Prashasan July 2025, Vol. 57, Issue 1, No. 141, 206-216

https://doi.org/10.3126/prashasan.v57i1.80668
www.mofaga.gov.np/prashasanjournal
ISSN: 2565-5043 Print / ISSN: 2822-1974 Online

Enacting Data Protection Law in Nepal

Dr. Newal Chaudhary††††††††††

Abstract

In today's interconnected world, digital transactions and online activities have become indispensable facets of daily life, revolutionizing the way we communicate, conduct business, and access information. However, this rapid digitalization has also raised a critical concern, the protection of personal and sensitive data. As individuals and organizations increasingly rely on digital platforms and services, the risk of unauthorized access, disclosure, or theft of confidential information has escalated significantly.

Data breaches, which involve the unauthorized acquisition of sensitive data, pose grave risks to both individuals and organizations. For individuals, a data breach can lead to identity theft, financial fraud, and misuse of personal information, potentially causing long-lasting harm and financial losses. Organizations, on the other hand, may face severe reputational damage, loss of customer trust, legal liabilities, and substantial financial consequences resulting from data breaches.

Nepal, like many other nations, has witnessed a surge in data breach incidents in recent years, exposing vulnerabilities in its digital landscape and highlighting the pressing need for a comprehensive legal framework to address this critical issue. High-profile cases, such as the breach of the Ramailo app database in 2023 and the Vianet data breach in 2020, have underscored the urgency of implementing robust measures to safeguard the privacy and security of individuals' personal information.

This article explores the current legislative landscape in Nepal by examining existing laws and policies related to cybersecurity and data protection. It critically evaluates the gaps and shortcomings in the current legal framework, highlighting the lack of specific provisions and enforcement mechanisms needed to effectively address the complexities of data breaches.

Through comprehensive analysis, the article advocates for the enactment of a dedicated data protection law in Nepal. Such a law would encompass key aspects like mandatory breach notification requirements, stringent data protection standards, and effective enforcement mechanisms. By addressing these crucial elements, a robust data protection law can safeguard the rights and interests of Nepali citizens, fostering a secure and trusted digital environment that promotes economic growth, innovation, and public confidence in the digital ecosystem.

††††††††††*Assistant Professor of Law (T.U.), Nepal Law College, Kathmandu*
Email: nc2067@gmail.com

This article emphasizes the importance of a comprehensive legal framework that aligns with international best practices and facilitates cross-border cooperation in combating the global threat of data breaches. By establishing clear guidelines, accountability measures, and consumer protections, a dedicated data protection law can empower individuals, organizations, and regulatory bodies to proactively address data breaches, mitigate potential risks, and uphold the principles of privacy and data security in the digital age.

Keywords: data breach, data protection, cybersecurity, privacy, breach notification.

Introduction

"Every byte of data breach is a bite on an individual's privacy."

In the digital age, data has emerged as a highly valuable and strategic asset for individuals, businesses, and governments alike. The exponential growth of digital technologies and online activities has led to the generation and storage of vast amounts of data, ranging from personal information such as names, addresses, and contact details to financial records, intellectual property, and confidential business information. While this data revolution has ushered in unprecedented opportunities for innovation, efficiency, and connectivity, it has also exposed vulnerabilities that can lead to data breaches, the unauthorized access, disclosure, or acquisition of sensitive, confidential, or protected information.

Data breaches can occur due to various factors, including sophisticated cyber-attacks orchestrated by malicious actors, human error or negligence within organizations, system vulnerabilities or software flaws, and even malicious insiders with unauthorized access to sensitive data. Regardless of the cause, data breaches can have severe and far-reaching consequences. For individuals, a data breach can result in identity theft, financial fraud, and misuse of personal information for nefarious purposes. Organizations, on the other hand, may face significant reputational damage, loss of customer trust, legal liabilities, and substantial financial losses. Furthermore, data breaches can undermine national security and the integrity of critical infrastructure, posing risks to government agencies and essential services.

Nepal, a rapidly digitizing nation, has not been immune to the growing threat of data breaches. In recent years, the country has witnessed several high-profile incidents exposing vulnerabilities in its digital landscape. One notable example is the 2023 breach of the Ramailo app database, which compromised the personal information of thousands of Nepali citizens, including their names, addresses, and email addresses.

Such incidents have highlighted the pressing need for a comprehensive legal framework to address data breaches in Nepal. While the country has taken steps to address cybersecurity and data protection through existing laws and policies such as the Electronic Transaction Act, 2008, these instruments lack specific provisions and enforcement mechanisms to effectively manage the complexities of data breaches.

The absence of a dedicated data protection law has left Nepal vulnerable to the growing risks posed by cyber threats and the mishandling of sensitive data. Without a robust legal framework, individuals

and organizations may lack necessary safeguards, notification procedures, and remedies in the event of a data breach, potentially exposing them to significant harm and exacerbating the consequences.

In light of these challenges, it has become increasingly evident that Nepal urgently needs a comprehensive data protection law to protect the rights and interests of its citizens, foster a secure and trusted digital environment, and align with global efforts to combat the threat of data breaches.

Data Breaches in Nepal

A data breach occurs when information is illicitly taken from a system without the knowledge or authorization of the system's owner. It can affect both small businesses and large enterprises, compromising sensitive data such as credit card details, customer records, trade secrets, or even matters of national security.

In 2017, NIC Asia Bank, one of Nepal's private-sector commercial banks, fell victim to a cyber-attack. Hackers exploited vulnerabilities in the bank's security measures, breaching the system and orchestrating fraudulent transactions via the SWIFT interbank messaging system. This breach exposed sensitive customer information, including account details and transaction histories, undermining public trust in the banking sector and resulting in financial consequences.

On June 27, 2017, the Department of Passport experienced a cyber intrusion, compromising governmental data. The hackers issued threats to the Government of Nepal, leveraging the stolen information as a bargaining tool. Moreover, on July 25, 2017, a coordinated attack by a group named **'Paradox Cyber Ghost'** targeted 58 government websites simultaneously, further exposing vulnerabilities in Nepal's cyber infrastructure.

In 2020, Foodmandu, a prominent e-commerce food delivery company, experienced a devastating cyber-attack. Hackers infiltrated their system and obtained the personal details, names, addresses, and phone numbers, of 50,000 customers. The attackers later disclosed this sensitive information on a public platform, jeopardizing the security and privacy of Foodmandu's clientele. This incident underscores the critical importance of robust cybersecurity measures to safeguard customer data, as well as the need for consumer vigilance. A Twitter handle named **Mr. Mugger** revealed the dump of data and shared the associated link.

In October 2020, eSewa, Nepal's first and largest digital wallet, experienced a data breach. A perpetrator exposed confidential information of at least 21 users, including email addresses, encrypted passwords, and account funds. The breach may have occurred due to the lack of **OTP (One-Time Password)** authentication during internet sign-in. The company denied any hacking or direct data theft, attributing the incident to unauthorized access gained through a phishing scheme involving third-party websites.

Also in 2020, Vianet, a major internet service provider (ISP) in Nepal, suffered a significant data breach affecting over 170,000 customers. A security flaw in the company's system allowed unauthorized access to personal details such as names, email addresses, phone numbers, and other data. This breach exposed subscribers to risks including phishing and identity theft. A hacker using

the Twitter handle 'नरपिचास' posted a link to the leaked data on the dark web, prompting the immediate restriction of the account and breach URL.

The Ramailo app, a popular Nepali application, was at the center of a major data breach in 2023. The unauthorized access compromised personal information of thousands of users, including names, addresses, and email addresses, raising serious concerns about cybersecurity in Nepal[‡‡‡‡‡‡‡‡‡‡]. A hacker named **"deadlyweapon1337"** leaked the entire database on a dark web breach forum. This incident further emphasized the urgent need for robust data protection measures in Nepal's digital ecosystem.

Current Legal Landscape

Nepal has initiated efforts to address cybersecurity and data protection through existing laws and policies. However, these measures are limited in scope and lack the comprehensive framework required to effectively tackle the escalating threat of data breaches.

One of the principal legal instruments is the **Electronic Transaction Act of 2008**, which was enacted to grant legal recognition to electronic records and transactions, thereby facilitating the adoption of digital technologies across various sectors. While the Act contains provisions related to cyber security and data protection, such as penalties for unauthorized access, damage, or alteration of computer systems and data—its primary focus remains on establishing the legal validity and admissibility of electronic documents and records in Nepal.

The provisions in the Electronic Transaction Act are relatively broad and do not specifically address the complexities inherent to data breaches. Key elements such as mandatory breach notification requirements, data protection standards, and enforcement mechanisms are notably absent. This leaves a significant gap in Nepal's legal framework for responding to and mitigating the consequences of data breaches effectively.

Moreover, Nepal currently lacks a dedicated data protection authority or regulatory body tasked with overseeing and enforcing data protection standards and addressing data breach incidents. The absence of such a central authority exacerbates the challenges in ensuring effective data protection and breach response mechanisms.

The present legal landscape underscores the urgent need for a comprehensive and dedicated data protection law. Although the existing laws and policies acknowledge the importance of cybersecurity and data protection, they are insufficient to cope with the rapidly evolving nature of data breaches and cyber threats. Without a robust legal framework, individuals and organizations in Nepal remain vulnerable to risks arising from unauthorized access or misuse of sensitive data.

To safeguard the rights and interests of Nepali citizens and foster a secure digital environment, a dedicated data protection law is essential. Such legislation should clearly define key terms, establish specific obligations and data protection standards, incorporate breach notification requirements, and

---

‡‡‡‡‡‡‡‡‡‡*Chaudhary, B., & Yadav, R. P. (n.d.). Nepali data on the dark web. Online Khabar English. Retrieved April 9, from https://english.onlinekhabar.com/nepali-data-dark-web.html*

provide enforcement mechanisms. Additionally, it should align with international best practices in cybersecurity and data protection.

International Landscape

In comparison, countries such as India have made significant advances in this area. India's Information Technology Act of 2000, along with subsequent amendments in 2008, includes specific provisions on data protection, requiring corporate entities to implement reasonable security practices and procedures to protect sensitive personal data. More recently, India enacted the Digital Personal Data Protection Act, 2023, which mandates organizations to report data breaches to the relevant authorities within a specified timeframe.

India also recognized privacy as a fundamental right in 2017, and the Digital Personal Data Protection Act aims to establish a comprehensive data protection framework. This framework encompasses breach notification protocols, individual rights, and the creation of a data protection authority. The Act brings India's data protection regime closer to global standards, such as the European Union's General Data Protection Regulation (GDPR).

Many developed nations have similarly implemented comprehensive data breach notification laws and robust data protection frameworks. The GDPR, which came into effect in 2018, is widely regarded as one of the world's most stringent data protection regulations. It requires organizations to report data breaches to supervisory authorities within 72 hours of discovery and imposes substantial penalties for non-compliance[*].

Similarly, in the United States, data breach notification requirements are governed by a patchwork of federal and state laws. Although there is no comprehensive federal data breach notification law, most states have enacted their own statutes mandating that companies notify affected individuals—and in some cases, regulatory authorities—when a breach involving personal information occurs. This decentralized yet robust approach ensures timely notification and accountability across jurisdictions.

Other countries such as Canada, Australia, and Singapore have also established comprehensive data breach notification laws and data protection frameworks. These measures reflect a global trend toward strengthening cybersecurity and safeguarding personal data in an increasingly digital world[†].

world[†].

---

[*] *DLA Piper. (2024, January). DLA Piper GDPR fines and data breach survey: Retrieved from https://www.dlapiper.com/en/insights/publications/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024*

[†]*In Canada, data breach notification is governed at the provincial level, with specific laws in place in place in Alberta, Quebec, and British Columbia. The Personal Information Protection and Electronic Documents Act (PIPEDA) applies to businesses engaged in commercial activities across the country, and it requires businesses to notify the Office of the Privacy Commissioner of Canada and affected individuals of a privacy breach. Australia has mandatory notification of all "eligible data breaches," which must be reported unless a specific limited exemption applies. The notification requirements apply to all organizations that are covered by the Privacy Act 1988, which includes most Australian*

In comparison, Nepal's current legal landscape lacks the specificity, enforcement mechanisms, and dedicated regulatory bodies necessary to effectively address the complexities of data breaches. While existing laws provide a general framework for cybersecurity and data protection, they fall short of addressing critical elements such as mandatory breach notification, clear data protection standards, and stringent enforcement.

The absence of a comprehensive data protection law leaves both individuals and organizations vulnerable to cyber threats. Furthermore, it limits Nepal's ability to harmonize its legal standards with international best practices. As the digital economy grows and data breaches become more frequent and sophisticated, this regulatory gap poses significant risks to citizens' privacy, national security, and economic interests.

To bridge this gap, Nepal must prioritize the enactment of a comprehensive data protection law aligned with global standards. Such legislation should establish clear definitions, prescribe mandatory breach notification procedures, set data protection obligations, and empower a dedicated regulatory authority with enforcement capabilities. By learning from the experiences of other countries and adopting internationally recognized frameworks, Nepal can build a secure and trusted digital environment that protects the rights and interests of its citizens, while fostering innovation and economic growth in the digital age.

The Principle of Proportional Reparations

The Principle of Proportional Reparations proposes a framework for compensating individuals affected by data breaches in a manner that reflects the severity and potential impact of the breach. It acknowledges that not all data breaches result in equal harm, and therefore, the reparations should be scaled according to the actual or potential damage experienced by the affected parties.

For example, a minor breach exposing non-sensitive information such as names and email addresses might warrant only services like free credit monitoring. Conversely, a severe breach compromising sensitive financial data or personally identifiable information could necessitate more extensive reparations, including long-term identity theft protection, monetary compensation, and ongoing monitoring assistance.

By establishing a tiered reparations system tied to breach severity, this principle encourages organizations to adopt rigorous data protection measures and ensures accountability through

---

government agencies, private sector organizations with an annual turnover of $3 million or more, and certain other organizations. In Singapore, the Personal Data Protection Act (PDPA) requires organizations to notify the Personal Data Protection Commission (PDPC) and affected individuals if a data breach is likely to result in significant harm to the affected individuals. The PDPA applies to organizations that collect, use, or disclose personal data in Singapore, regardless of whether the organization is located in Singapore or not.

meaningful restitution. It moves beyond mere notification requirements by instituting a binding mechanism for risk assessments and proportional redress based on the breach's impact on individuals.

Proposing the Principle of Proportional Reparations for Nepal

While existing data protection proposals primarily focus on notification and general standards, there is a critical need to address adequate reparations for those affected by breaches. Incorporating the Principle of Proportional Reparations into Nepal's data protection law can mark a pioneering step in legal innovation. This principle, yet unrecognized globally as a standalone concept, rests on the understanding that reparations must be proportional to the actual or potential harm suffered.

The key components of this principle would include:

A. Breach Severity Tiers

The law should define clear tiers of breach severity, considering factors such as the sensitivity of compromised data, the number of individuals affected, the nature of the breach **(accidental vs. malicious)**, and the likelihood of data misuse. These tiers would serve as the basis for determining the reparations owed.

B. Reparations Matrix

A detailed reparations matrix should map breach severity levels to prescribed compensation packages. These could range from credit monitoring and identity protection services to monetary compensation and long-term recovery support for high-severity incidents involving critical personal or financial data.

C. Accountability and Enforcement

To ensure the principle's effectiveness, regulatory authorities should be empowered to audit organizational preparedness, investigate breaches, and impose penalties linked to the severity tier and reparations obligations. This enforcement framework incentivizes organizations to prioritize data protection and fulfill their reparations responsibilities comprehensively.

By integrating this principle, Nepal can foster responsible data stewardship, bolster public trust, and ensure affected individuals receive adequate protection and compensation tailored to the breach's impact.

The Need for a Comprehensive Data Protection Law

The adage, "Breach of data is akin to being digitally naked," underscores the profound vulnerability that data breaches impose on individuals. Just as physical nudity exposes one's privacy and dignity,

a data breach exposes personal information, stripping away control and exposing individuals to risks like identity theft and fraud.

To effectively address the escalating threat of data breaches and safeguard the rights of Nepali citizens, Nepal urgently requires a comprehensive data protection law encompassing the following critical elements:

a. Mandatory Breach Notification

Organizations must be legally obligated to promptly notify affected individuals, regulatory authorities, and relevant entities upon discovering a data breach. Timely notification, ideally within 72 hours, ensures transparency and enables individuals to take protective measures. The law should provide clear guidelines on the notification content and delivery methods to maximize effectiveness.

b. Data Protection Standards

The law should mandate robust standards for handling sensitive data, including requirements for encryption, access controls, secure storage, and safe disposal. Organizations should be required to implement industry best practices such as standardized encryption protocols and strict authentication measures. Regular security audits and risk assessments must be mandated to proactively identify and mitigate vulnerabilities.

c. Enforcement Mechanisms

Effective compliance requires strong enforcement powers. Nepal should establish a dedicated Data Protection Authority or empower existing regulatory bodies with investigative, auditing, and penalty-imposing powers, similar to **the UK's Information Commissioner's Office (ICO)**[*] or **Singapore's Personal Data Protection Commission (PDPC)**[†]. Such an authority would play a

[*]*The Information Commissioner's Office (ICO) is a UK-based independent regulatory body responsible for enforcing data protection and privacy laws in the country. The ICO is tasked with promoting openness by public bodies and data privacy for individuals, as well as ensuring that organizations comply with their data protection obligations under the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). The ICO has a wide range of powers and responsibilities, including investigating potential breaches of data protection laws, providing guidance and advice to organizations on data protection best practices, and imposing fines and penalties for non-compliance. The ICO also has a role in promoting transparency and accountability in the use of personal data, particularly in the context of public sector organizations and their use of data for public interest purposes.*

[†]*The Personal Data Protection Commission (PDPC) is a Singaporean regulatory body responsible for enforcing the Personal Data Protection Act (PDPA). The PDPC is tasked with ensuring that organizations comply with the PDPA's data protection requirements, which include obtaining consent for the collection, use, and disclosure of personal data, implementing appropriate data protection measures, and providing individuals with access to their personal data. The PDPC has a wide range of powers and responsibilities, including investigating potential breaches of the PDPA, providing guidance and advice*

pivotal role in overseeing adherence, investigating breaches, and imposing sanctions for non-compliance.

d. Consumer Rights and Remedies

The law must clearly articulate the rights of individuals affected by data breaches, including access to compensation, identity theft protection services, and avenues for legal recourse in cases of negligence or willful misconduct. For instance, individuals impacted by breaches involving financial data should be entitled to free credit monitoring for a defined period to detect and prevent fraud.

The Information Commissioner's Office (ICO) is a UK-based independent regulatory body responsible for enforcing data protection and privacy laws in the country. The ICO is tasked with promoting openness by public bodies and data privacy for individuals, as well as ensuring that organizations comply with their data protection obligations under the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). The ICO has a wide range of powers and responsibilities, including investigating potential breaches of data protection laws, providing guidance and advice to organizations on data protection best practices, and imposing fines and penalties for non-compliance. The ICO also has a role in promoting transparency and accountability in the use of personal data, particularly in the context of public sector organizations and their use of data for public interest purposes.

e. Sector-Specific Regulations

While a comprehensive data protection law should establish a general framework applicable across all sectors, it must also accommodate sector-specific regulations that address the unique challenges and sensitivities of particular industries. Sectors such as healthcare, finance, and telecommunications often handle especially sensitive personal data, necessitating tailored regulatory requirements.

For example, the healthcare sector requires stringent protections for patient medical records and robust enforcement of privacy laws, given the critical sensitivity of health information. Likewise, the financial sector demands specialized guidelines for securing customer financial data and precise reporting protocols for breaches involving financial transactions. These sector-specific regulations ensure that data protection measures are appropriately calibrated to the nature and risk profile of the data involved.

f. International Cooperation and Harmonization

Data breaches frequently transcend national boundaries, making international cooperation an essential component of effective data protection. Nepal’s data protection law should therefore facilitate mechanisms for international collaboration and harmonization with global standards and best practices.

---

to organizations on data protection best practices, and imposing fines and penalties for non-compliance. The PDPC also has a role in promoting transparency and accountability in the use of personal data, particularly in the context of organizations that collect, use, or disclose personal data on a large scale or for sensitive purposes.

This can include protocols for sharing information and expertise, mutual legal assistance agreements, and cooperation with international law enforcement and Cybersecurity organizations, particularly in cases involving cross-border data transfers or cyber threats originating abroad.

Moreover, aligning Nepal's data breach legislation with internationally recognized frameworks, such as the European Union's General Data Protection Regulation (GDPR)[*] or the Asia-Pacific Economic Cooperation (APEC)[†] Privacy Framework, will enhance consistency, compatibility, and credibility on the global stage. This alignment can facilitate smoother international data exchanges, improve Nepal's digital economy integration, and strengthen its overall Cybersecurity posture.

By aligning with global data protection standards, Nepal can facilitate cross-border data flows and enhance its reputation as a secure and trusted digital environment for both businesses and individuals. Incorporating these key elements into a comprehensive data protection law will establish a robust legal framework for safeguarding personal data, ensuring transparency and accountability, and fostering a secure and trustworthy digital ecosystem that supports economic growth and innovation.

Conclusion

The increasing frequency and severity of data breaches, along with their far-reaching consequences for individuals, businesses, and the nation's digital landscape, highlight the urgent need for Nepal to enact a comprehensive data protection law. The potential risks, ranging from identity theft and financial fraud to reputational damage and legal liabilities, demand a proactive and robust response from lawmakers and stakeholders alike.

---

[*]*The General Data Protection Regulation (GDPR) is a binding legislative act that applies to all organizations operating in the European Union, regardless of where the data is processed. It imposes several obligations on organizations, such as appointing a Data Protection Officer and conducting impact assessment analysis for high-risk processing activities. The GDPR also has robust enforcement mechanisms, including the power to impose hefty fines for non-compliance. The GDPR mandates data controllers and processors to notify data protection authorities of any data breach that imposes any risk to the rights and freedoms of natural persons. It also requires organizations to implement appropriate technical and organizational measures to ensure the security of personal data and to conduct regular data protection impact assessments for high-risk processing activities.*

[†]*The APEC Privacy Framework is a regional data protection framework developed by the Asia-Pacific Economic Cooperation (APEC) forum. It promotes a flexible approach to information privacy protection across APEC member economies while avoiding the creation of unnecessary barriers to information flows. The APEC Cross-Border Privacy Rules (CBPR) System is a voluntary, accountability-based system that facilitates privacy-respecting data flows among APEC economies. It requires participating businesses to implement data privacy policies consistent with the APEC Privacy Framework and have these policies assessed and enforced by an Accountability Agent. The APEC Privacy Framework is designed to promote a consistent approach to privacy protection across APEC member economies. It emphasizes the need for organizations to implement appropriate confidentiality measures and have accountability mechanisms in place. However, it does not impose specific obligations on organizations or have robust enforcement mechanisms like the GDPR.*

By establishing a strong legal framework that includes mandatory breach notification, stringent data protection standards, effective enforcement mechanisms, clearly defined consumer rights and remedies, sector-specific regulations, and provisions for international cooperation, Nepal can demonstrate its commitment to safeguarding the privacy and security of its citizens in the digital age.

Enacting a dedicated data protection law is not merely a legal necessity but a critical step toward building a resilient and secure digital infrastructure that fosters public trust, supports economic growth, and encourages innovation. In today's interconnected world, where data flows seamlessly across borders, aligning Nepal's data protection standards with global norms and best practices is essential for enhancing the country's competitiveness in the digital economy.

The consequences of inaction are severe. Without a comprehensive legal framework, individuals and businesses in Nepal remain vulnerable to escalating threats such as cyber-attacks, data misuse, and unauthorized access to sensitive information. This lack of protection not only compromises the privacy and financial well-being of citizens but also undermines Nepal's ability to attract foreign investment, drive innovation, and actively participate in the global digital marketplace.

It is imperative that policymakers prioritize the development of an effective, context-sensitive data protection law tailored to Nepal's unique needs and aspirations.

Addressing Nepal's unique needs and challenges, while ensuring alignment with international standards and best practices, is essential for effective data protection. Industry leaders have a crucial role to play, not only in advocating for strong data protection measures but also in implementing robust cybersecurity practices and actively participating in the policymaking process. Their engagement will help ensure that the resulting legislation reflects the practical realities and challenges faced by businesses operating in Nepal.

Civil society organizations and consumer advocacy groups must also be actively involved. Their role includes raising public awareness about the importance of data protection, championing strong consumer rights and remedies, and holding both policymakers and businesses accountable for upholding privacy and security standards.

Through a concerted and collaborative effort, Nepal can lay the foundation for a secure and trusted digital future, one in which individuals and businesses can thrive within an environment that values privacy, transparency, and accountability. By proactively addressing the threat of data breaches and fostering a culture of data protection, Nepal can position itself as a leader in the digital era. This will not only attract investment and drive innovation but also ensure the protection of the rights and interests of its citizens in an increasingly data-driven world.