

Humanities and Social Sciences Journal

2026 (June); Volume 18, Number 1: 218-231

<https://rrlc.tu.edu.np>

doi: <https://doi.org/10.3126/hssj.v18i1.99866>

ISSN: 2594-3065 (Print); ISSN: 3021-9744 (Online)



Tribhuvan University,
Ratna Rajyalaxmi Campus,
Research & Educational
Development Project
Management Committee (RMC)

A critical assessment of Nepal's digital data protection framework: Legal gaps and reform directions

Tul Bahadur Khadka

Deputy Government Attorney

Office of the Special Government Attorney, Kathmandu, Nepal

Email: kc.daart@gmail.com; tulbahadur.khadka@nepal.gov.np

<https://orcid.org/0009-0008-9098-9794>

To cite this article: Khadka, T. B. (2026). A critical assessment of Nepal's digital data protection framework: Legal gaps and reform directions. *Humanities and Social Sciences Journal*, 18(1), 218-231. <https://doi.org/10.3126/hssj.v18i1.99866>

Received: August 3, 2026; **Accepted:** September 1, 2026; **Published:** September 9, 2026

Abstract

Nepal has taken up digital technologies, e-governance systems, and digital financial services at speed, and social, economic, and administrative life has changed with them. Services are faster now, and easier to reach. They have also brought new trouble over personal data, privacy, and digital security. This article looks at the legal and institutional framework governing digital data protection in Nepal and sets out where the regulatory gaps leave individual privacy poorly protected. The article uses a qualitative doctrinal method, supported by Key Informant Interviews (KIIs) with legal practitioners, cyber law experts, academics, and technology policy professionals. It looks at the constitutional guarantee of privacy under the Constitution of Nepal (2015), the Individual Privacy Act (2018), the Electronic Transactions Act (2006), and related policy documents. It also draws lessons from data protection systems abroad, above all the European Union's General Data Protection Regulation (GDPR). The findings show that Nepal's framework is scattered across different laws and is too weak for present-day problems such as large-scale data processing, artificial intelligence, cloud computing, and the transfer of data across borders. The main shortcomings are the lack of an independent Data Protection Authority, thin regulatory duties for private sector data controllers, limited enforcement, and weak accountability structures. The article argues that Nepal needs a comprehensive Digital Data Protection Act, along with institutional reform, stronger compliance rules, and enforcement that works. A sound data governance framework matters for protecting citizens' informational privacy, and it also builds public trust and keeps digital transformation sustainable.

Keywords: Data protection, data privacy; informational privacy; cyber law; data governance; regulatory gaps; Nepal.



© Author(s). This paper is distributed under the terms of the Creative Commons CC BY-NC 4.0 DEED (<https://creativecommons.org/licenses/by-nc/4.0/>), which permits copying and redistributing the material in any medium or format for non-commercial uses with proper attribution to the creator.

Introduction

The move to digital governance, digital financial services, and online social interaction has changed how personal information is collected, processed, and used. Personal data is now a valuable resource that shapes economic activity, public administration, and the choices individuals make (Solove, 2004). Depending on digital systems to this degree has, at the same time, raised serious worries about privacy, security, and whether personal information is being used responsibly (Westin, 1967).

Digital growth in Nepal has been rapid over the past decade. Government initiatives such as the Digital Nepal Framework, the National Identity Card system, the Nagarik App, online public services, and digital payment platforms have sped up the move toward a data-driven society (Ministry of Communication and Information Technology, 2019). Private services have done the same. Mobile banking, digital wallets, e-commerce platforms, and other online service providers now collect and process more of citizens' personal and financial information (Nepal Rastra Bank [NRB], 2025).

Digitalization has improved efficiency, access, and inclusion, but it has also increased the risk of unauthorized access, misuse, data breaches, and poor control over personal information (General Data Protection Regulation [GDPR], 2016, Recitals 4–6). Public bodies and private ones alike hold biometric data, financial records, location information, and other sensitive personal details. Holdings of that kind call for a strong legal and institutional framework if accountability is to be secured and individual privacy protected (Council of Europe, 2018).

Privacy is a fundamental right in Nepal under Article 28 of the Constitution of Nepal (2015), and that recognition is an important legal foundation for data protection. What follows from it in ordinary law, though, is scattered. The Individual Privacy Act (2018) and the Electronic Transactions Act (2006) do not go far enough to meet the difficult demands of modern digital data governance (Electronic Transactions Act, 2006; Individual Privacy Act, 2018). Questions of institutional oversight, private sector accountability, cross-border data transfers, data retention, and effective enforcement are still largely unresolved.

This article therefore examines Nepal's digital data protection framework, identifies the legal and institutional gaps in it, and considers the reforms needed to build a comprehensive and effective data protection regime. It also suggests the legal and institutional reforms that would strengthen Nepal's digital data protection framework.

Data Protection and Privacy

Data Privacy

Data privacy is part of the wider idea of privacy. Privacy has long been seen as the right to be "let alone," a phrase first made famous by Warren and Brandeis in 1890 (Warren and Brandeis, 1890). Later, Alan Westin gave a definition of privacy that has influenced much of the modern debate. He said privacy is the right of people to decide for themselves when, how, and to what extent information about them is shared with others (Westin, 1967). This idea forms the basis of what we call data privacy.

Data privacy means protecting information about individuals when it is collected, stored, processed, and shared. It ensures that people have some control over their personal information and that such information is not misused. Laws have been developed to put this into practice. The GDPR is the most important example. It sets out key principles such as fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and confidentiality (GDPR, 2016, art 5). These principles show that privacy is not only about secrecy. It is about ensuring that data is used in ways that are fair and lawful.

Data privacy is also closely linked with dignity and autonomy. Solove explains that privacy is not one single idea, but rather a set of related problems such as surveillance, aggregation, and secondary use of data (Solove, 2008). These problems affect the ability of people to make choices and to shape their own lives. Without data privacy, individuals can easily be profiled or targeted in ways they cannot control.

In the digital age, relying only on individual control is not enough. Consent alone does not protect people, because data systems are complex and often invisible to users (Cohen, 2012). For this reason, modern approaches emphasise structural solutions. These include privacy by design, data protection impact assessments, and oversight by independent bodies. Hildebrandt also argues that privacy should be treated as an issue of architecture. This means protections should be built into the design of systems and technologies, not left as an afterthought (Hildebrandt, [year], pp. 112–115).

Data privacy plays several roles at the same time. It protects individual rights such as dignity and autonomy. It helps maintain trust and fairness in society. It also limits the power of states and corporations by ensuring that surveillance and data processing remain under legal control. In today's world, where personal information can be collected and linked in new ways, data privacy is one of the most important tools we have to protect human rights in a digital society.

Data Protection

Data protection is a legal and social concept that ensures personal information is collected, processed, stored, and shared in ways that respect the rights and dignity of individuals. It is closely related to, but distinct from, the broader notion of privacy. While privacy concerns the general right to be left alone or to control access to personal spaces, data protection specifically addresses the management and safeguarding of information that can identify a person (Media Defence, 2020).

At its core, data protection is about control, accountability, and responsibility. It recognises that personal data is not merely a resource for organisations or states; it belongs to the individual. Effective data protection allows individuals to maintain control over their information, determine who can access it, and decide how it can be used. At the same time, it imposes obligations on organizations and institutions to handle data responsibly, preventing misuse, unauthorized access, and harm (SSRN, 2021).

The significance of data protection has grown dramatically in the digital age. The increasing reliance on digital technologies, online platforms, and automated systems has resulted in unprecedented collection and processing of personal information. In this context, data protection serves several critical functions. First, it safeguards individual rights and

dignity, ensuring that personal information is not misused in ways that could harm reputation, autonomy, or personal freedom. Second, it promotes fairness and equality, preventing discrimination and ensuring that data is used responsibly and transparently. Third, it builds trust between individuals, organisations, and the state, which is essential for the effective functioning of digital services and governance. Finally, data protection contributes to the protection of democratic values and freedoms, by limiting the potential for surveillance, manipulation, and arbitrary use of personal information (Rodotà, 2009).

The concept of data protection rests on several essential elements that define its scope and operation:

- **Personal Data:** Information that relates to an identified or identifiable individual, including names, contact details, location data, identification numbers, and biometric or genetic information.
- **Data Subject:** The individual whose personal information is collected, stored, or processed.
- **Data Controller:** The person or organization responsible for deciding how and why personal data is processed. Controllers have the primary responsibility for ensuring lawful and ethical data practices.
- **Data Security:** Technical and organizational measures to protect data from loss, misuse, theft, or unauthorized access. This includes encryption, access controls, and secure storage protocols.
- **Accountability and Responsibility:** The principle that those who process personal data must be answerable for their actions, ensuring that data is accurate, lawfully processed, and adequately safeguarded (GDPR, 2016, arts 5–6).

Data protection establishes a framework that balances the opportunities offered by data-driven technologies with the potential risks to individuals. It recognizes that personal data has value, not only economically but socially and legally, and that improper handling can have significant consequences. By defining the responsibilities of data controllers and the rights of data subjects, data protection ensures that individuals retain agency over their information, even in complex digital environments (Hildebrandt, 2020, pp. 95–115).

Thus, understanding data protection is fundamental for assessing the challenges and responsibilities associated with the collection and use of personal information. It provides the conceptual foundation upon which legal norms, policy measures, and technical safeguards are built, making it an indispensable part of modern digital governance and human rights protection.

State of Data Protection in Nepal

Digital technology in Nepal has spread faster than the country's legal and institutional capacity to protect personal data, and the gap between the two is wide. Public institutions, financial organizations, healthcare providers, and private technology companies now collect and process large volumes of personal, biometric, and financial information (Ministry of Communication and Information Technology [MoCIT], 2019; Nepal Rastra Bank [NRB],

2025). All of this happens within a regulatory setting that has no dedicated, comprehensive digital data protection law (see General Data Protection Regulation [GDPR], 2016).

Nepal recognizes privacy as a fundamental right under Article 28 of the Constitution and has passed the Individual Privacy Act (2018), yet the existing legal framework does not deal well with how complicated data processing has become. On the duties of data controllers it says little, and the same goes for data minimization, retention periods, breach notification, cross-border data transfers, and the rights individuals hold over their own information (General Data Protection Regulation [GDPR], 2016, arts. 5, 6, 12–22).

No independent regulatory authority exists, which weakens enforcement and accountability further (European Data Protection Board [EDPB], 2020). Someone whose data privacy has been violated is left with ordinary court remedies, and those sit badly with disputes that turn on technical detail. Private companies in digital services, financial technology, e-commerce, and online platforms also work without clear enough compliance duties or monitoring (Solove, 2008).

Newer technologies such as artificial intelligence, cloud computing, and big data analytics have made the need for a modern and comprehensive data governance framework more urgent (OECD, 2013). Without working legal safeguards and institutional oversight, Nepal's digital transformation could raise the risk of data misuse, unauthorized disclosure, identity theft, and loss of public trust (World Bank, 2021).

Theoretical Framework: From Spatial Privacy to Informational Privacy

What people mean by privacy has shifted a great deal alongside social, technological, and economic conditions. It once meant, above all, being safe from physical intrusion into one's private sphere. Samuel Warren and Louis Brandeis (1890) captured that older view in their influential work, describing privacy as the "right to be let alone" and stressing protection against unauthorized interference with personal life (Warren & Brandeis, 1890).

Digital technology has changed what privacy concerns are about. In a data-driven society, privacy is no longer tied to physical space or personal secrecy alone; it now turns on how public and private bodies collect, process, store, and use personal information. Out of that shift came the idea of informational privacy, which is a person's ability to control how their personal data is used and passed on (Schwartz & Solove, 2011).

Alan Westin (1968) developed the modern understanding further by stressing individual control over personal information (Westin, 1967). Privacy risks in the digital age, on his account, come from how personal data is gathered together, processed, and misused, and not simply from direct surveillance (Solove, 2004). The harms he describes arise from information collection, from secondary use, from insecurity, and from the absence of individual control (Solove, 2008).

The principle of data self-determination builds on these theories. It holds that individuals should have real control over their personal information, including decisions about collection, processing, retention, and deletion (Bygrave, 2002). Present-day data protection frameworks, including the European Union's General Data Protection Regulation (GDPR), follow this

approach and give individuals rights over their personal data that can be enforced (General Data Protection Regulation [GDPR], 2016, arts. 5, 12–22).

This theoretical framework is the basis on which Nepal's digital data protection regime is assessed here. The article asks whether Nepal's existing law protects informational privacy well enough, and whether it gives people workable means of controlling how their personal data is collected and used in the digital environment.

International Practices: GDPR and Comparative Data Protection Models

Modern data protection laws owe much to international regulatory models that try to balance technological innovation against individual privacy rights. Of these, the European Union's General Data Protection Regulation (GDPR), in force since 2018, is one of the most far-reaching approaches to personal data governance (General Data Protection Regulation [GDPR], 2016, arts. 5, 24, 25, 44–50).

The GDPR built its approach on rights and accountability. Duties for data controllers and processors are spelled out, and the rights of data subjects are strengthened. Its main principles are lawful and transparent processing, purpose limitation, data minimization, accuracy, storage limitation, security, and accountability. A set of individual rights goes with them: access, rectification, erasure, data portability, and objection to certain kinds of processing. Oversight falls to independent supervisory authorities, and penalties for non-compliance are heavy.

A developing country, though, has to weigh its own institutional capacity, technological infrastructure, and social and economic conditions before taking on a framework of that kind. For Nepal the useful comparison is India's Digital Personal Data Protection Act (DPDPA), 2023: the two countries sit in the same region, are going through the same fast digital expansion, and run into similar governance problems. The DPDPA introduces the ideas of Data Fiduciaries and Data Principals, sets duties for bodies that process personal data, and creates an institutional mechanism in the Data Protection Board of India (Digital Personal Data Protection Act, 2023, ss. 2, 8, 18).

Japan, Singapore, and South Korea have likewise built wide-ranging data governance systems that combine privacy protection with digital innovation (Act on the Protection of Personal Information [APPI], 2003/2020; Personal Data Protection Act, 2012; Personal Information Protection Act, 2023). Their experience shows how much depends on independent regulators, clear compliance duties, arrangements for cross-border data governance, and public awareness work.

There are useful lessons here for Nepal. Copying a foreign model outright would not serve. What Nepal needs is a framework suited to its own setting, one that takes in international principles while dealing with domestic legal, institutional, and technological realities.

Data Protection and Privacy Laws in Nepal

Writing on technology law in Nepal has mostly dealt with cybercrime, electronic transactions, online fraud, and questions of digital evidence under the Electronic Transactions Act (2006) (Electronic Transactions Act, 2006; see also Cyber Bureau, 2023). That work has helped explain the criminal side of online activity, but digital data protection as a legal and governance subject in its own right has received little attention.

Nepal's legal architecture for data protection and privacy rests on a combination of constitutional guarantee and ordinary legislation, but the two levels do not yet form a coherent regulatory whole. Article 28 of the Constitution of Nepal (2015) establishes privacy as a fundamental right, declaring the privacy of a person's residence, property, documents, data, correspondence, and character to be inviolable except as provided by law (Constitution of Nepal, 2015, art. 28). This provision supplies the constitutional legitimacy on which any statutory privacy regime must build, yet it is declaratory rather than operational: it does not itself define the duties of data controllers, prescribe procedures for lawful processing, or establish an institution to monitor compliance. Whether constitutional protection translates into practical safeguards for individuals therefore depends entirely on the ordinary legislation enacted beneath it, and on the institutions available to enforce that legislation.

That operational function is carried, in principle, by the Individual Privacy Act, 2018, Nepal's main statute on personal privacy. The Act sets out obligations governing the collection, use, storage, and disclosure of personal information and requires a lawful basis for such processing (Individual Privacy Act, 2018). It thereby gives Article 28's general guarantee a measure of statutory substance, establishing baseline duties for those who handle personal data. However, the Act was drafted before many of today's digital challenges had fully emerged, and it does not offer a framework covering matters such as data controller and processor obligations, data breach notification, data portability, the right to erasure, privacy impact assessment, and independent regulatory supervision (General Data Protection Regulation [GDPR], 2016, arts. 5, 12–22, 25, 33, 35). It provides basic privacy protection, then, but falls short of what contemporary digital data governance requires.

The remaining gap is only partially filled by the Electronic Transactions Act, 2006, Nepal's principal cyber law, which contains provisions on unauthorized access, electronic records, and cyber offences (Electronic Transactions Act, 2006). Its orientation, though, is toward regulating cybercrime rather than protecting personal data (OECD, 2013), and having been drafted at an early stage of Nepal's digital development, it says little about present-day concerns such as algorithmic processing, cloud-based data storage, artificial intelligence, and the management of personal data at scale. The ETA thus remains a useful tool for addressing cyber offences, but it was never designed to function as a data protection statute and cannot serve as one. Taken together, the constitutional guarantee, the Individual Privacy Act, and the ETA form a foundational but incomplete architecture — one whose adequacy for modern digital governance the following sections examine in greater detail.

Critical Analysis of Legal and Institutional Gaps

The analysis of Nepal's existing digital data protection framework brings out several serious legal, institutional, and enforcement gaps. Nepal has put constitutional and statutory protections in place for privacy and personal information, yet the current framework is still not equal to the demands of modern digital data governance.

The main structural weaknesses found through the doctrinal legal analysis and the stakeholder interviews are summarized below:

Structural Weaknesses in Nepal's Data Protection Framework	Implications for the Digital Ecosystem
Absence of an Independent Data Protection Authority	Lack of regulatory oversight, compliance monitoring, and accountability mechanisms
Inadequate Regulation of Private Sector Data Processing	Unclear obligations regarding data collection, retention, sharing, and secondary use of personal data
Lack of Comprehensive Rules on Cross-Border Data Transfers	Uncertainty regarding jurisdiction, foreign data processing, and protection of personal information stored abroad
Weak Enforcement Mechanisms and Limited Penalties	Insufficient deterrence against data misuse, data breaches, and non-compliance by organizations

Each of these gaps is discussed in detail below.

Absence of a Centralized, Independent Data Protection Authority (DPA)

The lack of a central, independent Data Protection Authority is one of the largest institutional gaps that both the statutory analysis and the stakeholder interviews brought out. The Individual Privacy Act (2018) protects personal privacy in law, but people whose data protection rights are violated have to seek a remedy mainly through the ordinary courts, including civil proceedings (Electronic Transactions Act, 2006).

The Key Informant Interviews raised doubts about relying on the courts alone to settle complex data protection disputes. Legal practitioners and cyber law experts pointed out that these disputes usually turn on technical questions: handling digital evidence, cybersecurity weaknesses, server security, encryption practice, and automated data processing. Participants stressed that Nepal has no specialist regulator with the power to audit compliance, issue data protection guidelines, investigate violations, deal with complaints, and impose administrative sanctions on organizations that fail to comply (General Data Protection Regulation [GDPR], 2016, arts. 51–59).

Nepal, unlike countries that have an independent data protection authority, still has no institutional mechanism able to provide oversight in advance and hold the digital data ecosystem to account.

Inadequate Regulation of Private Sector Data Processing

Digital businesses in Nepal have grown quickly. Fintech companies, e-commerce platforms, online service providers, and other technology-based enterprises now collect and process much more personal information than before. The existing legal framework, though, does not set out detailed enough duties for the private bodies that collect, store, and process personal data.

The Individual Privacy Act (2018) applies to public and private bodies alike, yet it does not amount to a full regulatory framework built on the main principles of modern data protection: data minimization, purpose limitation, retention periods, privacy impact assessments, and the accountability duties of data controllers and processors (General Data Protection Regulation [GDPR], 2016, arts. 5, 24, 25, 35).

Many private organizations can therefore collect a great deal of personal information while saying little about how that data is processed, shared, kept, or deleted. Users give consent

by accepting long terms and conditions, usually without real understanding of, or control over, what happens to their information afterwards(Solove, 2008).

The Key Informant Interviews raised concerns about the absence of clear compliance duties for private sector data controllers. Legal practitioners and technology policy experts said that digital service providers, financial technology companies and online platforms among them, need stronger legal responsibilities for data collection, security measures, sharing practices, and data retention(Key Informant Interviews, 2026). They stressed that consent by itself is not enough unless it is backed by transparency requirements, accountability standards, and regulatory supervision that works.

Nepal therefore needs a fuller legal framework, one that spells out what private bodies are responsible for and secures responsible processing of personal information at every stage of the data lifecycle.

Lack of Comprehensive Rules on Cross-Border Data Transfers

Growing reliance on cloud computing, international digital platforms, and foreign technology infrastructure has created new difficulties in protecting and governing personal data that moves across national borders. Nepal's current digital data protection framework has no comprehensive provisions on cross-border data transfers.

Existing laws do not say clearly when personal information may be sent to a foreign jurisdiction, what foreign data processors are responsible for, or how the data of Nepali citizens held outside the country is to be protected. That leaves jurisdiction, accountability, and legal remedies uncertain whenever international data processing or a data breach is involved.

Without clear cross-border data governance mechanisms, law enforcement agencies, regulatory bodies, and the individuals affected all face difficulties when personal information sits on foreign servers or passes through foreign digital platforms. Sensitive data needs stronger safeguards still, since biometric, financial, and health-related information can affect both individual rights and national interests.

Cyber law experts and technology policy professionals interviewed for this article treat cross-border data governance as an emerging challenge for Nepal's digital ecosystem. They pointed out that many digital services running in Nepal depend on cloud infrastructure and service providers based abroad, which makes accountability and effective investigation hard when a breach happens outside Nepal's jurisdiction.

The interviews also point to a need for clear legal provisions on international data transfers, covering the standard of protection required, what data processors are responsible for, and how Nepal would cooperate with regulatory authorities in other countries.

Weak Enforcement Mechanisms and Limited Penalties

Data protection works only where enforcement is strong, remedies are real, and sanctions are proportionate enough to bring public and private bodies into line. Nepal's current legal framework offers limited enforcement and has no full system of administrative penalties for breaches of data protection duties(General Data Protection Regulation [GDPR], 2016, arts. 58 and 83).

As things stand, a person whose personal data rights are violated has to go to court for a remedy. That puts a heavy burden on the individual, who must first spot the violation, then gather digital evidence, then establish liability in a case that is often technically complex.

The penalties on the books also bear little relation to the harm that a large-scale data breach, an unauthorized disclosure, or the misuse of personal information can cause. For an organization holding large volumes of personal data, a small sanction gives little reason to invest in stronger cybersecurity and data governance practices (General Data Protection Regulation [GDPR], 2016, art. 83).

The Key Informant Interviews revealed doubts about whether current enforcement mechanisms can secure compliance with data protection duties at all. Legal practitioners and cyber law experts stressed that data protection depends on regulators supervising in advance, on mandatory breach notification, and on stronger institutional accountability, rather than on individual complaints and remedies after the fact (Key Informant Interviews, 2026).

The interviews also indicate that Nepal needs a modern enforcement framework with administrative sanctions, compliance monitoring, and grievance mechanisms that work, if personal data is to be protected in any meaningful way in the digital environment.

Discussion

The findings of this article show a wide gap between how fast Nepal has gone digital and how slowly an effective legal and institutional framework for protecting personal data has followed. Nepal recognizes privacy as a fundamental right and has passed laws such as the Individual Privacy Act (2018), but the framework in place is not enough for the difficult problems that today's digital technologies create

Nepal's current approach to data protection is largely reactive rather than preventive. Existing legal mechanisms deal with privacy violations after they have happened, while modern data protection frameworks put the weight on regulating in advance, on institutional accountability, and on compliance measured against risk (General Data Protection Regulation [GDPR], 2016, arts. 5, 24, and 25). That difference is part of a wider global shift, from treating privacy protection as a remedy for the individual to treating data governance as an institutional responsibility (Bygrave, 2002). In this regard, the author suggest following way forwards to address the concerns for a comprehensive data protection and privacy framework in Nepal.

Need for an Accountability-Based Framework

Article 28 of the Constitution of Nepal recognizes privacy, and that recognition is an important foundation for protecting individual autonomy and personal information. On its own, though, it cannot deliver effective protection without supporting legislation, regulatory institutions, and enforcement mechanisms. Nepal's existing framework is aimed mainly at controlling unauthorized disclosure or misuse of information, not at setting out full responsibilities for the bodies that collect and process personal data. Modern data protection regimes ask organizations to show accountability through transparency, security safeguards, internal compliance mechanisms, and responsible data management practices.

Nepal requires a competent Data Protection Authority, backed by legislation, with a mandate to enforce the accountability-based approach into effect. In absence of an independent

authority to ensure oversight, data protection still rests on individual complaints and traditional legal remedies, which are not well suited to privacy risks that run through a whole system. The existing authority, i.e. Nepal Police, is already too burdened with the regular work of peace and order. Considering the sensitive nature and technology requirements a separate body within the Nepal Police can also be an alternative to regulatory authority to enforce the much accountability based framework.

Adapting Comparative Lessons from International Data Protection Frameworks

Experience elsewhere shows that effective data protection takes more than recognizing privacy rights in law. It takes strong institutions, clear duties, and individual rights that can be enforced. The European Union's General Data Protection Regulation (GDPR) sets out a wide-ranging model, resting on accountability, transparency, data minimization, and individual control over personal information. Its independent supervisory authorities are proof of how much institutional oversight matters if compliance is to be secured.

India's Digital Personal Data Protection Act (2023) is a closer comparison for Nepal, another developing country going through rapid digital growth. With the ideas of Data Fiduciaries and Data Principals, and with enforcement through the Data Protection Board, India has tried to give digital data governance a clear structure.

In a similar manner, Japan, Singapore, and South Korea show in turn that digital transformation succeeds only where innovation and privacy protection are kept in balance. What stands out in these countries is regulatory capacity, readiness on cybersecurity, public awareness, and cross-border data governance that works (Act on the Protection of Personal Information [Japan], 2003; Personal Data Protection Act [Singapore], 2012; Personal Information Protection Act [South Korea], 2011).

Nepal can also draw its reference from the comparative practices of these nations, to learn and adapt the best practices that is suitable for Nepalese contexts and may help to address the concerns over here.

Implications for Nepal's Digital Governance

Government services, financial systems, and private platforms now depend heavily on personal data, and public trust has become essential to any successful digital transformation. Weak data protection mechanisms can lower citizens' confidence in digital services and raise the risk of identity theft, financial fraud, unauthorized data use, and privacy violations (OECD, 2013). Strengthening Nepal's data protection framework is therefore more than a matter of legal reform. Therefore, the government should read the urgency of the matter and prioritise the strengthening of data protection and privacy to ensure a viable and efficient digital governance and foster sustainable technological development.

Conclusion

This article concludes that Nepal's digital data protection framework is still at an early stage of development and faces serious legal, institutional, and enforcement challenges. Privacy is a fundamental right under the Constitution of Nepal (2015), and the Individual Privacy Act (2018) lays a basic legal foundation for protecting personal information. The two together are still not enough for how complicated the digital environment has become.

Several critical gaps emerge: no independent Data Protection Authority, weak regulation of private sector data processing, no comprehensive rules on cross-border data transfers, and poor enforcement. What the stakeholder interviews add is that the trouble does not stop at the wording of the legislation. It lies as much in the practical difficulty of implementation, in institutional capacity, and in accountability.

Digital governance, financial technology, and data-driven services keep expanding in Nepal, and protecting personal information has become essential both to holding public trust and to making that transformation a responsible one. A scattered and reactive approach to data protection leaves individuals and institutions open to growing risks of data misuse, security breaches, and loss of privacy.

What Nepal needs, then, is a comprehensive and modern data protection framework that moves past traditional privacy protection toward a model of governance based on accountability. Such a framework should set clear duties for data controllers, strengthen institutional oversight, and provide remedies and enforcement that work, in line with international standards and with Nepal's own legal and technological circumstances.

References

- Solove, D. J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. NYU press
- Westin, A. F. (1967). *Privacy and freedom*. Atheneum.
- Ministry of Communication and Information Technology. (2019). *Digital Nepal framework*. Government of Nepal.
- Nepal Rastra Bank. (2025). *Payment systems oversight report (2081/82)*. Government of Nepal.
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88.
- Council of Europe. (2018). *Convention for the protection of individuals with regard to automatic processing of personal data (CETS No. 223 / Convention 108+)*. Council of Europe Treaty Series.
- Constitution of Nepal. (2015). *Nepal Gazette*. Government of Nepal.
- Electronic Transactions Act, 2063. (2006). *Nepal Gazette*. Government of Nepal.
- Individual Privacy Act, 2075. (2018). *Nepal Gazette*. Government of Nepal.
- Ministry of Communication and Information Technology. (2019). *Digital Nepal framework*. Government of Nepal.
- Nepal Rastra Bank. (2025). *Payment systems oversight report (2081/82)*. Government of Nepal.

- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.
- European Data Protection Board. (2020). Guidelines 3/2019 on the processing of personal data through video devices (GDPR framework). European Union.
- Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.
- Organisation for Economic Co-operation and Development. (2013). *OECD guidelines on the protection of privacy and transborder flows of personal data*. OECD Publishing.
- World Bank. (2021). *Data protection and digital development: Global trends and policy challenges*. World Bank Group.
- Council of Europe. (2018). *Convention 108+: Convention for the protection of individuals with regard to the processing of personal data*. Council of Europe Treaty Series.
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220.
- Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *New York University Law Review*, 86(6), 1814–1894.
- Westin, A. F. (1967). *Privacy and freedom*. Atheneum.
- Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. NYU Press.
- Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.
- Bygrave, L. A. (2002). *Data protection law: Approaching its rationale, logic and limits*. Kluwer Law International.
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.
- Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). (2023). *The Gazette of India*. Ministry of Law and Justice, Government of India.
- Act on the Protection of Personal Information, Act No. 57 of 2003. (2020). *Personal Information Protection Commission*, Government of Japan.
- Personal Data Protection Act 2012 (Act No. 26 of 2012). (2012). *Singapore Statutes Online*. Government of Singapore.
- Personal Information Protection Act, Act No. 10465 of 2011. (2023). *Personal Information Protection Commission*, Government of South Korea.
- Cyber Bureau. (2023). *Annual cyber crime statistics report*. Nepal Police, Government of Nepal.

- Electronic Transactions Act, 2063 (2006). (2006). Nepal Gazette. Ministry of Communication and Information Technology, Government of Nepal.
- Individual Privacy Act, 2075 (2018). (2018). Nepal Gazette. Ministry of Law, Justice and Parliamentary Affairs, Government of Nepal.
- Organisation for Economic Co-operation and Development. (2013). OECD guidelines governing the protection of privacy and transborder flows of personal data. OECD Publishing.
- Legal Practitioners and Technology Policy Experts. (2026). Key informant interviews on digital privacy and legal frameworks [Unpublished primary data]. Kathmandu, Nepal.
- As observed during the Key Informant Interviews (2026) conducted in Kathmandu, legal experts noted a critical lack of specialized procedural guidelines for handling digital evidence.
- Bygrave, L. A. (2002). Data protection law: Approaching its rationale, logic and limits. Kluwer Law International.
- Act on the Protection of Personal Information (Act No. 57 of 2003). (2003). Personal Information Protection Commission, Japan.
- Personal Data Protection Act 2012 (No. 26 of 2012). (2012). Personal Data Protection Commission, Singapore.
- Personal Information Protection Act (Act No. 10465). (2011). Personal Information Protection Commission, Republic of Korea.
- Organisation for Economic Co-operation and Development. (2013). OECD guidelines governing the protection of privacy and transborder flows of personal data. OECD Publishing.
- Cyber Bureau, Nepal Police. (2025). Annual statistics on cyber crime and financial fraud in Nepal. Nepal Police Headquarters.
- Digital Rights Nepal. (2025). The state of digital rights and safety in Nepal 2025. Digital Rights Nepal.