PROTECTING CUSTOMER DATA: BEST PRACTICES FOR STARTUPS IN THE DIGITAL ERA

Aditi Sharma, B.B.A., LL.B. (Hons.), NMIMS, Indore

ABSTRACT

In the digital age, data has become the new currency, with customer information being particularly valuable for startups. The rapid growth of startups in India over recent years has enabled the country to rank third globally in the startup ecosystem. This trend is especially relevant for startups that often depend on customer data to drive their business strategies. This paper explores the concept of data as a valuable asset, likening it to a gem, and delves into the various types of customer data that startups collect. It highlights the significant value of customer data in driving business growth and enhancing customer relationships. The legal framework surrounding data protection is examined, focusing on the "General Data Protection Regulation" (GDPR) and India's "Digital Personal Data Protection Act" (DPDPA). Key compliance requirements for startups are outlined, including obligations under both regulations. The paper further discusses best practices for protecting customer data, such as encryption, tokenization, data minimization, purpose limitation, and employee training. Each of these practices plays a crucial role in safeguarding sensitive information and ensuring compliance with legal standards. Additionally, case studies of successful startups that have effectively implemented data protection measures are presented to illustrate practical applications of these concepts. The conclusion emphasizes the necessity of robust data protection strategies for startups in the era of digitalization and suggests areas for future research, including the impact of evolving regulations on startup operations and the effectiveness of various data protection technologies. By adopting these best practices, startups can not only protect customer data but also build trust and foster long-term relationships with their clients.

Keywords: Startups, Customer data, GDPR, DPDPA, Data Protection

I. Introduction

Data has become a valuable gem it represents a precious jewel that fuels operations and forms the basis of strategies. But accompanying this treasure is the responsibility of its protection, especially as more and more businesses are beginning to log onto their specific digital platforms and services. Data plays a key role in fundamentally reshaping how businesses operate and interact with consumers. Data acts as a powerhouse for businesses and drives their operations and strategies. The value of data speaks for itself in terms of its measure of protection, mainly because much of the data comes from the customers themselves. To ensure customer trust and customer faith, businesses simultaneously comply with state requirements, and handling data responsibly concerning privacy and fair use becomes unavoidable. Compliance with legal and regulatory standards is a must for the startups concerned with the smooth running of the business, minimization of the risks of legal complications and financial sanctions, and achieving protection for their corporate reputation.[1] In Industry data-driven approach gives power not only to support short-term success through targeted marketing but also long-term growth by improving customer retention and satisfaction, which in turn results in the growth of a business.

II. Understanding Customer Personal Data with its Types

A. Customer-Sensitive Data - Sensitive data related to a customer includes all information that would otherwise have to remain confidential. This is because its access or disclosure could result in a potential risk. Examples of such data include personally identifiable information, such as credit card details, bank account details, and personal health records. Despite the fact that businesses use various methodological developments to protect sensitive data, the practice frequently lacks an overview as well as a guide on how to use data protection methods and tools.[2] When this sensitive data is breached, it can lead to massive financial, emotional, and reputational harm to both the individuals and the organisations involved.

[1] Nitesh Kumar, Decoding DPPA: Road Ahead For Startups, Businessworld, Aug 19, 2023, https://bwdisrupt.businessworld.in/article/Decoding-Data-Protection-Bill-2023-Road-Ahead-For-Startups/1908-2023-488167/.

[2] Templ, M., & Sariyar, M. A systematic overview on methods to protect sensitive data provided for various analyses. *International Journal of Information Security*, 21, 1233–1246 (2022). https://doi.org/10.1007/s10207022-00607-5.

B. Demographic Data - Customer demographic data is essential for the business to understand their characteristics which often includes, but is not limited to, gender, age, race, location, education, income, or career.[3] It helps businesses know whom they are dealing with so that an effective plan can be designed. For instance, the younger group prefers trendy things and high quality, whereas the older lot wants genuine quality. Location also decides the preference ones residing in the city prefer convenience, whereas the ones living in villages prefer practicality.

C. Transactional Data - Data obtained from transactions is known as customer transactional data. It documents the date, time, and place of the transaction as well as the cost of the goods bought, the payment methods used, any discounts that were given, and any additional quantities or characteristics related to the transaction. Usually, transactional data is recorded at the point of sale. It helps in making customer profiles that can be built using electronic sources, such as registration forms, feedback forms, log files, cookies, and collaborative software, to capture online behaviour and transactional histories. Customer transaction histories that are recorded in-store at the point of sale of goods or services and offline data from marketing events can be combined to create customer profiles.[4]

D. Behavioural Data - Behavioural data, generated by user interactions like website views, newsletter sign-ups, and shopping cart activities, reveals detailed preferences and patterns, enabling personalization and predictive modelling. It gives insights into how customers interact with products or services. Some examples include purchase history, shopping cart abandonment rates, and usage patterns (e.g., service usage frequency). This would mean very important knowledge about customer preferences and behaviour, hence making them have the most effective engagement strategies and is useful because it looks into behaviour in natural, uncontrolled settings, such as interactions between people and technology. With the growing prevalence of decision support, automation, and recommendation systems, accurate predictions of human behaviour are critical.[5]

[3] An, J., Kwak, H., Jung, S. G. et al. Customer segmentation using online platforms: isolating behavioral and demographic segments for persona creation via aggregated user data. *Social Network Analysis and Mining*, 8, 54 (2018). https://doi.org/10.1007/s13278-018-0531-0.
[4] Mobasher, B. Data mining for web personalization. In *The Adaptive Web*, vol. 4321, pp. 90–135 (2007).
[5] Dewangana, Maleesha. Introduction to Behavioral Data Science. DOI: 10.13140/RG.2.2.13519.15524 (2023).

III. Value of Customer Data in Startups

Data is the lifeblood of modern startups as it plays a pivotal role in forming key strategic decision-making. From new product development to personalizing consumer interactions and boosting marketing or sales activities, everything depends on data. Through data, startups are now able to find market opportunities, trends, and patterns. Thus, they use data to tailor their offerings to meet each customer's demands so that each customer feels special, this approach not only allows startups to scale efficiently but also increases attraction to investors who can invest in the startup and happy customers help in word-of-mouth marketing, this offers startups a competitive advantage in fast-changing markets. Startups leverage and utilize data analytics to gain insight into areas where they can apply information to various business concerns. With the data, startups can observe patterns, and trends and implement novel improvements in products and services so that they can perform well in the market. Through the analysis of this data, they can identify which customer segments would be most profitable and target them appropriately. The ability to track user behaviour and feedback helps ensure that a startup refines its offerings enough to come close to meeting the customers' expectations.

Ultimately, data analytics enables startups to measure both short-term success through revenue metrics and long-term viability through customer retention rates, guiding strategic decisions and driving sustainable growth.[6] As a startup grows, the potential for generating data grows along with it, turning into a huge competitive advantage if harnessed properly. With advanced processing through various machine learning algorithms, such wealth of information refines products and services which attracts larger and larger clientele, thereby creating a growth cycle. This continuous optimization allows startups to enhance their value proposition with potential benefits. They've grown to nearly be able to outpace competitors similarly as businesses reapring significant network effects. Ultimately, this self-reinforcing loop of data drives improvement; improvement spurring growth; and growth fueling additional data all of which may become more salient for long-term success.[7] By embracing this data-driven culture, startups will take on challenges with confidence and position themselves in a more favourable light for sustainable growth in an ever-competitive landscape.

[6] Piyanka Jain, *A Practical Guide to Increasing Startup Success Through Data Analytics*, Entrepreneur (Nov. 2, 2022), https://www.entrepreneur.com/growing-a-business/how-data-analytics-can-help-your-startup-achievesuccess/436929.

[7] Hagiu, Andrei & Wright, Julian. When data creates competitive advantage: and when it doesn't. *Harv. Bus. Rev* (Jan.-Feb. 2020), https://hbr.org/2020/01/when-data-creates-competitive-advantage.

IV. Legal Framework Surrounding Data Protection

With the flow of data worldwide data protection laws are becoming increasingly relevant, as evidenced by their historical transformation. Laws aimed at preventing manual record-keeping have evolved to tackle the challenges of the digital age requiring international cooperation and harmonisation of legal standards.[8] Data protection affirms privacy as an essential human right.

Many national constitutions and international charters protect individuals from unauthorised use of their personal data.

Overview of the European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023 (DPDPA)

A. **Global Data Protection Regulations (GDPR)**, one of the most robust data protection regulations, serves to harmonise data protection regulations across EU members; many countries even outside the EU have drawn inspiration from this legislation. Going beyond its core purpose of protecting personal data in these jurisdictions, this legislation lays down criteria for the transfer of personal data outside the EU, which ensures that handling personal data in any other part of the world is done to rather high standards. At the heart of the GDPR philosophy is the giving of unprecedented control to EU citizens and residents over his or her personal data. This regulation seeks to empower individuals by granting them control over their personal data while simplifying the regulatory environment for international business by establishing a uniform data protection framework throughout the EU.[9]Key principles of GDPR include "*Lawfulness, Fairness, and Transparency; Purpose Limitation; Data Minimisation; Accuracy; Storage Limitations; Integrity and Confidentiality; and Accountability.*"[10]

B. **Digital Personal Data Protection Act, 2023 (DPDPA)** marks a milestone in India's data protection landscape, aligning with global standards such as GDPR. It creates a comprehensive framework for protecting personal data, including

[8] Lynskey, O. Complete and effective data protection. *Current Legal Problems*, 76(1), 297–344 (2023). https://doi.org/10.1093/clp/cuad009.
[9] Singh, Nandinee. Data protection and privacy as a fundamental right: an in-depth analysis of the European Union and India's data protection legislation. *IJFMR*, 6(2), March-April 2024. DOI: 10.36948/ijfmr.2024.v06i02.15869.
[10] Art. 5 GDPR – Principles relating to processing of personal data. *General Data Protection Regulation (GDPR)* (Oct. 22, 2021). https://gdpr-info.eu/art-5-gdpr/.

consent mechanisms, individual, obligations for data fiduciaries, cross-border data transfer obligations, Processing of personal data of minors, and data principal's rights. It addresses emerging challenges in protecting sensitive personal information by responding to the growing digitisation of services and the proliferation of personal data collection in India. [10]It introduces wide-ranging changes in the treatment of personal data by organizations in India, with enforcing arrangements and penalties for non-compliance. Here, it underscores financial penalties over criminal sanctions approach is expected to promote accountability in data management while protecting the privacy rights of individuals.

V. Compliance Requirements for Startups

Key Obligations under GDPR & DPDPA

A. **Extraterritorial Scope** - Every organization that handles the personal data related to individuals who live in the EU is subject to GDPR, regardless of where the data processing is carried out. This suggests that non-EU businesses must follow this legislation if they do business with goods or services to EU citizens or monitor their travels within the EU. DPDPA governs the processing of digital personal data both inside and outside of India as long as it is done in conjunction with an activity linked to providing goods or services to Data Principals, to whom the data relates inside India.

B. **Lawful Processing** - Under GDPR, organizations must process personal data lawfully, fairly, and transparently. They also have to tell data subjects about how their information is being used. Furthermore, companies must have a legitimate reason for processing personal data, such as consent, a need to fulfil a contract, a legal requirement, the pursuit of a public purpose, legitimate interests, or vital interests. A person may only process a Data Principal's personal data under this DPDPA and for a lawful purpose, which is any use that isn't specifically prohibited by law and includes situations in which the Data Principal has granted consent or for specific legitimate uses.[11] This ensures that personal data is handled responsibly and in compliance with established legal standards,

[10] Thapa, Jaya. Data privacy vis-à-vis the Digital Personal Data Protection Act, 2023. *IJFMR*, 6(3), May-June 2024. DOI: 10.36948/ijfmr.2024.v06i03.23530.
[11] Digital Personal Data Protection Act, 2023, § 4 (India).
https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

thereby protecting the rights of individuals.

C. **Consent** - Consent is required by GDPR to be freely provided, explicit, informed, and unambiguous. Before processing personal data, businesses must get express consent, which individuals can revoke at any time. Under the DPDPA, getting people's explicit consent before processing their personal data is highly valued. For personal data to be processed for the intended purpose with clear affirmative action, free, explicit, informed, unconditional, and clear consent from the data principal is required. Additionally, it needs to be limited to the data that is truly needed.

D. **Data Subject or Principal Rights** - Organizations are required to respect data subjects' rights under the GDPR to access, correct, erase, and object to the processing of their personal data. The Indian Act gives individuals (data principals) the ability to access, correct, and erase their personal data as well as file complaints and designate how their data is processed. The organization handling the personal data has a duty to grant these rights.

E. **Data Breach Notification** - GDPR compliance requires organisations to notify the supervisory authority within 72 hours of becoming aware of a breach. Under the DPDPA, organisations are required to notify the Data Protection Authority of India (DPAI) of any data breaches as soon as possible. This makes the handling of incidents more transparent.

F. **Penalties for non-compliance** - If an organization violates the GDPR, it may be fined up to 20 million euros, or 4% of its global turnover from the previous fiscal year, whichever amount is higher. Penalties for non-compliance with the DPDPA can range from INR 10,000 to INR 250 crores, contingent on the type of violation.

VI. The Best Methods for Safeguarding Customer Data

Technical, legal, and ethical factors must all be taken into account when implementing best practices for safeguarding consumer data. Data classification, encryption, access controls, and the use of approved tools are among the key technical measures. [12]

[12] Ruivo, Pedro et al. Success factors for data protection in services and support roles: combining traditional interviews with Delphi method. In *Advances in Information Security*, ch. 42 (2018). DOI: 10.4018/978-1-52257113-1.ch042.

A. Use of encryption, secure storage solutions, and Tokenization

Strong encryption algorithms and protocols should be used to guarantee secure data transmission and storage. Data encryption represents the process of converting the plaintext into unreadable ciphertext so that only authorized parties with the proper decryption keys can access the information. Proper encryption algorithms such as AES with 256-bit keys ensure that data is well secured, either at rest or in transit. Organizations can also implement several encryption techniques, including full disk encryption, file-level encryption, and database encryption, to provide better security for data.[13]

In addition to encryption, secure storage practices are also of the highest priority. The cloud offers architecture zero knowledge, which prevents the users from accessing data other than their own; HSM offers strong key management, including tokenization by replacing sensitive values with non-sensitive ones to minimize exposure risk, and TLS for data during transit to protect interceptions. Integration of these strategies within any organization will, therefore most likely lead to the significant strengthening of defences against data breaches and sustained customer trust. Encryption software and protocols should be updated regularly to address vulnerabilities and meet changing security standards. Regular audits and vulnerability assessments can identify and address security risks or weaknesses in encryption implementation.

Data tokenization is also a recommended practice. it is the process of swapping out sensitive data with distinct identification symbols that guarantee data security and preserve all pertinent information. Tokenisation replaces sensitive information with equivalent nonsensitive data. Tokens are non-sensitive replacement information. Tokens can be generated in the following ways:

- Using a mathematically reversible cryptographic function and a key;
- Using a non-reversible function, such as a hash function;
- Use an index function or a randomly generated number.

[13] Kostic, Nikola. Secure data storage solutions: 15 strategies to protect your data. *phoenixNAP*, (2024), https://phoenixnap.com/blog/secure-data-storage-solution.

As a result, the token becomes the exposed information, while the sensitive information it represents is securely stored on a centralised server known as a token vault. The token vault is the only location where the original information can be traced back to its corresponding token.[14] Tokenization and encryption are two distinct cryptographic methods for data security. The primary distinction between the two is that tokenization does not affect the length or type of the data being protected, whereas encryption does.

B. Data Minimization and Purpose Limitation

Collect only the data that is necessary to run the business. Conduct data audits regularly to determine what data is truly required to achieve the defined purpose and to eliminate redundant data to reduce exposure. Collecting minimal personally identifiable information (PII) for research or program purposes.[15] Establishing data retention policies to store personal data only for the necessary timeframe and securely dispose of it when no longer needed. Furthermore, that data should only be kept for as long as necessary to fulfil the stated purpose. Data should not be collected for future, unexpected, or undisclosed purposes. Data should only be used for a specific, legitimate business purpose, and should not be processed in any way that contradicts that purpose. It means that data collected for one purpose should not be used for another unless further notice is provided and consent is obtained.

C. Employee Training and Awareness

Comprehensive employee training is one of the most effective ways to ensure that a Startup has superior data privacy practices. Regular training programs in data protection policies: Employees must be well-equipped with knowledge of data protection policies and practices. Thus, these training programs have to cover topics such as the maintenance of privacy, from phishing attempts, secure handling of personal data, and compliance with such regulations as GDPR and DPDPA. Continuing education would groom the employees for an action response: preponderantly as the first line of defense against a data breach or security threat. Training sessions on a variety of topics, including compliance, security awareness, the significance of training initiatives,

[14] Lutkevich, Ben. What is tokenization? TechTarget. https://www.techtarget.com/searchsecurity/definition/tokenization.
[15] McCallister, E. et al. Identifiable information (PII). NIST Special Publication, 800, 122 (2010).

training materials that are privacy-specific, and training mandates, should be provided to employees. Employers who provide their employees with the knowledge and skills necessary to handle data securely can lower the risks of data breaches and privacy violations.[16] Startups should promote a culture of data protection to drive vigilance and accountability towards data protection. This can be done by introducing a thoroughly inclusive approach that brings together privacy issues within everyday business practices and decision-making. Leadership should communicate and foster a sense of information security, encourage dialogue on security practices, and reward employees who demonstrate compliance with the data protection measures.

D. Handling Data Breaches

A proper comprehensive incident response plan is perhaps one of the more important ways of handling data breaches effectively. This plan includes how you will manage a breach, and all the necessary steps that should be taken when a breach happens, starting from assembling a response team and identifying the scope of the breach, to having containment measures in place. Such a plan should be regularly reviewed and updated to cope with new emerging threats and ensure everybody is trained on their roles in a breach situation. The implementation plan should also contain procedures for preserving evidence and conducting a thorough investigation of what caused the breach as well as its impact. Respond quickly to protect your systems and address any vulnerabilities that may have allowed the hack to occur. Take action to keep it from occurring in the future. Any physical locations connected to the breach should be secured. When necessary, lock them and modify the access codes. Immediately mobilize your breach response team to prevent additional data loss.[17] Notify the supervisory authority within the specified time frame.

E. Communicating transparently with customers in case of a breach

Give intimation to customers and communicate Openly with Customers in the Event of a Breach An overall requirement is being transparent when communicating with a customer about an event of breach. The organization should let affected persons know

[16] Noss, Sam. Data privacy training for employees. DataGrail, (June 5, 2023), https://www.datagrail.io/blog/data-privacy/data-privacy-training-for-employees/.
[17] Federal Trade Commission. Data breach response: a guide for business. https://www.ftc.gov/businessguidance/resources/data-breach-response-guide-business-.

immediately, stating what information has been compromised, the possible risks involved, and what actions the organization is taking regarding this breach. It must give clear and straightforward guidance on what customers can do to safeguard themselves by showing them what they could do, for instance changing some of their passwords or monitoring accounts for suspicious activity.

VII. Case Studies

Successful Startups with Strong Data Protection Practices

Kubit - This startup has, to begin with, pointed out the importance of data encryption and strong security policy together as a component of the overall strategy. The encryption, through AES with a key length of 256 bits, goes both ways in transit and to all data at rest, thus leaving customer data exceedingly secure. They regularly conduct training of employees on the best practices of cybersecurity to help instil data protection awareness within an organization. Kubit's reputation for robust data security and compliance with industry-recognized regulations, like SOC2 and GDPR, can be attributed to its proactive approach, which demonstrates a commitment to the highest standards of security and data protection. They may then be able to build trust as a result with their partners and clients. A robust cybersecurity infrastructure has more advantages than disadvantages, even though it might require an initial time and resource investment.[18]

Zerodha - one of the leading fintech startups in India, which has ensured the protection of its data by employing strong encryption mechanisms and multi-factor authentication for customers. In conjunction, the company has systems of regular security audits along with periodic employee training programs to ensure compliance with data protection rules. Commitment to transparency and user privacy has helped Zerodha build a firm reputation within the financial services industry.[19]

[18] Gretchenliev, Doino. Top security tips for startups: protecting your business and customers. *Kubit*. https://kubit.ai/top-security-tips-for-startups-protecting-your-business-andcustomers/#compliance.
[19] Zerodha. Security practices at Zerodha. https://zerodha.com/z-connect/general/security-practices-at-zerodha.

VIII. Conclusion

This puts customer data protection at the pinnacle of concern for the startup industry in the digital age. Data breaches and privacy are the order of the day. To ensure risk mitigation in data handling, best practices include comprehensive data privacy policies, robust security implementations, and a culture of data protection. Regular training of employees regarding data protection increases the awareness and compliance level; thus, all members know where they fit into the safeguarding of confidential information.

For example, although not necessarily a regulatory requirement in itself, data treatment transparency is part of the basic practice: openness to customers on the volume and nature of data gathered, how it is used, and how it is protected. This can serve both trust building and indeed meet regulatory needs such as the GDPR and DPDPA. In this way, data protection can be viewed as a strategic advantage and not a compliance burden for start-ups, and will also differentiate them through marketplaces along with long-term customer loyalty.

Ultimately, such a proactive approach to data protection-the integration of privacy into product development and the maintenance of robust incident response plans-will have the effect not only of assisting a startup in complying with all legal obligations but also of positioning a startup for sustainable growth in such an increasingly data-centric world. Thus, such practices are necessary for any startup willing to thrive while making its customers' data security and privacy secure.

Future Considerations

Due to the constantly changing nature of data protection, such instances offer many entry points for future studies regarding the uptake and transition of startups towards the solicitation of compliance with emerging regulations, especially in India, through the Digital Personal Data Protection Act (DPDPA) and its rules.

- Impacts of Regulatory Changes on Startups: This can be a focus of further research regarding the impact of the DPDPA as well as its counterparts to the activities of startups and particularly the relevance to compliance cost and operational adjustments. The knowledge, therefore, may reveal the challenges

and the opportunities presented.

- Data protection technologies: It will allow a startup to compare various data protection technologies such as encryption, tokenization, or secure data storage to identify best practices that lead toward improved security at affordable costs.

- User Trust and Transparency: Future studies can be conducted to show the link between customers' data protection practices and trust about customers. The research analysis about how transparency of the management of data impacts consumer activity can prove to be handy advice for the startups that want to engage in lifelong relationships with customers.

- Training and Culture: Studying on the impact of the employee training programs on awareness of data protection in the startups may contribute to the understanding of the relationship between organizational culture and compliance/security practices.

- Comparative Analysis: Cross-sectional analysis of data protection practices could better throw out different strategies or approaches adopted by startups for varying regulatory requirements across countries or industries while maintaining data security.

- Long-term Consequences of Compliance: A longitudinal study could look into the longterm consequences of data protection compliance on the growth, customer retention, and market share position of start-ups.

Pursued under these research avenues, scholars and practitioners shall focus on illuminating how innovation, data protection, and regulatory compliance are intertwined at a deeper level while helping better the ability of the startup to navigate the related complex landscape.