DATA PRIVACY PRACTICES IN NEPAL'S MOBILE WALLET ECOSYSTEM: AN ANALYSIS

December 2025

Digital Rights Nepal

Writing and Editing
Sushmita Sharma

Publisher

Digital Rights Nepal

Supported By

Norway ICNL

Disclaimer

The views, analyses, and conclusions expressed in this publication are solely those of the author and are based on the author's independent research and ideas. They do not necessarily reflect the official position, views, or policies of Digital Rights Nepal (DRN).

Executive Summary

Nepal's digital payment landscape has undergone rapid transformation with significant financial inclusion. Mobile wallets like eSewa, Khalti, IME Pay, Moru, and PrabhuPay are now widely used for everyday transactions. These platforms benefits millions of users making them vital to Nepal's digital economy. However, this growth has outpaced the development of strong data privacy and protection safeguards.

This policy paper examines the data privacy practices of the existing major mobile wallets within the existing constitutional, legal, and regulatory framework. The study is based on the desk review of publicly available policies of major wallet service providers and key regulatory instruments issued by Nepal Rastra Bank and is analyzed based on the six key core areas: data collection and purpose limitation; consent and transparency; data storage and retention; third-party data sharing and cross-border transfers; security safeguards and breach response; and user rights and grievance redress mechanisms.

The findings shows that the mobile wallet providers though mostly comply with NRB's licensing, operational, and consumer-protection requirements the substantive data privacy protections remain weak. Most often, data collection is done more than what is required, consent mechanisms are bundled and non-granular, and transparency regarding data retention, third-party processing, and cross-border data flows is limited. Security commitments are generally expressed in broad terms without clear breach-notification obligations, and users lack meaningful rights to access, delete, or control their personal data. As a result, privacy is treated primarily as a compliance and risk-management issue rather than as an enforceable user right. These gaps, in additional to consumer protection risks, also invites a longer-term threat to trust, regulatory credibility, and the sustainability of Nepal's digital payments ecosystem.

The analysis highlights the limitations of relying solely on sector-specific financial regulation to effectively manage current data protection challenges. To strengthen privacy governance in Nepal's digital payment ecosystem, coordinated action is required. This includes robust regulatory directives from the Nepal Rastra Bank (NRB), the implementation of a comprehensive personal data protection law, the establishment of clearer institutional accountability, and the adoption of improved privacy practices by mobile wallet providers. In the absence of such measures, the consumers will be continually exposed to the increasing data related risks which may have unforeseen consequences.

1. Introduction

Digital payment services are expanding rapidly in Nepal. Consumers are using mobile wallets to pay bills, send remittances, merchant payments, government services, and people to people transfers. There are several digital wallets operating in the Nepali market. For example: eSewa, Khalti, IME Pay, Moru, PrabhuPay and others. As per Payment System Oversight Report (NRB, FY 2023/24), the number of digital wallet users increased from 6.27 million in 2020 to over 23.4 million by mid-2024, with a total wallet transaction value reaching NPR 302.69 billion. This shows broad adoption across the population and the growing role of digital payments in daily financial activity. It is reported that there are around 10 million registered wallet users currently using digital payments services. This digitization has changed the practice of how people pay, transfer, and manage money. The table below summarizes the adoption of mobile wallets in Nepal, based on available user data.

Table 1-1 Access on Payment Systems

S.N.	Particulars	Mid-August 2020	Mid-May, 2024	% Change
1	Wallet Users	6,274,129	22,615,122	260.45
2	Debit Cards	7,437,602	12,789,656	71.96
3	Credit Cards	164,386	286,253	74.13
4	Mobile Banking Customers	11,464,867	23,797,680	107.57
5	Internet Banking Customers	1,045,558	1,938,888	85.44
6	connectIPS Users	162,117	1,251,440	671.94

Alongside these benefits, however, there are growing concerns around data privacy issues and protection of users' personal information. It is because while accessing these services, the user must submit their personal data and information, comply with Know Your Customer (KYC) processes, and depend on the platform to safeguard their sensitive data. In the process, these mobile wallets are gathering their personal sensitive information without any transparency and security assurances. So, there may be a risk that their information can be misused by these service providers thereby increasing the vulnerability of the users. In practice, users often have limited visibility into how their data is collected, stored, shared, or retained. They accept the terms and conditions without understanding data implications, limiting users' ability to exercise informed choice or control over their personal information.

These types of weak privacy safeguards can increase risk of digital fraud, phishing attacks, identity theft, and unauthorized transactions (World Bank, 2020; OECD, 2013). But Nepal does not yet have a comprehensive data protection law or a dedicated regulatory mechanism to govern personal data processing in digital financial services. Nepal currently regulates data privacy through the Electronic Transactions Act (ETA 2063), National Penal Code provisions on privacy, Consumer Protection Act, and Banking and NRB directives. But these instruments do not adequately define and safeguard user rights and uphold their privacy. So, it has become important to understand the data privacy practices of mobile wallet providers in Nepal in order to introduce and enforce stronger data safeguards.

2. Methodology:

This study has employed qualitative research techniques with a desk review done from November-December 2025 and is based on the publicly available documents of the eSewa, Khalti, IME Pay, Moru, Qpay, CellPay, NamastePay and PrabhuPay. The documents include their privacy policies, terms and conditions, grievance pages, app-store privacy disclosures, NRB's Unified Directives (Payment Systems), IT & Cybersecurity Guidelines, and Anti-Money Laundering (AML) or KYC requirements. The analysis is made based on the six privacy indicators: (a) Data Collection and Purpose Limitation, (b) Consent and Transparency, (c) Data Storage and Retention, (d) Third-Party Sharing and Cross-Border Data Flow, (e) Security Safeguards and Breach Response, and (f) User Rights and Grievance Redress Mechanisms. Likewise, NRB's key regulatory instruments, like Payment and Settlement Bylaw (NRB), NRB Unified Directives 2022 - 24 (Payment Systems), IT and Cybersecurity Guidelines for BFIs and PSP/PSOs, Guidelines on Electronic Payment and QR Code Standardization, and Anti-Money Laundering (AML) or Combating the Financing of Terrorism (CFT) Requirements for Payment Service Providers (PSPs), were also examined.

3. Constitutional and legal provisions on data privacy in Nepal

Data privacy practices in Nepal's Mobile Wallet Ecosystem are regulated by privacy and data protection laws, policies, guidelines, and directives of Nepal.

3.1. Constitutional and legal protection of privacy and data protection in Nepal

Privacy and data protection are enshrined in the Constitution of Nepal. Article 28 makes privacy inviolable except in accordance with law, and it is broad enough to cover modern digital environments because it explicitly includes documents, data, and correspondence among the protected interests. As a state party to different human rights instruments like the International Covenant on Civil and Political Rights (ICCPR), Universal Declaration of Human Rights (UDHR), and Convention on the Rights of the Child (CRC), Nepal's international commitments are also vital in relation to privacy and individuals' data protection. Taken together, these constitutional and international commitments establish a normative legal standard that requires data-processing practices to be lawful, necessary, proportionate, and justified, and prohibit arbitrary interference through excessive data collection, opaque profiling, or unjustified data sharing. However, as discussed in subsequent sections, the extent to which these standards are reflected in actual data-handling practices within the digital payment ecosystem remains limited and uneven.

The constitutionally protected right is operationalized through the Privacy Act, 2075 (2018). Though the Act is mainly focused on the privacy perspectives, it also regulates the ability of business entities like mobile wallets for collecting and processing personal information.

The Privacy Act matters in at least three ways:

- Purpose limitation: Wallet providers should be able to justify why each category of data is collected and how it is used (e.g., onboarding/KYC, transaction execution, fraud monitoring, dispute resolution, regulatory reporting) as per the with Sections 5, 7 and 8 of the Privacy Act, 2075 (2018), which restrict the collection and use of personal information to lawful, necessary, and specified purposes.

- Disclosure controls: Sharing personal information with third parties (vendors, affiliates, credit scoring partners, marketing platforms, or cross-border processors) should have a clear legal/consent basis and safeguards, and be subject to appropriate safeguards, in accordance with Sections 5, 8, and 9 of the Privacy Act, 2075 (2018), which restrict unauthorized disclosure and impose a duty of confidentiality on data handlers.

- Institutional duty of care: Institutions handling personal data have an affirmative obligation to protect individuals against privacy harms under Sections 3 (protection of privacy), 9 (confidentiality obligation), and 12 (liability for privacy breach) of the Privacy Act, 2075 (2018). In the digital payments sector, this duty is regulated through Nepal Rastra Bank's cybersecurity, operational, and supervisory requirements for licensed PSPs and PSOs.

Nepal's Electronic Transactions Act (ETA), 2063 (2008) is a foundational cyber law that recognizes electronic records and regulates cyber offenses. While not a dedicated data protection acts in Nepal, it is often invoked for unlawful digital activities and provides a legal environment for trust in electronic transactions and penalties for certain cyber-related misconduct. ETA's relevance is practical as it is important to strengthen the enforcement ecosystem against hacking, unauthorized access, and certain forms of misuse of electronic records. This complements sector rules by providing a broader statutory basis to treat serious digital misconduct as an offense, beyond contractual breaches.

The constitutional recognition of privacy under Article 28 of the Constitution, together with its statutory operationalization through the Privacy Act, 2075 (2018), is important for the mobile wallet ecosystem because e-wallet services inherently depend on continuous collection and processing of personal and transactional data (identity/KYC information, device identifiers, location or IP logs, transaction histories, merchant details, etc.). In principle, any interference with privacy or misuse/disclosure of data must have a legal basis and satisfy constitutional standards of legality and justification.

3.2. Sector-specific policy provisions/framework:

Some sector-specific laws, policies, and directives are more specific to regulate data privacy within mobile wallets operation. As mobile wallets are part of the national payment system, the most direct regulatory driver for privacy/security compliance is the payment system regulatory framework under Nepal Rastra Bank (NRB).

a) Payment and Settlement Act, 2075 (2019):

The Payment and Settlement Act, 2075 establishes NRB's legal basis to regulate payment systems and participants. It underpins licensing, supervision, and system integrity expectations (including operational, governance, and risk controls). This Act is important as the sector enabling law that makes NRB directives and guidelines binding for payment institutions [Payment Service Providers (PSPs)/Payment Service Operators (PSOs)], including wallet operators.

b) "Unified Directives" for payment-system licensees 2081:

NRB's Payment System related Unified Directives (2081) are highly relevant because they translate oversight into concrete operational duties for licensed payment institutions, including e-wallet providers.

Though the directives are not framed as a data privacy policies/guideline, they shape privacy outcomes through risk management, security, governance, reporting, and consumer protection requirements. For example, the directives include a dedicated provision on information/data reporting, requiring licensed institutions to submit specified information within set timeframes through NRB's supervisory/reporting systems. This is significant because:

a) It formalizes data flow from wallet operators to the regulator (regulatory access to operational and transactional statistics);

b) It increases accountability (audit trails, standardized reporting formats);

c) It creates compliance pressure to maintain accurate, secure, and well-governed data infrastructure.

From a data privacy-practice perspective, these directives give mandates to the wallet operators where they must design internal controls around (i) what data is collected, (ii) how it is stored, (iii) who can access it, and (iv) how it is reported - because reporting obligations are ongoing and supervisory scrutiny is expected.

c) Licensing policy for payment-related institutions:

NRB also issues policy instruments governing permission/licensing for payment-related activities (including amendments). These instruments frame who can operate, under what conditions, and often embed baseline governance and compliance expectations for PSPs/PSOs (including wallet providers).

d) NRB cyber resilience and security expectations: protecting confidentiality, integrity, and availability

A core part of data privacy in payment systems is security. The weak security turns data privacy rights responsibility into theoretical promises. NRB's Cyber Resilience Guidelines (issued for licensed institutions) set expectations on governance, cyber risk culture, training, resilience testing, and recovery planning. Crucially for wallet ecosystems, these guidelines emphasize:

- Institution-wide responsibilities (board and senior management accountability, training, role-based controls);
- Data protection and recovery - including the need to protect and recover critical data (not only transactional data but also other sensitive operational data) and to ensure accurate recovery following breaches/disruptions.
- This connects privacy to enforceable operational standards: if a wallet operator fails cyber resilience expectations, it increases breach risks and undermines constitutional privacy protections in practice.

e) NRB oversight reports: data privacy and security as supervisory priorities

NRB's Payment Systems Oversight Report (2080/81 – 2023/2024) indicates that NRB's payment supervision increasingly focuses on system safety, integrity, and oversight of licensed PSPs/PSOs where data security and privacy are part of the ecosystem risk landscape. In a policy analysis, data privacy in wallet ecosystems is not only a rights issue but also a financial stability and consumer trust issue in NRB's oversight logic.

4. Key Discussion:

4.1. Data Collection and Purpose Limitation:

As per the Unified Directives of NRB, Payment Service Providers (PSPs) only need to collect customer data that are necessary for lawful purposes, including Know Your Customer (KYC) verification, AML/CFT compliance, and payment processing, and to avoid unnecessary or excessive data collection (Nepal Rastra Bank, 2024). In practice, however, the a review of privacy policies indicate that Nepalese mobile wallets routinely collect data beyond these minimum requirements and rely on broadly framed purposes that weaken the principle of purpose limitation.

eSewa, a licensed PSP, collects not only KYC information, and transaction records, technical data such as device identifiers through cookies and, in some cases, location data (eSewa Ltd., 2010). While eSewa's publicly available privacy policy and an information-security section outlines general categories of personal data collection and use, such as "service improvement," "analytics," "business enhancement," "processing the transactions," "periodic emails," and "promotional actitivies", it does so in broad and loosely defined terms that weaken the principle of purpose limitation. The policy does not distinguish between mandatory regulatory data and optional or value-added data, nor does it specify limits on reuse (eSewa Ltd., 2010). The absence of clear limitations on data reuse, defined retention periods, or purpose-specific safeguards indicates that data initially collected for lawful payment services may be repurposed in ways that dilute the principle of purpose limitation envisaged under Nepal Rastra Bank's regulatory framework.

Khalti and IME Pay, now operating as "Khalti by IME," show comparatively stronger regulatory alignment by providing more structured explanations of data collection and explicitly acknowledging disclosure obligations to NRB and other authorities. Along with detailed description of data collection and how that data is used, Khalti by IME also detailed out the purpose limitation of such collected data. The policy lists legitimate functional purposes such as facilitating transactions, verifying identify, complying with KYC/AML/CTF, detecting fraud, and providing customer support. Nevertheless, their privacy policies continue to rely on expansive concepts such as "improving user experience", "internal audits," and "service optimisation". These categories are not accompanied by clear explanations of how long personal data is used for such purposes, what specific activities are covered under analytics or optimisation, or what limits apply to secondary use. As a result, these broadly framed purposes allow extended and possibly indefinite use of personal data beyond the original transaction context (Khalti by IME, 2024).

Moru and PrabhuPay also collect standard KYC and device related information but provide minimal justification for the scope of data collected or its linkage to specific, clearly defined purposes. (ParbhuPay, 2019) CellPay and NamastePay's privacy policies also has limited clarity on how data collection is restricted to what is strictly necessary. Although QPay offers somewhat clearer purpose statements, it still doesn't fully demonstrate the strict data-minimization practices (QPay, 2024).

Across all reviewed wallets, minimum KYC compliance is generally met. However, none of them reflect rigorous data minimization or narrowly defined purpose limitation in practice. The generic and vague purpose statements reflect a systemic weakness in Nepal's digital payment governance, where regulatory compliance requirements coexist with weak safeguards against secondary data usage, function creep, and extended data exploitation.

4.2. Consent and Transparency

Transparency is a core component of Nepal Rastra Bank's (NRB) consumer-protection framework. It requires Payment Service Providers (PSPs) to clearly inform users of applicable terms, charges, risks, and responsibilities before service use (Nepal Rastra Bank, 2024b). Despite this requirement, the findings indicate that consent mechanisms across Nepal's mobile wallet ecosystem is largely procedural rather than rights-based.

Most wallet providers depend on bundled consent models. They require users to accept all terms and privacy conditions as a prerequisite for accessing services. One of the service providers, eSewa, for example, require users to agree to a single set of terms covering multiple forms of data collection and processing. It does not offer a separate or granular consent options for different forms of data processing. Its privacy policy, originally published in 2010, provides limited information about analytics, tracking technologies, and how long data is kept. This limits users' ability to provide informed consent and weakens transparency in practice. (eSewa Ltd., 2010)

Khalti by IME Pay seem to have comparatively stronger transparency because they publish more detailed privacy policies. They also clearly acknowledge that personal data may be disclosed to NRB and other authorized government bodies. Khalti's dormant-wallet policy also is in line with the NRB's consumer protection objectives by reducing the risk of unauthorized access to inactive accounts (Khalti, 2024). However, despite these improvements, Khalti also uses broad and non-specific consent language such as "service optimisation" or "user experience improvement" without providing purpose specific or revocable consent options.

In contrast, Moru provides minimal transparency and explicitly shifts responsibility for third-party platforms to users, weakening institutional accountability (Moru, 2024). It does not specify how users can review or control data sharing with these third parties, nor does it describe contractual or technical safeguards to ensure data protection once shared. PrabhuPay's privacy policy remains generic, and transparency concerns are heightened by NRB's notice indicating that its PSP license was not renewed during the review period (Nepal Rastra Bank, 2025). NamastePay's privacy policy provides relatively clearer disclosures on data sharing, retention, and lawful access, including explicit references to third-party service providers and law-enforcement requirement. However, while the policy demonstrates stronger transparency in form, user consent remains largely implied through service use rather than obtained through granular or purpose-specific mechanisms.

Overall, consent across all reviewed platforms is typically bundled, non-granular, and non-revocable. Users are not provided with choices and options regarding different categories of data processing, nor are they provided with clear mechanisms to withdraw consent once services are activated. This authoritative "take it or leave-it" consent models undermine user independence and highlights the absence of enforceable, rights-based transparency standards within NRB's current regulatory framework.

4.3. Data Storage and Retention:

The review of data storage and retention practices shows a significant disconnect between Nepal Rastra Bank's (NRB) regulatory requirements and the level of transparency demonstrated by mobile wallet providers. NRB requires Payment Service Providers (PSPs) to securely store customer data, retain transaction and KYC records for AML/CFT purposes, commonly for a minimum period of five years and ensure the confidentiality and integrity of stored information (Nepal Rastra Bank, 2024a). Despite these obligations, the findings show a consistent lack of publicly available information regarding how mobile wallets store and retain user data. For example, NamastePay mentioned in its privacy policy that the collected data won't be kept longer than needed, but the time of such need is not specified.

While some wallet providers have disclosed limited information on data storage and retention, overall transparency remains uneven. For instance, PrabhuPay explicitly states that user data is stored and processed within Nepal, and that information of users located abroad is transferred to and processed domestically. Similarly, Khalti specifies a minimum data retention period of ten years in line with regulatory requirements. However, across providers, critical details remain unclear, including post-retention deletion practices, data anonymisation standards, backup storage locations, and safeguards governing third-party or cross-border processing. The absence of comprehensive and standardized disclosures continues to limit users' ability to assess long-term data risks and jurisdictional exposure. Although providers such as eSewa and Khalti broadly state that user data is stored "securely," these assurances are not supported by technical or procedural details, such as encryption standards, access controls, data segregation, or deletion and anonymization practices. The absence of information on post closure data handling further leaves users uncertain as to whether their personal and financial data is retained indefinitely.

The lack of transparency shows a significant privacy concern within Nepal's digital payment system. The indefinite or unspecified retention of sensitive KYC documents increases the potential for data breaches, while undisclosed cross-border storage poses the jurisdictional and regulatory risks. Collectively, these practices undermine the widely recognized principles of data minimization and storage limitation and weaken user trust in digital financial services (OECD, 2013).

4.4. Third-Party Sharing and Cross-Border Data Flow

The review of third-party data sharing and cross-border data flows within Nepal's mobile wallet ecosystem shows a significant transparency and accountability gap. According to the Nepal Rastra Bank (NRB) requirements, Payment Service Providers (PSPs) are expected to disclose third-party involvement as a part of operational risk management and, to ensure that customer data is neither shared nor processed externally without appropriate safeguards (Nepal Rastra Bank, 2024a). However, the review finds that most major wallets such as eSewa, Khalti/IME Pay, and PrabhuPay state in general terms that user data may be shared with "service providers," "vendors," or "business partners," without specifying these entities or clarifying their roles, purposes, or scope of access.

None of the reviewed platforms clearly disclose whether user data is stored or processed outside Nepal, nor do they provide information on cross-border data-transfer safeguards, contractual controls, or applicable jurisdictions. Moru adopts a particularly concerning approach by explicitly disclaiming responsibility for the privacy practices of third-party platforms, effectively transferring data-protection risks to users and undermining institutional accountability (Moru, 2024). QPay demonstrates comparatively stronger disclosures and references adherence to international data-protection principles; however, its transparency remains incomplete and does not comprehensively address third-party processing arrangements or cross-border data flows (QPay, 2024).

Overall, these foggy data-sharing practices prevent users from determining whether their personal and financial data is hosted on foreign cloud infrastructure, integrated into commercial analytics ecosystems, or subject to profiling and secondary use. While platforms such as eSewa, Khalti/IME Pay, and PrabhuPay acknowledge regulatory data sharing with NRB, they remain largely silent on commercial data-sharing arrangements. This lack of disclosure about third-party partners and foreign data transfers is a major systemic problem in Nepal's mobile wallet system. This situation exposes users to privacy and jurisdictional risks that is not in the reach of the users.

4.5. Security Safeguards and Breach Response

The review of security safeguards and breach response mechanisms shows a significant accountability gap between Nepal Rastra Bank's (NRB) cybersecurity requirements and the publicly disclosed practices of mobile wallet providers. NRB requires that Payment Service Providers (PSPs) to comply with IT and cybersecurity guidelines, implement multi-layered security controls that includes encryption, multi-factor authentication, and audit trails. This is to ensure the confidentiality and integrity of customer data, and report significant cybersecurity incidents to the regulator (Nepal Rastra Bank, 2024b).

Despite these obligations, the privacy policies and public disclosures of all reviewed wallets rely heavily on generic statements such as "industry-standard security" or "multi-layer controls," without verifying these claims through concrete technical or procedural details. None of the platforms disclose encryption standards, penetration-testing practices, security audit outcomes, or incident-response timelines, nor do they clarify whether users would be entitled to compensation or remedial support in the event of a data breach.

Concerns regarding weak security governance are reinforced by publicly reported data-compromise incidents involving major mobile wallet providers in Nepal. In November 2024, a former employee of Khalti was arrested for allegedly selling customers' personal data, including phone numbers and transaction-related information, to criminal groups, highlighting serious gaps in internal access controls and insider-risk management (Kantipur, 2024). This incident demonstrates that data-privacy risks in Nepal's mobile wallet ecosystem are not limited to external cyberattacks but also arise from insufficient institutional safeguards against internal misuse.

Similarly, eSewa has previously been linked to reported data exposure incidents. In 2020, a hacker publicly released personal details of multiple eSewa users, including account credentials, raising concerns about data-security practices, breach detection, and user-notification mechanisms (Republica, 2020). Although the company disputed the scale of the breach, the incident underscored the absence of transparent breach-notification procedures and independent verification mechanisms within Nepal's digital payment ecosystem.

More critically, none of the reviewed wallets publishes a clear breach-notification policy explaining how affected users would be informed, the timeframe for disclosure, or the measures that would be taken to mitigate post-breach harms. As a result, Nepal's mobile wallet ecosystem operates largely under a model of security by assumption rather than security by accountability. The absence of transparent, verifiable information on security controls and breach-response procedures leaves users uninformed and unprotected, significantly weakening consumer trust and undermining NRB's broader objectives of system integrity and financial consumer protection (World Bank, 2020).

4.6. User Rights and Grievance Redress Mechanisms

Nepal Rastra Bank (NRB) requires Payment Service Providers (PSPs) to maintain consumer complaint-handling mechanisms and encourages linkage with the NRB-operated Gunaso Portal as part of its financial consumer-protection framework (Nepal Rastra Bank, 2024b). Despite these requirements, the review shows that Nepal's mobile wallet ecosystem remains largely service-oriented rather than rights-based.

Wallets such as eSewa and Khalti/IME Pay provide customer support mechanisms and, in some instances, reference NRB's grievance system. But these mechanisms are basically designed to resolve transactional or service delivery issues rather than to address data protection or privacy violations. Moru and PrabhuPay similarly maintain complaint channels, but these focus narrowly on transaction failures, account issues, or payment disputes, with little recognition of privacy-related grievances. As a result, privacy concerns are largely treated as operational matters rather than as enforceable user rights.

Across all reviewed platforms, users are not afforded fundamental data rights commonly recognized under global privacy standards. These include the right to access or download personal data, request permanent deletion, view records of third-party data sharing, or object to profiling and marketing uses. Privacy specific grievance pathways are either absent or poorly expressed, with only limited and inconsistent references to the NRB Gunaso Portal.

Users have no meaningful or enforceable privacy rights within Nepal's mobile wallet ecosystem. Grievance mechanisms function primarily as customer-service tools rather than as rights-based remedies, significantly weakening user agency, transparency, and institutional accountability in the digital payments sector

.

Overall, while NRB's current directives establish a necessary procedural baseline through licensing and complaint-handling requirements. But it remains insufficient to ensure robust, rights-based data-privacy protection. The core standards relating to user rights such as access, deletion, objection, and transparency are largely absent. This highlights the structural limitations of relying solely on sector-specific financial regulation to address contemporary data protection challenges in digital financial services.

5. Regulatory expectations under NRB's unified directives and oversight framework

Nepal Rastra Bank (Nepal Rastra Bank) establishes a clear set of expectations for Payment Service Providers (PSPs) and Payment System Operators (PSOs) through its Bhuktani Pranali Sambandhi Akikrit Nirdeshan-2081(Unified Directives – Payment Systems), oversight reports, and IT/cybersecurity guidance. It requires to ensure the confidentiality and integrity of customer and payment data, requiring PSPs to protect personal and financial information from unauthorized access, misuse, or disclosure. PSPs are also expected to provide clear and accessible "Most Important Terms and Conditions (MITC)", informing users in simple language about applicable charges, key responsibilities, operational risks, and dispute-resolution mechanisms prior to service use. In addition, NRB requires them to comply with IT and cybersecurity controls, including encryption, authentication mechanisms,

audit logs, backup and disaster recovery arrangements, and compulsory reporting of major incidents to the regulator. Record keeping and retention of transaction and KYC data for regulatory and AML/CFT purposes commonly for a minimum of five years is another requirement alongside consumer protection requirements (internal complaint-handling systems and linkage to NRB's Financial Consumer Protection (Gunaso) Portal). Finally, PSPs are required to operate strictly under a valid and current license, appearing on NRB's official lists and complying with renewal conditions and supervisory directives.

5.1. Overall compliance trends among licensed PSPs

A desk review of publicly available materials including privacy policies, terms and conditions, customer support pages, and app-store disclosures shows that most of the licensed PSPs in Nepal demonstrate formal alignment with NRB's licensing and baseline consumer-protection framework. Major wallets such as eSewa, Khalti, IME Pay, Moru, PrabhuPay, CellPay, NamastePay, and QPay have been listed as licensed PSPs by NRB during the review period, and several explicitly reference NRB or other regulatory authorities within their dispute-resolution or grievance-handling provisions. This indicates that licensing, basic security assurances, and the existence of complaint channels are now normalized features within Nepal's digital payments ecosystem.

5.2. Variation in substantive transparency and privacy protection

Despite this formal alignment, the depth and quality of privacy transparency and rights-based protection vary significantly across providers. Khalti/IME Pay and QPay have published comparatively more detailed privacy and dispute policies, with Khalti also maintaining an inactive or dormant wallet treatment policy that aligns with NRB's emphasis on risk reduction and consumer protection. By contrast, eSewa and CellPay largely meet minimum regulatory expectations on licensing and security commitments. But, their publicly available privacy documentation remains high-level or dated and does not clearly explain data retention schedules, third-party data-sharing arrangements, or cross-border data flows in a user-friendly manner. These gaps limit users' ability to understand the full lifecycle of their personal and financial data.

5.3. Heightened concerns among selected providers

Moru, and PrabhuPay illustrate additional regulatory and transparency concerns. Moru visibly aligns with NRB's structural requirements by identifying itself as a PSP, linking to grievance mechanisms, and referencing the NRB Gunaso Portal. However, its privacy policy is brief and explicitly shifts responsibility for third-party platforms to users, without setting out clear rules on data retention, localization, or breach notification. PrabhuPay presents a distinct regulatory risk case. Although it maintains a generic privacy policy and links to NRB grievance processes, NRB has issued a notice indicating that Prabhu Technology Pvt. Ltd.'s PSP license has not been renewed. This shows how regulatory status and the credibility of consumer data-protection assurances can change over time.

5.4. Synthesis and regulatory implication

Overall, the comparative analysis demonstrates that NRB's current directives are necessary but not sufficient to ensure robust and consistent privacy practices across Nepal's mobile wallet ecosystem. Licensing, high-level security language, and basic dispute mechanisms are widely present. But there is no uniform or enforceable standard on core privacy dimensions such as purpose limitation, granular consent, data-retention schedules, cross-border data transfers, breach notification, or user rights (access, correction, deletion, objection). This regulatory gap reinforces the need for NRB to adopt a dedicated privacy and data-protection framework for payment services, complemented by the enactment of a comprehensive Personal Data Protection Act. This will bring in all the digital-finance stakeholders to a clear, rights-based, and enforceable obligations.

6. Key Findings and Policy Recommendations:

This study finds that Nepal's mobile wallet ecosystem has expanded rapidly in terms of adoption and usage. However, it remains institutionally weak in embedding robust data protection and privacy safeguards. The key findings are as follows:

- **Compliance-oriented rather than rights-based governance**

Across all core privacy indicators i.e. data collection and purpose limitation, consent and transparency, data storage and retention, third-party data sharing, security safeguards, and user rights, the prevailing approach among Payment Service Providers (PSPs) remains minimal and compliance-driven, rather than rights-based and accountable.

- **Excessive data collection and weak purpose limitation**

While most wallets comply with Nepal Rastra Bank's (NRB) baseline requirements for KYC, AML/CFT, and transaction processing, they routinely collect data beyond what is strictly necessary. Broad and vague purposes such as "service improvement" or "analytics" are commonly used, undermining the principle of purpose limitation.

- **Bundled and non-negotiable consent mechanisms**

Consent across platforms is typically bundled and non-granular, offering users limited choice or control over different categories of data processing and providing no meaningful mechanisms for consent withdrawal.

- **Opacity in data storage, retention, and cross-border data flows**

While some wallet providers have begun to disclose limited information on data storage and retention, overall transparency remains uneven. This lack of transparency prevents users from assessing data longevity and jurisdictional risks.

- **Non-transparent third-party data sharing**

Although wallets acknowledge sharing data with third parties, disclosures remain generic and do not identify partners, processing roles, or safeguards. This opacity makes it impossible to assess risks related to profiling, commercial exploitation, or secondary data use.

- **Weak security accountability and absence of breach transparency**

While all wallets claim adherence to "industry-standard security," none publishes breach-notification policies, incident-response timelines, or user remediation mechanisms, leaving users uninformed in the event of a data compromise.

- **Absence of enforceable user rights**

User rights are largely absent in practice. Complaint mechanisms focus on transactional issues rather than privacy violations, and users lack basic rights such as access to personal data, data portability, deletion, consent withdrawal, or objection to profiling and marketing practices.

- **Structural regulatory deficit**

Collectively, these gaps indicate a systemic regulatory weakness rather than isolated provider failures. NRB's current directives establish a necessary operational baseline but do not adequately articulate privacy as an enforceable consumer right within Nepal's digital payments ecosystem.

6.1. Policy Recommendations

a) For Nepal Rastra Bank (NRB):

To address the identified gaps, the following regulatory measures are recommended for Nepal Rastra Bank.

- Introduce a dedicated Privacy and Data Protection Directive for PSPs and PSOs:

NRB should issue a binding Privacy and Data Protection Directive as a mandatory supplement to the existing Unified Directives on Payment Systems, explicitly addressing data protection obligations in digital payment services.

- Mandate uniform privacy and transparency standards across all licensed entities

The directive should require standardized disclosures covering:

- purposes of data collection and processing,
- consent standards and limitations,
- data-retention and deletion rules,
- *cross-border data-transfer protocols and safeguards,*
- *purpose limitation and minimal data-collection principles.*

Publicly accessible privacy notices should be mandatory to ensure that users can easily understand how their personal and financial data is handled.

- Introduce mandatory data classification and enhanced protection protocols:

NRB should require PSPs to classify data based on sensitivity and apply heightened safeguards for sensitive personal and financial data, including KYC documents, biometric identifiers, transaction histories, and authentication credentials. This should include proportionate access controls, encryption standards, and internal data-handling restrictions.

- Require annual independent privacy and data-protection audits:

PSPs should be subject to mandatory, independent privacy audits on an annual basis. NRB should require the publication of non-confidential audit summaries to enhance transparency, regulatory accountability, and consumer trust.

• Establish clear and enforceable breach-notification requirements:
NRB should mandate PSPs to notify both the regulator and affected users within a defined timeframe following any personal-data or cybersecurity breach. This would replace reliance on vague "industry-standard security" claims with measurable and enforceable accountability.
• Standardize MITC and privacy-policy templates:
NRB should enforce mandatory MITC and privacy-policy templates, written in simple Nepali and English, to ensure consistency, accessibility, and comparability across mobile wallet providers.
• Strengthen oversight of privacy-related complaints:
PSPs should be required to separately record, categorize, and report privacy- and data-protection–related complaints, distinct from transactional disputes. This would enable NRB to identify systemic privacy risks and supervisory gaps within the digital payments' ecosystem.

b) For the Government of Nepal:

Enact a Comprehensive, Cross-Sectoral Personal Data Protection Act (PDPA)

• Prioritize the enactment of a unified Personal Data Protection Act applicable across all sectors, including digital financial services, telecommunications, health, education, and emerging data-driven services.
• Replace the current fragmented and sector-specific regulatory approach with a single, coherent statutory framework to ensure legal certainty, consistency, and equal protection of personal data.
• Align the PDPA with internationally recognized privacy principles (such as purpose limitation, data minimization, and accountability) while grounding it firmly in Nepal's constitutional right to privacy and domestic legal context.

c) For the Government of Nepal:

Enact a Comprehensive, Cross-Sectoral Personal Data Protection Act (PDPA)

• Prioritize the enactment of a unified Personal Data Protection Act applicable across all sectors, including digital financial services, telecommunications, health, education, and emerging data-driven services.
• Replace the current fragmented and sector-specific regulatory approach with a single, coherent statutory framework to ensure legal certainty, consistency, and equal protection of personal data.
• Align the PDPA with internationally recognized privacy principles (such as purpose limitation, data minimization, and accountability) while grounding it firmly in Nepal's constitutional right to privacy and domestic legal context.

• **Guarantee Enforceable Data Subject Rights**
• Explicitly recognize and protect core user rights under the PDPA, including:
the right to access personal data held by public and private entities;
the right to rectification of inaccurate or incomplete data;
the right to erasure where data processing is no longer lawful or necessary;
the right to withdraw consent without adverse consequences;
the right to object to specific forms of processing, including profiling, targeted advertising, and marketing.
• Ensure that these rights are legally enforceable through clear remedies, complaint mechanisms, and defined timelines for compliance by data controllers and processors.

• **Establish an Independent and Empowered Data Protection Authority (DPA)**
• Establish an autonomous Data Protection Authority through legislation, ensuring functional, financial, and decision-making independence.
• Empower the DPA with authority to:
audit and inspect data controllers and processors;
investigate data misuse, unlawful processing, and personal data breaches;
issue binding corrective orders and impose proportionate and dissuasive penalties.
• Mandate structured coordination mechanisms between the DPA and sectoral regulators, including Nepal Rastra Bank, to prevent regulatory overlap, clarify jurisdictional responsibilities, and strengthen enforcement.

• **Regulate the Use of Digital Identity and KYC Data**
• Standardize the collection, use, and sharing of digital identity and KYC data across public and private sectors to prevent commercial exploitation and function creep.
• Introduce strict safeguards to limit secondary use of identity data beyond lawful and necessary purposes.
Consider mandating data localization for sensitive financial and identity data, or at a minimum require robust cross-border data-transfer safeguards, including adequacy assessments, contractual protections, and regulatory approvals, to mitigate jurisdictional, sovereignty, and security risks.

d) For Mobile Wallet Companies:

• **Revise and Strengthen Privacy Policies**
• Undertake a comprehensive revision of privacy policies to ensure clarity, transparency, and regulatory compliance.
• Clearly disclose:
o data-retention periods and deletion practices;
o identities and roles of third-party data processors and service providers;
o purpose limitation in precise, non-generic terms.
• Distinguish mandatory regulatory data (e.g., KYC and AML/CFT records) from optional or value-added data to enhance user understanding and trust.

• **Enhance Technical and Organizational Security Practices**
• Implement robust security measures, including:
o multi-factor authentication for user access;
o end-to-end encryption for sensitive personal and financial data;
o regular penetration testing and vulnerability assessments.
• Establish and document incident-response and breach-management plans aligned with regulatory expectations and industry best practices.

• **Operationalize User Rights Through Platform Design**
• Introduce user-facing privacy control tools that enable:
o account deletion or deactivation;
o downloading or exporting personal data;
o withdrawal of consent for non-essential data processing.
• Ensure that these controls are accessible, functional, and clearly explained within the platform interface.

• **Publish Transparency and Accountability Reports**
• Go beyond minimum compliance by publishing periodic transparency reports that include:
o data-retention timelines;
o categories of third-party data processors;
o reported breach incidents, if any;
o high-level outcomes of security or privacy audits.
• Use transparency reporting as a mechanism to demonstrate accountability and differentiate responsible providers in the market.

• **Invest in User Awareness and Privacy Literacy**
• Develop and implement privacy-awareness initiatives, such as:
o in-app notices and prompts explaining data use and user rights;
o public campaigns on responsible data handling;
o clear, accessible messaging on privacy risks and safeguards.
• Strengthen user understanding of privacy rights and risks to reduce disputes and build long-term trust in Nepal's digital payment ecosystem

References

• eSewa Ltd. (2010). Privacy Policy and Terms of Use.
https://blog.esewa.com.np/privacy-policy
• IME Pay. (2024). Privacy Policy.
https://www.imepay.com.np/privacy-policy
• ParbhuPay. (2019). Privacy Policy.
https://prabhupay.com/privacy&policy
• Kantipur. (2024, November 26). Khalti wallet employee arrested for selling customers' personal details to criminal gangs.
https://ekantipur.com/business/2024/11/26/en/pocket-wallet-employee-arrested-for-selling-customers-personal-details-to-criminal-gangs-35-40.html
• Khalti by IME. (2024). Privacy policy. https://khalti.com/privacy-policy
• Khalti Digital Wallet. (2024). Privacy Policy and Terms.
https://khalti.com/privacy-policy/
• Moru (Pay Nep Pvt. Ltd.). (2024). Privacy Policy.
https://moru.com.np/privacy-policy
• NamastePay. (2024). Official Website and Policy Pages.
https://www.namastepay.com
• Nepal Rastra Bank, Financial Intelligence Unit. (2024). FIU Nepal Strategic Analysis Report 2024. Kathmandu: NRB.
https://www.nrb.org.np/contents/uploads/2024/11/FIU-Nepal-Strategic-Analysis-Report-2024.pdf
• Nepal Rastra Bank. (2024a). भुक्तानी प्रणालीसम्बन्धी एकीकृत निर्देशन – 2081 (Unified Directives on Payment Systems).
https://www.nrb.org.np/contents/uploads/2024/07/Unified-Directives-Payment-Systems-2081.pdf
• Nepal Rastra Bank. (2024b). IT and Cybersecurity Guidelines & Financial Consumer Protection Framework.
https://www.nrb.org.np/financial-consumer-protection/
• Nepal Rastra Bank. (2025). Notice on Non-Renewal of PSP License: Prabhu Technology Pvt. Ltd.
https://www.nrb.org.np/notice-on-psp-license/
• OECD. (2013). The OECD Privacy Guidelines.
https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
• QPay. (2024). Privacy and Security Policy.
https://www.getqpay.com/privacy-policy/
• Republica. (2020). eSewa data breached: A hacker releases nearly two dozen users' details including passwords.
https://myrepublica.nagariknetwork.com/news/esewa-data-breached-a-hacker-releases-nearly-two-dozen-esewa-users-details-including-passwords
• World Bank. (2020). Consumer Protection and Data Governance in Digital Financial Services.
https://documents.worldbank.org/en/publication/documents-reports/documentdetail/307781588589071007
• World Bank. (2020). Consumer Risks in Digital Financial Services. Washington, DC.
https://www.worldbank.org/en/topic/financialconsumerprotection/publication/consumer-risks-in-digital-financial-services