

Our training courses cover a range of important topics such as Prevention of Sexual Harassment (PoSH), Diversity, Equity & Inclusion (DEI), Anti-Bribery & Anti-Corruption (ABAC), Data Protection and Privacy (DPP), and more. By participating in our training programs, organizations can ensure that their employees are well-versed in the latest compliance regulations and corporate governance standards.

With our innovative training methods and expertise in corporate compliance, Rainmaker is dedicated to helping organizations achieve their goals of creating ethical and compliant workplaces.

Preface

This handbook aims to provide a thorough overview of the legal and regulatory framework for data protection and privacy in India, and to analyze the compliance requirements for companies operating in the country. The research delves into the various laws and regulations that govern data collection, storage, and use in India, such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under the Information Technology Act, 2000, as well as the General Data Protection Regulation (GDPR). Additionally, the handbook examines the best practices and technologies that organizations can implement to protect personal data, such as access controls, and incident response plans. It also explores the potential impacts of data breaches on individuals and organizations, and discusses the measures that can be taken to mitigate these risks. Overall, the goal of this handbook is to provide a comprehensive understanding of the legal and regulatory landscape for data protection and privacy in India, and to offer practical guidance for companies to effectively manage and protect personal data.

Context

The COVID-19 pandemic has shifted our focus towards virtual environments, altering the way we work, interact online, and maintain our digital presence. As a result, data has become a valuable asset for companies, and protecting it from cyberattacks and data breaches has become a top priority for maintaining a strong brand, reputation, and trust in the marketplace.
As per a report by Indusface, there were 829 million cyber-attacks blocked during the fourth quarter of 2022, with 59% of the websites having their origin in India.

The Supreme Court of India has repeatedly ordered the Central Government to establish a robust data protection system, marking the beginning of efforts to ensure a proficient data protection and privacy regime for the country. In multiple data privacy cases, such as Karmanya Singh Sareen v Union of India, the Court has emphasized the need for a strong regulatory regime. This case specifically addressed the violation of the right to privacy by WhatsApp and its infringement of privacy tactics.

In our quest to develop a comprehensive privacy legislation, India has thus far seen four versions of the Data Protection Bill. The current version is the Digital Personal Data Protection Bill, 2022 (DPDP Bill). The objective of this new Bill is to cater to the individual's right to privacy and protection. It sets structured parameters for administering digital personal data and outlines specific rights and duties for data subjects and data processors, as well as penalties for non-compliance. It also aims to provide much-needed clarity for businesses on how to align their strategies and internal policies with standard procedures.

Understanding Data Protection and Privacy

A Comprehensive Overview

Data protection and privacy are essential for any organization, as they help safeguard sensitive information from various cybersecurity threats. To operate effectively, a business must develop a data protection plan that ensures the integrity of its data. As the amount of data being generated and stored increases, so does the importance of data protection. Cyberattacks and data breaches can have severe consequences, and it is crucial for organizations to proactively secure their data and regularly update their security protocols.

It is important to protect data and privacy at all times, but the importance of cybersecurity is even greater when trust and reputation are at stake. This is particularly true for organizations whose reputation is closely tied to the data they are entrusted with. Data privacy plays a crucial role in the growth and success of a business, as well as its goodwill.

Consonance with Indian Laws

Many countries around the world have implemented legal frameworks to address the issue of data protection, as the challenges surrounding data protection have become increasingly prevalent.

In India, the Information Technology Act, 2000 (the "IT Act") and the Rules (including subsequent Amendments) made under it, provide for the collection, storage, disclosure, and transfer of electronic data and give legal recognition to these activities. The IT Act also establishes penalties for offenses and non-compliance.
In addition to the IT Act, there are also the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("SPDI Rules"), the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("CERT-In Rules"), and CERT-In Guidelines, 2022 which provide a structured approach to dealing with compliance requirements for organizations in India. These regulations aim to protect against unauthorized access to and monitoring of customer data. Any company that collects or stores sensitive information about customers must comply with strict privacy regulations.

Previously, the right to privacy was not recognized as a guaranteed fundamental right under the Indian Constitution. However, in the landmark case of Justice K S Puttaswamy (Retd.) & Anr. vs. Union of India and Ors., the Supreme Court of India recognized the right to privacy as a fundamental right under the ambit of Article 21 of the Constitution, as a component of the right to "life" and "personal liberty." According to Justice Kaul, the Court has recognized an element of the right to privacy known as "informational privacy," and it has decided that the right to access information about a person and their personal information deserves privacy protection.

Navigating Compliance in India

A Checklist for Companies

The laws aim to impose strict compliance obligations on both individuals and business organizations. Compliance requirements for Indian companies are covered under the IT Act (2000), SPDI Rules (2011), CERT-In Rules (2013), and CERT-In Guidelines (2022). The IT Act 2000 applies to any firm, sole proprietorship, or association of individuals engaged in professional or commercial activities registered in India, as well as to corporate entities or firms that conduct business in India and maintain servers within the country's borders.

The SPDI Rules, 2011, apply to body corporates and anyone who acts on behalf of that body corporate in or outside India. The CERT-In Guidelines cover all body corporates, such as companies or firms that engage in commercial or professional activities in India or any network located in India.

Hereinforth, 'You' or 'Your' refers to the company.

These are certain compliance measures that can help your business:

Concept of Notice:

As per the SPDI Rules, you must make sure to disclose information about the data being collected by the company, as this helps promote transparency and increases the confidence of clients/consumers in your venture.

Consent while Collection:

One of the pillars of an efficient data privacy compliance system is consent. In some circumstances, obtaining your consumer's informed consent may eliminate your liability for cybersecurity breaches. The SPDI Rules allow consumers to withdraw their consent at any time while availing of the services offered by a company.

Focus on Data Minimization:

You should only collect and use data that is required for a specific purpose and must take care not to retain it after the satisfaction of the particular objective. The notion of purpose limitation and data minimization is also included within the ambit of the SPDI Rules.

Right to Erasure:

Once you collect data from your clients or consumers, you should provide them with an option to erase or edit that data. The SPDI Rules mandate you to provide data subjects access to their information and the right to correct any inaccurate information.

Maintain a Privacy Policy:

While dealing with personal information, you must maintain a transparent and readily available privacy policy, according to the SPDI Rules. This privacy policy will ensure that your business is safeguarded from all cybersecurity threats and will also provide you with a plan of action while dealing with such threats.

Conduct Periodic Audits:

To understand the compliance requirements and identify any loopholes, your business must conduct periodic audits in accordance with the IS/ISO/IEC norms mentioned in the SPDI Rules. These audits must be carried out by independent auditors authorized by the Central Government.

Third-Party Disclosures:

Your company's privacy policy must include a mandate for disclosing the sharing of data with third parties. You are required to periodically review and update your privacy policy and ensure that consumers give their consent when collecting their sensitive personal data, as per the SPDI Rules.

Have a Robust Grievance Redressal System:

Your business must appoint a Grievance Officer and establish a grievance resolution mechanism for customers to address their complaints and queries. The SPDI Rules mandate the appointment of such a person to act as a first responder to any grievances received by the company.

Notify the Concerned Authority:

According to the CERT-In Guidelines, you are required to report any data breaches to the concerned authority, CERT-In (the Indian Computer Emergency Response Team), within 6 hours of receiving information about the incident. Adhering to this deadline will allow the response team to quickly trace the offender.

Appoint a Person of Contact:

Your business must appoint a Point of Contact (PoC) to communicate with CERT-In. All messages from CERT-In requesting information and offering instructions for compliance will be forwarded to the POC in accordance with the CERT-In Rules and Guidelines.

Maintenance of Logs:

Your business must maintain and enable logs of your ICT systems for a rolling period of 180 days. These logs will help you trace back all your digital activities and must be maintained within Indian jurisdiction, as per the CERT-In Guidelines.

Violations of the Information Technology Act 2000

as amended by the Information Technology (Amendment) Act 2008, can result in the following penalties:

- Damages to compensate individuals for a company's negligence in implementing and maintaining appropriate security measures to protect personal data (Section 43A, IT Act, as amended by Section 22, IT Amendment Act).

- Imprisonment and/or fines for disclosing personal information in violation of a contract or without consent (Section 72A, IT Act, as amended by Section 37, IT Amendment Act).

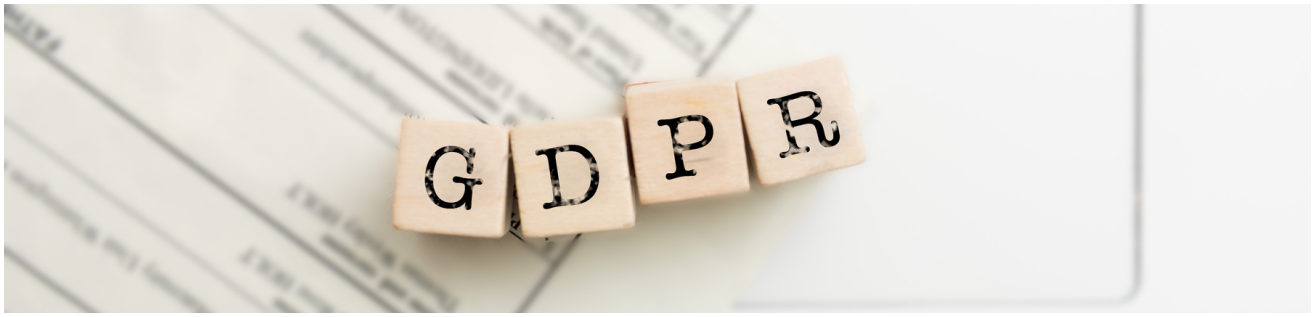
- Imprisonment and/or fines for a company's failure to provide information to the Computer Emergency Response Team or comply with their directions.

Penalties may vary depending on the specific violation and can include imprisonment for up to three years, fines of up to INR 5,00,000, or both. [Section 70B(7), IT Act, as amended by Section 36, IT Amendment Act].

Complying with GDPR

A Checklist for Companies

The General Data Protection Regulation (GDPR) is a comprehensive data protection law that came into effect on May 25, 2018. It replaced the 1995 EU Data Protection Directive and harmonized data protection laws across the European Union (EU). The GDPR applies to all companies that process the personal data of EU residents, regardless of the company's location. This includes organizations based outside of the EU if they offer goods or services to, or monitor the behavior of, EU residents. The GDPR sets out strict rules for the collection, storage, and use of personal data, and gives EU residents new rights in relation to their personal data, including the right to access, correct, and delete their data. Companies that fail to comply with the GDPR can be fined up to €20 million or 4% of their global annual revenue, whichever is higher.



Note: Hereinforth, 'You' or 'Your' refers to Company.

To help your company comply with GDPR, here are some key actions you should take:

- [ ] **Appoint a Data Protection Officer (DPO) if Required:**

  As per GDPR, certain companies must appoint a DPO. This includes public authorities, companies that engage in large-scale processing of special categories of data such as data about health, religion, or ethnicity, and companies that engage in large-scale monitoring of individuals such as through behavioral tracking.

- [ ] **Conduct a Data Audit:**

  Before you can comply with GDPR, you need to understand what personal data you process and how you process it. Conducting a data audit will help you identify what personal data you hold, where it came from, and how you use it. This will also help you identify any data protection risks and take steps to mitigate them.

Review and Update Your Privacy Notice:

Under GDPR, you must provide individuals with clear and concise information about how you use and process their personal data. Your privacy notice should explain what personal data you collect, why you collect it, and how you use it. You should also explain the individual's rights such as access to personal data or object to its processing.

Review and Update Your Data Protection Policies and Procedures:

GDPR sets out several principles you must follow when processing personal data. These include the principles of lawfulness, fairness, and transparency. Maintain a data retention policy to limit the data input and minimize the threat that comes with it. You should review your data protection policies and procedures to ensure that they comply with these principles and the GDPR.

Train Your Employees:

GDPR requires that all employees that handle personal data are trained to understand the regulation and their responsibilities. Train your employees to understand their responsibilities and how to handle personal data in compliance with GDPR.

Your staff is crucial to data protection compliance. It is vital that they understand their obligations under GDPR and how to handle personal data in compliance with the law. You should provide training to ensure that your staff knows and can fulfill their responsibilities.

Implement Appropriate Technical and Organizational Measures:

GDPR requires you to implement appropriate technical and organizational measures to protect personal data against unauthorized access, misuse, or loss. This includes measures such as encryption, secure servers, and access controls. Perform risk assessments to identify the potential risks to personal data and implement measures that are appropriate to the level of risk. This includes conducting regular security audits, testing and monitoring the effectiveness of the security measures in place, and ensuring that security is built into the design and development of products, services, and systems. Additionally, ensure that incident management processes, disaster recovery and business continuity plan are in place to address and mitigate any data breaches.

Invest in Cyber Security Insurance:

In addition to implementing technical and organizational measures to protect personal data, investing in cyber security insurance can provide added protection for your business. Cyber security insurance can help cover costs associated with data breaches, such as legal fees, investigations, and public relations efforts. It can also help mitigate financial losses caused by cyber attacks, such as lost revenue or customers. It is important to note that investing in cyber security insurance should not be seen as a replacement for implementing proper security measures, but rather as an additional layer of protection for your business. It's also good to work with a cyber security expert and insurance broker to understand the coverage and limits of the policy, and tailor it to the specific needs of your organization.

Train your Staff:

Your staff is crucial to data protection compliance. It is vital that they understand their obligations under GDPR and how to handle personal data in compliance with the law. You should provide training to ensure that your staff knows and can fulfill their responsibilities.

Review Your Contracts and Agreements:

Your staff plays a crucial role in data protection compliance and it is essential that they understand their obligations under GDPR and how to handle personal data in compliance with the law. Providing regular and effective training is necessary to ensure that your staff is aware of their responsibilities and can fulfill them. This can include training on how to handle personal data in a compliant manner, how to recognize and report a data breach, and how to respond to data subject's rights requests. It is also important to have ongoing training and awareness programs to ensure that your staff stays up-to-date with the latest data protection regulations and best practices.

Implement a Process for Handling Data Breaches:

Under GDPR, you are required to report certain data breaches to the supervisory authority and, in some cases, to the individuals affected by the breach. To comply with this requirement, it is essential to have a process in place for identifying, reporting, and responding to data breaches. This process should include procedures for assessing the likelihood and severity of a data breach, procedures for notifying the relevant authorities and individuals, and procedures for documenting the breach and the actions taken in response.

It should also include incident management procedures, and a disaster recovery and business continuity plan, to minimize the impact of a data breach on your organization and the individuals affected by it. Regularly testing and reviewing the process will ensure that it is effective and that your organization is prepared to respond to data breaches in a timely and compliant manner.

Additionally, having a data incident response plan in place that includes the roles, responsibilities, and procedures to be followed in case of a data breach, will help you respond to data breaches effectively and efficiently.

Keep Records of Your Processing Activities:

The GDPR requires you to keep records of your data processing activities. These records should include details of the personal data you process, the purposes of the processing, the categories of individuals whose data you process, and the categories of personal data you process. You should also keep records of any data protection impact assessments (DPIA) you conduct and any measures you have implemented to mitigate data protection risks.

Having accurate and up-to-date records of your data processing activities will demonstrate your compliance with GDPR and provide you with an accurate picture of the data you hold and process. It will also help you to respond to data subject's rights requests in an efficient and timely manner. It is also important to review and update these records regularly to ensure that they are accurate and up-to-date.

Respond to Subject Access Requests:

Under the GDPR, individuals have the right to access their data and obtain information about how it is being processed. If an individual makes a subject access request, you must provide them with a copy of their data and information on how you are processing it, without undue delay and within one month at most. It is important to have a process in place for responding to subject access requests, which includes identifying and locating the data, verifying the identity of the individual making the request, providing the data in an accessible format, and providing the required information within the prescribed time frame.

You should also have a designated person or team responsible for handling subject access requests, and ensure that your staff is trained on how to respond to these requests. It is also important to keep accurate records of any subject access requests and how they were handled, as well as any correspondence with the individual making the request.

Enforcing GDPR Compliance

Understanding Offences and Penalties for Non-Compliance

Non-compliance with the General Data Protection Regulation (GDPR) can result in significant administrative penalties for businesses. The GDPR outlines two levels of fines for infractions, with the maximum amount being determined by the specific provisions of the regulation that have been violated.
Level 1 fines can reach up to 10 million Euros or 2% of the company's annual global turnover. Level 2 fines can reach up to 20 million Euros or 4% of the company's annual global turnover.

In recent years, many companies have been hit with significant fines for failing to comply with the GDPR. For example, Google was fined $575 million in 2019 by French authorities for not adequately informing consumers that the company was collecting data to target ads at them.

Similarly, H&M was fined $41 million in 2020 for unlawfully maintaining extensive files on its employees' personal information and using it to make hiring and firing decisions.

These examples demonstrate that non-compliance with the GDPR can result in significant financial penalties for companies and it's important for organizations to be aware of their compliance obligations and take steps to ensure that they are in compliance.

Final Thoughts

Data compliance has become increasingly important for organizations as they face a growing number of legal requirements related to protecting user data. Adhering to these standards not only helps organizations meet their legal obligations but also mitigates the risks associated with data breaches, protects their reputation, and builds trust with users. Companies must be aware of compliance requirements in their local and foreign jurisdictions.

In India, a new Data Protection Bill is on the verge of success, which aims to enhance the country's IT laws and bridge privacy gaps. A strong data protection framework will create a more conducive environment for businesses to operate.

Given the vast amounts of data being captured by organizations and the increasing sophistication of data attacks, it is advisable for businesses to seek professional assistance in maintaining digital hygiene and building robust data protection strategies. At Rainmaker, we offer services tailored to clients' specific needs, helping them integrate digital hygiene into their business practices, and ensuring compliance with global standards.

Contact Rainmaker to book a consultation or learn more about our cybersecurity-oriented services.

For more information, please visit our website: https://rainmaker.co.in/