Data Governance Framework: Nepal

Data for Development — South and Southeast Asia

Semanta Dahal & Avash Mainali

October 1, 2025

Table of contents

[1] Directives for Managing the Use of Social Media, 2080 (2023), available at "https://api.giwms.gov.np/storage/22/posts/1701329617_80.pdf"

[2] "PDF," n.d.

List of abbreviations

API	Application Programming Interface
BAFIA	Bank and Financial Institution Act
ESB	Enterprise Service Bus
ETA	Electronic Transaction Act
GIDC	Government Data Center
GRDC	Government Recovery Data Center
NeGIF	Nepal E-Government Interoperability Framework
NRB	Nepal Rastra Bank
RTI	Right to Information
SOA	Service Oriented Architecture

About this report

About LIRNEasia

LIRNEasia is a pro-poor, pro-market regional policy think tank. Our mission is *Catalysing policy change and solutions through research to improve the lives of people in the Asia and Pacific using knowledge, information and technology.*

Address: 15 2/1, Balcombe Place, Colombo 8, Sri Lanka.
Telephone: +94 11 267 1160
Email: info@lirneasia.net
Website: https://lirneasia.net/
Twitter: https://x.com/LIRNEasia
Facebook: https://www.facebook.com/lirneasia/
YouTube: https://www.youtube.com/@LIRNEasia-
LinkedIn: https://lk.linkedin.com/company/lirneasia
Instagram: https://www.instagram.com/lirneasia/

Funding

This work was carried out with the aid of a grant from the International Development Research Centre, Ottawa, Canada. The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

1 Introduction

This report on data governance in **Nepal** is part of the 'Harnessing Data for Democratic Development in South and Southeast Asia' (D4DAsia) project, which aims, *inter alia*, to create and mobilise new knowledge about tensions, gaps and the evolution of the data governance ecosystem taking into account formal and informal policies and practices.

In today's digital age, data governance ecosystems play a crucial role in shaping our societies. These ecosystems, comprising policies, laws, practices, behaviours, and technologies, aim to govern data in ways that protect rights, foster innovation, enhance transparency, and ultimately promote democratic and inclusive governance. An ideal data governance system would protect rights, enable innovation, improve transparency, and help in bringing about democratic, inclusive governance. However, the landscape of data governance is complex and often fraught with challenges, particularly in South and Southeast Asia.

Through the rest of the report, unless the context indicates otherwise, the term 'policies' is used as shorthand for policies, statutes, regulations, rules, administrative orders and even practices and technologies that are used to implement all of those as part of data governance ecosystems.

Data is increasingly being recognised as an enabler for development. It is an essential requirement for policymaking and monitoring of development goals and targets. When effectively managed, data can be used as an asset to support significant development actions such as poverty reduction, food security, mitigating impact of climate change, and disaster management. If mismanaged, it can exacerbate inequalities and undermine the development potential of the same actions.

The D4DAsia project has produced nine reports so far: seven detailed individual country reports that deal with the issues of data governance in the following countries; India, Indonesia, Nepal, Pakistan, Philippines, Sri Lanka and Thailand; a detailed look at data protection in South Korea; and a synthesis report that summarises the findings from the various countries while drawing out the contrasts amongst them, along with detailed findings for the research questions we had posed. The questions are:

1. What is common, and what is nationally specific, in the emerging data governance architectures in South and Southeast Asia? What are the explanations?
2. What are the implications of the emergent nature of the governance architecture? Because there is no overall design that envisions how the parts fit together, it is likely that there will be friction points and even contradictions. How are these being worked out?
3. The emerging governance architecture involves trade-offs among objectives such as greater accountability of powerholders, economic growth, including the creation of employment and wealth, resilience of systems, etc. How have different societies: (a) explicitly recognised the trade-offs or not; and (b) handled them?
4. Are there legislative or policy innovations with potential for replication? What are the modalities of sharing experiences? Are developing countries learning from each other, or are they learning from the developed countries?
5. How were the laws and bills developed? What expertise was brought to bear? How open were the procedures? How receptive were drafters to suggestions and criticisms?
6. How were capacity challenges addressed: by simplifying the laws or by tolerating incomplete implementation?

1.1 Structure of the report

1.1.1 Governance background

This report starts by providing contextual information about the constitution and governance framework in **Nepal**, including how lawmaking powers are distributed and delegated, the powers of the judiciary to overturn laws or to enforce policies, and the legal and regulatory background in the country.

1.1.2 Increasing openness/access

The report then discusses policies that increase openness or access. By this we mean policies that allow greater access by citizens, consumers, and corporations to data, or facilitate interoperability or cross-border data transfer. Specifically, we do not include increased governmental access to citizens' private data or non-public corporate data.

This section discusses open data policies, the question of how much governmental data is made available proactively and how much is reactive as well as the quality of data being disseminated. The report also assesses government policies favouring or requiring free and open source software (FOSS) or open standards, noting any specific standards that are mandated.

1.1.3 Decreasing openness/access

The report then moves on to discuss the opposite, i.e. laws, policies and practices that decrease openness or access. By this we mean decreasing access of citizens, consumers, and corporations to data. To be clear, this is not a negative value judgement, since upholding important individual and collective rights, such as privacy and public security, necessitate reducing citizens' access to data.

This theme explores issues of security such as whether there are any data retention or localisation requirements, restrictions on the right to access information (such as national security, privacy etc.) and exceptions to data security requirements for law enforcement. We further discuss the privacy and copyright framework in brief and specifically try to answer whether there are any exceptions for search engines as well as for research and artificial intelligence (AI).

The issue of data governance and the policies surrounding its implementation is a critical one for governments, citizens and businesses across the world. As mentioned earlier, we use the term data governance to refer to 'diverse arrangements, including technical, policy, regulatory or institutional provisions, that affect data and their creation, collection, storage, use, protection, access, sharing and deletion across policy domains and organisational and national borders.'[3]

[3] OECD, *Going Digital Guide to Data Governance Policy Making*.

2 Introduction

This paper focuses on exploring the data governance framework in Nepal, a country where a comprehensive data governance legislation is yet to be established. In light of this a thorough examination of various legislations, guidelines, polices, and directives becomes imperative to understand the framework of data governance within the country. Furthermore, to navigate through the data governance structure more effectively, understanding the legal system of Nepal is crucial. The subsequent paragraphs will briefly elaborate on the legal system of Nepal.

2.1 Constitution of Nepal

The Constitution of Nepal 2072 (2015), the seventh constitution in the history of Nepal since 1948, is the fundamental law of Nepal. The Constitution with 308 Articles, 35 parts and 9 schedules serve as the cornerstone for governance in Nepal. The Constitution defines the legal landscape of the Nepalese republic. It embodies the nation's collective resolve to uphold the sanctity of law and also safeguards the rights and aspirations of every Nepali citizen. The constitution explicitly states in Article 1 (1), "This Constitution is the fundamental law of Nepal. Any law inconsistent with this Constitution shall, to the extent of such inconsistency, be void." Any law that is divergent from the constitution is *ultra vires* as it becomes unable to withstand the scrutiny of constitutional fidelity. Thus, the constitution reigns supreme.

2.2 Three tiers of Government

The main structure of Nepal consists of three levels- the Federal/central the State and the Local level. This multi-layered structure is outlined in the Constitution- one federal government for the whole country, 7 provincial governments for 7 provinces and 753 local level governments for 753 local level. The specific powers and responsibilities of each level are clearly delineated across several schedules — the powers of the Federation are enumerated in Schedule-5, powers of the States in Schedule-6, and powers of the Local level in Schedule-8 of the Constitution. Likewise, the concurrent powers of the Federation and the States are enumerated in Schedule-7 and the concurrent powers of the Federation, State and Local levels in Schedule-9. "Cooperation, Coexistence and Coordination" serves as the overarching principle of the Nepalese federalism. The federal structures have been created with multiple objectives in mind: to end the centralized and unitary State system, especially the discrimination and oppression that it creates, to maintain inclusive and participatory arrangement in different entities of the State and to ensure equality, social justice, sustainable peace, good governance, development with an aim to fulfill the aspirations of prosperity. This restructuring reflects a profound commitment to reimagining governance in Nepal, with a view to create a more equitable, just, and prosperous Nepal.

2.3 Court System

The Constitution of Nepal has established a three-tier court system consisting of the Supreme Court, 7 high courts, and 77 district courts. The Supreme Court, the supreme judicial authority of the nation, is also the court of record and has the final authority to interpret the Constitution and laws. Any interpretation of the Constitution or a law made by or any legal principle laid down by the Supreme Court is binding to all. The Supreme Court is entrusted with the responsibility to act as the guardian to protect the sanctity of the constitution, uphold the laws

of the nation protecting personal liberty and fundamental rights of the Nepalese citizens conferred by the constitution. The Supreme Court has the authority to declare a law as void *ab initio* if it finds that the impugned law contravenes the provisions of the constitution. It also has the power to issue appropriate orders and writs of *habeas corpus*, *mandamus*, *certiorari*, prohibition, and *quo warranto*. It also enjoys appellate jurisdiction to hear appeals against decisions made by lower courts, test judgments referred for confirmation, revise cases, hear petitions or review its judgments or final orders. The multifaceted jurisdiction and robust powers of the Supreme Court plays a pivotal role in safeguarding the rule of law and administering justice in the Nepalese society.

Some instances where the Supreme Court of Nepal has safeguarded the rule of law and upheld the Constitution of Nepal can be seen in the case of Meera Dhungana v Office of the Prime Minister and Council of Ministers[4] where the petitioners challenge the constitutionality of Sections 1 and 16 of the chapter on partition share (Angshabanda) of the National Code (Muliki Ain) 2020, arguing that these provisions discriminate against women's right to equal property and asserts that Section it is inconsistent with Article 11(2) of the Constitution of the Kingdom of Nepal, 1990, Article 2 of the UDHR-1948, Article 26 of the ICCPR-1966, Article 3 of the ICESCR-1966, and Articles 1, 15, and 16 of CEDAW-1979 and hence, declare such legal provisions void and ultra vires. The court ordered the government to present a bill reviewing the laws relating to property rights which led to the amendment of such laws upholding the right to equality enshrined under Article 11 of the Constitution of Nepal. In the case of Sapana Pradhan Malla v Office of Prime Minister and Council of minister and Others[5] the right to privacy of children, women victims of rape and HIV/AIDS-infected people were protected by the Supreme Court by making hearing of such cases closed hearing and ordered that privacy had to be maintained right from the time of registration of the case in the police office or any other body having authority till the disposal of the case or even after disposal of that case.

For the adjudication of prescribed constitutional disputes, the Constitution envisions a Constitutional Bench within the Supreme Court, consisting of the Chief Justice and other four Judges designated by the Chief Justice on recommendation of the Judicial Council.. The Constitution provides the Constitutional Bench with the jurisdictional power to hear and settle disputes relating to the jurisdiction between the Federal and a State, between States, between a State and a Local level and between Local levels, and Disputes relating to election to members of the Federal Parliament or State Assembly and matters relating to disqualification of a member of the Federal Parliament or of the State Assembly.[6]

As with the Supreme Court, the high courts also have the power to issue a variety of orders and writs including the writs of habeas corpus, mandamus, certiorari, prohibition and quo warranto. They play a significant role in the protection and enforcement of fundamental rights and legal entitlements. They also have the power to originally try and settle cases, hear appeals challenging decision of lower courts and test judgments referred for confirmation. This power provides a critical layer of oversight and ensures the accuracy and fairness of judicial outcomes.

The District Courts have the power to originally try and settle all cases under their jurisdiction, try petitions including habeas corpus and prohibition under law, hear appeals against decisions made by quasi-judicial bodies and Local level judicial bodies, and also institute contempt proceedings and punish for contempt of court. The District Courts play a crucial role in shaping the legal landscape of Nepal because it is the first instance court in many cases and thereby,

4 Writ No. 0545 of the year 2065 B.S. (2008) (Decision No.8928)

5 Writ No. 3561 of the year 2063 B.S. (2006)

6 Article 137, Constitution of Nepal 2072 (2015)

ensuring that justice is both accessible and equitable. It has also been granted jurisdiction over habeas corpus

2.4 Judicial Review

The practice of judicial review is not new to Nepal. Constitution of Nepal has provision for judicial review of any laws inconsistent with the provision of constitution, encroaching the fundamental rights and meddling the devolution of power and competencies among various level of government. The competency for this has been granted to the Supreme Court of Nepal. Provision of judicial review had also been incorporated in predecessors of the current constitution in force.[7][8] The power of judicial review has empowered the Nepalese Supreme Court to examine the constitutionality of laws and executive actions, allowing it to modify, amend, or even alter the constitution itself.[9]

2.5 Legal Framework applicable to Information and Communication Sector of Nepal

2.5.1 Electronic Transaction Act, 2063 (2008)

The internet was first introduced in Nepal only in 1994, hence only following that cybercrimes started emerging in Nepal. Before 2008, legal matters concerning cybercrimes fell under the jurisdiction of laws such as the Muluki Ain, Some Public (Crime and Punishment) Act 2027, and the Telecommunications Act 1997. However, with the increasing prominence and urgency of cyber-related offenses, there arose a necessity for legislation specifically addressing cyber law issues.

The Electronic Transaction Act, 2063 (2008) is an important piece of legislation for the regulation of transactions to be carried out by means of electronic data exchange or any other means of electronic communications , which paved way for the protection of data and privacy. It came into effect on 2nd September, 2006, this legislation represents Nepal's first legislative attempt to address the growing challenges of the digital age. It introduced crucial provisions aimed at protecting electronic records and ensuring the privacy of digital signatures, laying the foundation for a more secure and reliable digital environment.

This legislation provides for the authentication and regularization of the recognition, validity, integrity and reliability of generation, production, processing, storage, communication and transmission system of electronic records. It aims to make exchange of electronic data or electronic communication more secure and also criminalizes certain acts of unauthorized access and alteration of electronic records, marking a significant leap forward in the realm of cyber security within Nepal as it is the first major legislation to criminalize computer[10] related

---

7 Interim Const. Of Nepal, 2063, art. 107 (1) (2); Const. Of The Kingdom Of Nepal, 2047, Art. 88.

8 "PDF," n.d.

9 Bipin Adhikari, Constitutional Foundings in Nepal: Experience with Changing Parameters in Kevin YL Tan & Ridwanul Hoque, Constitutional Foundings in South Asia 165 (Hart Publishing 2021).

10 Section 2 (d), Electronic Transaction Act, 2063 (2008), "*means an electro-magnetic, optical or other high-speed data processing device or system, which performs logical, arithmetic and memory functions by manipulating electro-magnetic or optical impulses, and also includes all acts of input, output, processing, storage and computer software or communication facilities which are connected or related to the computer in any computer system or computer network*"

offences. This legislation served as a catalyst for subsequent legislative development for protection of privacy and data.

2.5.2 Constitution of Nepal, 2072 (2015)

The Constitution is the fundamental law of sovereign state of Nepal and any law inconsistent with the constitution shall be void to the extent of such inconsistency. The right to privacy and right to information are enshrined under the Constitution of Nepal as fundamental rights of every person.

2.5.3 Privacy Laws

The Privacy Act, 2075 (2018) and Individual Privacy Regulation, 2077 (2022) are the laws that safeguard the right to privacy of matters relating to body, residence, property, document, data, correspondence and character of every person, entrusted to any public body[11] or institution,where public body means a body which is parastatal. It seeks to promote the safe use of such information and to preventencroachment on the privacy of the individual.

2.5.4 The Right to Information Act, 2064 (2007)

This legislation was enforced to make state actions more open and transparent. It aims to make information of public importance held by public bodies accessible to the citizens of Nepal and protect the right of the citizens to be well informed. It also protects sensitive information to protect the interest of the nations and its citizens.

2.5.5 Directives for Managing the Use of Social Networks, 2080 (2023)[12] (the "Social Network Directive")[13]

The Social Network Directive recently came into effect on 27th November 2023 for the regulation of the use of social networks and to promote self-regulation by social network platform operators and users of social network platforms. The Social Network Directive provides for a list of responsibilities that social network platform operators must necessarily abide by. Such responsibilities include developing an algorithm (calculation method) and taking other measures in social networks in order to stop the publication or broadcasting of information, advertisements and materials that is contrary to the prevailing laws, to identify

---

[11] Section 2 (e), The Privacy Act, 2075 (2018), Public body mean the following: (1)The Government of Nepal, Provincial Government or Local Level or government office under the Government of Nepal, Provincial Government or Local Level, (2) A court, other judicial body, constitutional body or office thereunder, (3) A regulatory body or office thereunder, (4) A company, bank, committee having full or partial ownership or control of the Government of Nepal, Provincial Government or Local Level or commission, corporation, authority, incorporation, academy, board, center, council and other body corporate of similar nature established by the Government of Nepal, Provincial Government or Local Level pursuant to law. (5) A political party and organization registered under prevailing law, (6) A university, college, school, research center and other similar academic or educational institution that has been established or operated by the Government of Nepal, Provincial Government or Local Level or that has obtained full or partial grants from the Government of Nepal, Provincial Government or Local Level. (7) An institution operated with credit, grant or guarantee of the Government of Nepal, Provincial Government or Local Level. (8) An institution having full or partial ownership or control of the body mentioned in sub-clause (1), (2), (3) or (4). (9) Any other institution specified by the Government of Nepal as a public entity by publishing a notice in the Nepal Gazette.

[12] Directives for Managing the Use of Social Media, 2080 (2023), available at "https://api.giwms.gov.np/storage/22/posts/1701329617_80.pdf"

[13] "PDF," n.d.

contents that infringes the provision of the Social Network Directive and remove the same, to adopt necessary security standards to maintain privacy of personal details of social network user and not make such details or use them for other purposes, to broadcast necessary awareness and educational content in the interest and protection of social networks users from time to time, make proper arrangement for handling grievance, to verify facts of content published or broadcasted on social network platform, to adhere to the internationally developed Santa Clara Principles, to use banking system for payment of transactions emanating from operation of social network platforms, etc.[14]

2.5.6 Intellectual Property Laws

The Copyright Act, 2059 (2002) provides for the protection of artistic and creative work in Nepal. Whereas, Patent, Design and Trademark Act, 2022 (1965) gives protection to any invention, form or shape of any material and any word or symbol or picture or its combination used by any firm, company or an individual. Therefore, these two legislations govern and protect intellectual property in Nepal.

2.5.7 Telecommunication and Publication Laws

The Telecommunications Act, 2053 (1997) was enacted to regularize and standardize the telecommunication service in Nepal to make it more reliable and easily accessible to the public. It also introduced private sector in the telecommunication service and aimed to make such service more reliable. The Press and Publication Act, 2048 (1991) was enacted with the aim of safeguarding the freedom of expression in the field of journalism and to regulate the same in a dignified and responsible manner which would uphold the morality among the people from various backgrounds and places.

2.5.8 Banking Laws

The Bank and Financial Institution Act, 2073 (2017) (the "**BAFIA**") regulates and governs every aspect with regard to banks and financial institutions in Nepal. The Unified Directives issued by the Nepal Rastra Bank to "A", "B" and "C" Category Certified Institutions, 2079 (2023)[15] was issued under the authority granted by the BAFIA to further regulate the banks and financial institutions in Nepal and provides directions to the banking sector enterprises as per the changing laws of Nepal with regard to the banking sector. The Payment System Unified Directive,2079 (2023)[16] provides for the regulation of payment system operators and payment system provider. The Circular issued by Nepal Rastra Bank regarding Foreign Exchange Transactions,2079 (2023)[17] provides for the monitoring of foreign payments or transaction made in Nepal. These directives provide a framework for banks and financial institutions, payment system operators and providers to function according to international standards.

Even though Nepal has several laws and regulations in place to protect privacy and govern data, many of them are outdated and do not adequately address the challenges posed by emerging technologies. The existing legal framework struggles to keep up with rapid advancements in

---

[14] Section 8, Directives for Managing the Use of Social Networks, 2080 (2023)

[15] available at "https://www.nrb.org.np/contents/uploads/2023/02/Unified-Directives-2079-Magh-published.pdf" (last accessed on 3rd October, 2023)

[16] available at "https://www.nrb.org.np/contents/uploads/2023/01/PSD_unified-Directive-2079_Letter-combined.pdf" (last accessed on 3rd October, 2023)

[17] available at "https://www.nrb.org.np/contents/uploads/2023/04/FXMD-Circular-18_2079.80_Unified-Circular-2079.pdf" (last accessed on 3rd October, 2023)

data-driven innovation, leaving significant gaps in areas like cross-border data flows, cybersecurity threats, and the ethical use of artificial intelligence. These gaps not only put citizens' privacy at risk but also create legal uncertainty for businesses and investors, slowing down Nepal's digital transformation. A major challenge lies in the enforcement of current laws, which often lack the clarity and flexibility needed to adapt to modern data governance needs. Additionally, weak institutional capacity, low public awareness, and a shortage of technical expertise make effective implementation and oversight even more difficult. To ensure stronger data governance, Nepal must adopt a more cohesive and forward-thinking approach that not only protects individual privacy but also supports digital innovation and economic development. This requires updating existing laws, establishing clearer regulatory mechanisms, and strengthening institutional capacity to effectively oversee data management.

3 Openness/Increasing Access

By "increasing openness", we have come to understand that it means something that safeguards/increases access by citizens or companies to data or reduces access by government (and government alone) to citizens' or companies' data, or safeguards/increases citizens' liberties in relation to data.[18]

The Constitution of Nepal, under the directive principles of the state policies, provides that the State must ensure easy and simple access of the general public to information technology. This involves the development and expansion of information technology infrastructure in accordance with national requirements. Additionally, it also emphasizes the importance of maximizing the utilization of information technology for national development purposes.[19] It also provides the right to information, which entails the right to access information and data in public interest.[20]

A major piece of legislation that seeks to mandate openness in data is the Statistics Act, 2079 (2022) (the "**Statistics Act**"). The Statistics Act defines various terms related to data and its protection. The main purpose of the Statistics Act is to assist the Federal, Provincial and Local Government in efficient public service by ensuring the production, processing, collection, publication and distribution of statistics is organized and reliable. The act defines a "Computer Database"[2122] as a systematically organized collection of numerical environments, facts, information, maps, or concepts stored in a computer or computer network system and can be interpreted through visual, auditory, or other sensory means. "Statistics"[2324] refers to numerical data, statistics, physical, environmental, and related information, and involves the collection, presentation, or organization of such data, including the preparation of statistical statements. "Electronic record"[2526] refers to data, information, images, events, or audio-visual content obtained from an electronic medium and perceived as significantly different from the usual pattern.

The Statistics Act sets out the standard for demographic indicators. It also creates a repository for the data collected. It also states that provincial government or local level may collect, process, analyze, publish, distribute or store the statistical data.[2728]

The information processed and collected pursuant to the Statistics Act is published on the website of the National Statistical Office[2930], but it is very different from the *Data.gov.in, the*Indian government's open data portal, where documents published by multiple government agencies can be accessed,. Upon initial inspection of the website, it seems to have data missing and faces retrieval challenges. Following an interview with an interviewee from the Central Bureau of Statistics, National Statistics Office, it was determined that not all required

---

18 Pranesh doc.
19 Article 51 (f) (5), Constitution of Nepal, 2072 (2015)
20 Article 27, Constitution of Nepal, 2072 (2015)
21 Section 2 (b), Statistics Act, 2079 (2022)
22 "PDF," n.d.
23 Section 2 (e), Statistics Act,2079 (2022)
24 "PDF," n.d.
25 Section 2 (j), Statistics Act 2079 (2022)
26 "PDF," n.d.
27 Section 15, Statistics Act, 2079 (2022)
28 "PDF," n.d.
29 National Statistics Office, available at "https://censusnepal.cbs.gov.np/Home/Index/EN" (last accessed on 1st October, 2023)
30 National Statistics Office, *Census Nepal 2021.*

information is readily accessible to them and that the published data on the website is the summarized version of a larger set of data. This limitation is attributed to a shortage of technical personnel and insufficient coordination among various ministries, resulting in the absence of crucial data, notably pertaining to the banking and financial sectors.[31]

National Data Profile system that provides a platform on which all data and information related to geography, natural resources, environment, demographics, social, economic, and governance etc., of the country are kept and updated to support greater data-led decision making and monitoring of Sustainable Development Goals (the "**SDGs**").[32][33]

With the aim of increasing openness and encouraging the use of open software, the Digital Nepal Framework, 2019[34] (the "**Digital Framework**") has identified key sectors crucial for fostering socioeconomic advancement within Nepal's digital landscape. These sectors include agriculture, health, education, energy, tourism, finance, urban infrastructure, and digital foundations. Through this Digital Framework, the government aims to establish an outline for enhancing security, data protection, disaster recovery, resilience, data sharing and business continuity. It also provides guidelines for transitioning towards a paperless government and implementing automation initiatives across all three tiers of government. It also provides for the use of open-source software which can be more affordable and cost effective. This framework was influenced by the India's Digital India program.

The Digital Framework provides for the establishment of a National Steering Committee chaired by the Prime Minister and supported by a National Implementation Committee (the "**NIC**") chaired by the Secretary of the Ministry of Communication and Information Technology. The National Steering Committee ensures alignment with national development objectives, while the NIC oversees project execution and coordination. Sector-specific sub-committees will facilitate interdepartmental collaboration, and a Digital Nepal Program Management Office will support project execution, coordination, and monitoring. Furthermore, the framework outlines provisions for the establishment of Provincial Data Centers which are designed to serve as repositories for data generated by provincial and local-level governments. Additionally, a decentralized provincial database is envisioned to facilitate failover and recovery processes, ensuring robust data management at the regional level.

The Digital Framework provides that special benefits will be offered to the local information and communication technology (the "**ICT**") industry to support its growth into a globally competitive software sector. This will be achieved by encouraging the adoption of both proprietary and open-source solutions for serving both domestic and international markets. The government seems to encourage both proprietary and open-source solutions, but through our interviews we identified two prevailing perspectives from the government officials where the government discourages adopting open-source software due to security concerns, while others believe open source signifies globally recognized software. Nonetheless, various policies encourage the use of open standards. Additionally, steps will be taken to reduce obstacles for local IT companies and service providers to participate in government ICT projects, whether funded internally or internationally.[35]Therefore, pilot programs should be implemented to

---

31 Interview with the interviewee from the Central Bureau of Statistics, Annex-1

32 National Data Profile, National Statistics Office, available at "http://nationaldata.gov.np/"(last accessed on 1st October, 2023)

33 "National Data Portal-Nepal."

34 Digital Nepal Framework, 2019, available at "https://drc.gov.np/storage/backend/pages/resources/others/D8lp6SoTBuokqwXB7V9ohB9aodF4v6qTLGzUvN7M.pdf"

35 Digital Nepal Framework, 2019 (developing the ICT Industry Sector, point 4.5 , pg.276)

evaluate the feasibility of adopting open-source software, while collaboration and partnerships with open-source initiatives should be fostered. Additionally, negotiating the openness of data is essential to balance security and innovation.

Data protection, security, and privacy are essential components in building trust within a developing digital economy. Hence, it highlights the importance of conducting a comprehensive evaluation of Nepal's current policies regarding these aspects. The Digital Framework aims to establish a conducive environment for the adoption of digital solutions under the Digital Nepal Program.

While open-source software is widely recognized as a global standard, concerns remain regarding its security and integration within government systems. To address these issues while leveraging the benefits of open-source solutions, a structured approach should be adopted. One effective strategy is the implementation of pilot programs within select government agencies. These programs can serve as controlled test environments to evaluate the feasibility and security of open-source solutions. By running small-scale trials, agencies can assess compatibility with existing IT infrastructure, identify potential cybersecurity risks, and determine cost-effectiveness before broader adoption.

Additionally, collaboration with open-source communities can enhance technical expertise and provide access to a global network of developers who contribute to continuous security improvements and software advancements. Many governments worldwide have successfully integrated open-source solutions by fostering public-private partnerships and leveraging the collective intelligence of the developer community.

Furthermore, establishing partnerships with industry leaders and technology providers can facilitate structured negotiations on data openness. A well-defined approach should be taken to determine which data can be shared openly while ensuring compliance with privacy regulations and security protocols. This can be achieved by setting clear data governance policies, defining access controls, and implementing regular security audits. By adopting these measures, Nepal can explore the benefits of open-source software while addressing security concerns through a phased, well-monitored approach.

The Supreme Court of Nepal has taken steps to increase access to court-related information by publishing judgments and listing daily court hearings on its website.[36][37] However, this initiative has its limitations. Only the final judgments and in some cases orders from the Supreme Court are being uploaded, leaving a significant gap in the availability of comprehensive legal information. Unfortunately, judgments from the high courts and district courts are not uploaded on their website, which restricts public access to a broader spectrum of judicial decisions and undermines the overall goal of transparency in the judicial system. Other than that the Supreme Court annually publishes all the established precedents in their journal named 'Nepal Kanoon Patrika' which translates to Nepal Legal Newspaper. The Nepal Kanoon Patrika also has a website where all the published decisions can be accessed.[38]

The budget for every fiscal year is presented by the Minister of Finance in the Parliament and Ministry of Financed publishes the details of the budget including the Expenditure Details (the Red Book).[39][40]. The fiscal budget of each provincial government and local government is also

[36] Supreme Court of Nepal, available at "https://supremecourt.gov.np/web/" (last accessed on 1st October, 2023)

[37] "Supreme Court Nepal."

[38] Nepal Kannon Patrika, available at "https://nkp.gov.np/"

[39] Fiscal Budget, available at "https://www.mof.gov.np/site/publication-detail/3249" (last accessed on 5th October, 2023)

published by such government which can be publicly accessed by any individual through the website of the Ministry of Federal affairs and General Administration.[41]

The Government Website Management and Operational guidelines, 2078 (2021) also establish a standardized format for all government websites. These guidelines mandate specific contents to be included, such as the organization's objectives, introduction of officials with their contact details, relevant policies and legal provisions, essential links, office responsibilities, address details, site map, published notices and information, budget details, and fiscal plans.[42] The guidelines mandate that all government websites must be accessible to persons with disabilities,[43] upholding the right to information for every citizen enshrined under Article 27 of the Constitution of Nepal. This initiative is viewed as step to increasing access, setting a minimum benchmark for information dissemination on government websites.

Additionally, for the promotion of government websites, it is mandated to incorporate metadata (keywords) to ensure compatibility with search engines like Google, Bing, Baidu, Yahoo, Ask, DuckDuckGo, etc.[44]. The guideline stipulates that security assessments must be carried out annually by the IT department of each government office to uphold the security and reliability of their websites. The interviewee from the Government Integrated Data Centre informed us that regular security assessment is carried out but from our observation and media reports suggesting number of times security breaches in governmental websites it is likely that regular security assessments is not followed by most of the governmental institutions which resulted loss of data. Moreover, the protection of email data is emphasized by requiring all emails to be securely archived for a minimum of five years.[4546] The main server of the government of Nepal also has been facing cyberattacks and data breaches in the recent years.[4748]

The National Information Technology Center (the "**NITC**") which is also referred to as Government Integrated Data Centre (the "**GIDC**") was established in 2001, where in government data are managed and stored which provides an integrated platform for sharing government information within various governmental bodies or ministries.

The Government Website Management and Operational guidelines, 2078 also mandates that GIDC shall host all government website.[49] The GIDC created the domain named *NItc.gov.np* to host the domain of the government and to make an integrated system for intergovernmental communication. Its main role is to provide services like data storage, sharing computing resources, email/internet and website hosting, which are general function of any data center, to all the government ministries and departments. During an interview with various government organization, it came to light that a private company i.e. Mercantile Communication Pvt. Ltd. provides domain registration services in Nepal, which was later clarified by the interviewee from the GIDC that even though such domain registration service is provided by a private

---

40 Ministry of Finance, *Fiscal Budget*.

41 Available at "https://mofaga.gov.np/lgbudget"

42 Section 3, Government Website Management and Operational guidelines, 2078 (2021)

43 Section 4(3)(s), Government Website Management and Operational guidelines, 2078 (2021)

44 Section 5, Government Website Management and Operational guidelines, 2078 (2021)

45 Nepal Times, 'Open season on Hacking into gov.np' (29 Jan 2023), available at "https://nepalitimes.com/news/open-season-on-hacking-into-gov-np" (last accessed on 5th October, 2023)

46 Times, *Open Season on Hacking into Gov.Np*.

47 Prithvi Man Shrestha, 'Singha Durbar server continues to face cyberattacks', The Kathmandu Post,(30 January 2023), available at "https://kathmandupost.com/national/2023/01/30/singha-durbar-server-continues-to-face-cyberattacks" (last accessed on 5th October, 2023)

48 Shrestha, *Singha Durbar Server Continues to Face Cyberattacks*.

49 Section 4(4), Government Website Management and Operational guidelines, 2078 (2021)

company without the prior approval of GIDC such domain cannot be registered in Nepal. The interview also clarified that GIDC only manages the data of public or government entities and does not store or manage data of private entities. For recovery of data because of any loss the GIDC has one backup storage facility. However, the recent incident of many government data being hacked has made the role of GIDC even more imperative.

Although there is no integrated website for the publication or access of all government data, website of each government entity publishes the related information in their website which makes information accessible to the general public. For illustration purposes the following government entities have been considered for examples:

The Credit Information Bureau of Nepal (the "**CIB**") releases a list of borrowers and affiliated individuals, firms, or companies who have been blacklisted in accordance with the laws of Nepal. This list solely includes the names of the borrowers and their associated companies, while personal information such as citizenship IDs remains confidential.[50]

The Office of Company Registrar, operating under the Ministry of Industry, Commerce, and Supplies, regularly updates and publishes real-time statistics on the total number of registered companies, distinguishing between private and public entities.[51] Additionally, individuals can access specific information about a registered public company by entering its registration number on the Registrar's website. This information includes the company's type, registered address, and registration date. In addition to this, in case of public company, a copy of the memorandum of association, prospectus, annual accounts and audit or directors report shall be provided for, if it is demanded by any individual, as per the Company Act.[52] Furthermore, individuals seeking to register a new company can consult the list of previously registered names for reference.

The Department of Industry (the "**DOI**"), under the Ministry of Industry, Commerce, and Supplies, hosts a website where it discloses a catalog of registered industries and those endorsed for foreign investment. This inventory encompasses details like the industry's name, objectives, address, total capital, fixed capital, working capital, and employment figures.[53] Additionally, the DOI publishes information regarding the registration of industrial property, including patents, designs, and trademarks, which comprises of the total number of foreign and national registrations for each category on an annual basis.[54]

The Department of Land Management and Archives has established a Public Access Model (PAM) for providing online services for all land related matters starting from registration of land.[55] Under PAM, the Department of Land Management and Archives has provisioned for the Land-service Center wherein all data collected relating to land within the territory of Nepal can be accessed by any entity who has obtained license for land service center. It has to be noted that such information cannot be accessed by the general public. The Survey Department, under the Ministry of Land Management, Cooperatives and Poverty Alleviation also provides information such as map of land/blueprint which is in the format of CAD files, field book and cluster register of any property, once the citizenship and land registry book are submitted on its

---

50 Blacklist, Central Investigation Bureau, available at "https://cibnepal.org.np/assets/upload/block/blacklist_upload_2080-12-01_05_30pm.pdf"

51 Available at "https://ocr.gov.np/"

52 Section 25, Company Act 2063 (2006)

53 Industrial Satistics 2079/80, available at "https://doind.gov.np/detail/218"

54 Industrial Satistics 2079/80, available at "https://doind.gov.np/detail/218"

55 Available at "https://dolma.gov.np/office/dept/content/description-of-public-access-module-1634724366"

portal.[56]

[56] Available at “https://merokitta.dos.gov.np/”

4 Open Data/Content

4.1 Archives Preservation Act

The Archives Preservation Act, 2046 (1986)[57] (the "**Archives Act**") was enacted on May 28, 2008. It defines a 'document' as any handwritten text, book, picture, photograph, map, plan, chart, file, as well as original copies or copies stored in film, microfilm, tape (sound record), film, computer disk, or computer cassette.[58]The Archives Act provides for the establishment of a national archives responsible for maintaining records in a systematic and secure manner.[59]

Documents deemed of national significance from historical, religious, cultural, literary, economic, or other point of view are to be preserved by the National Archives as national property.[60] The classification of records is done by the National Archives which are based on factors such as antiquity, originality, cultural, economic, literary, regional, and thematic importance, as well as the materials used in their creation.[61]

Additionally, the Act outlines 'Prohibited records' which are safeguarded by the National Archives to ensure restricted access.[62] Only authorized individuals are permitted to view, move, or copy such records for a specified or unspecified duration.[63] Individuals are granted access to non-prohibited records upon application to the National Archives in the prescribed format and payment of applicable fees.[64] Whereas, it also actively excludes the disclosure of 'Prohibited records' where such records are defined in a precise manner and could include any document which is marked as prohibited by the National Archives or is prohibited from national perspective.

To enhance accessibility and efficiency, a digital access mechanism should be introduced, allowing non-prohibited records to be accessed through an online portal. This would significantly reduce the reliance on manual applications, streamlining the process for researchers, historians, and the general public.

First, efforts should be made to digitize all non-prohibited records, ensuring they are systematically archived and available in a structured format. By creating a secure and user-friendly online system, individuals can retrieve historical data without unnecessary bureaucratic delays. Additionally, the system should include search and indexing features to improve usability and quick access, along with appropriate security measures to ensure that any sensitive information remains protected. To maintain control over access, a permission-based system can be implemented, ensuring that different categories of records are accessible only to authorized users where necessary.

---

57 Amended in 2075 (2021), Available at " https://lawcommission.gov.np/np/wp-content/uploads/2021/01/%E0%A4%85%E0%A4%AD%E0%A4%BF%E0%A4%B2%E0%A5%87%E0%A4%96-%E0%A4%B8%E0%A4%82%E0%A4%B0%E0%A4%95%E0%A5%8D%E0%A4%B7%E0%A4%A3-%E0%A4%90%E0%A4%A8-%E0%A5%A8%E0%A5%A6%E0%A5%AA%E0%A5%AC.pdf"

58 Section 2.1.1, Archives Preservation Act, 2046 (1986)

59 Section 3, Archives Preservation Act, 2046 (1986)

60 Section 7, Archives Preservation Act, 2046 (1986)

61 Rule 4, Archives Preservation Rule, 2063 (2007)

62 Section 9, Archives Preservation Act, 2046 (1986)

63 Section 10, Archives Preservation Act, 2046 (1986)

64 Rule 5, Archives Preservation Rule, 2063 (2007)

While a fee structure may be necessary to cover maintenance costs and ensure the long-term sustainability of the system, it is important to acknowledge that it could create financial barriers for some users. Therefore, a balanced approach should be taken, such as implementing tiered pricing, subsidies for researchers, or free access to certain public-interest records, to ensure that historical data remains as accessible as possible while maintaining the integrity of the digital archive.

4.2 Open Government Partnership and Open Government Data

The Open Government Partnership (the "**OGP**") provides a unique platform for national governments to develop a multilateral, coordinated effort to make their societies more transparent, accountable and responsive.[65][66] It addresses the demand of citizens all over the world for greater openness and transparency from their government. There are 75 countries and 104 local jurisdictions who are member of the OGP. Nepal is not a member of OGP.

Nepal can become a member of OGP to support the open government initiatives but there are challenges that the Accountability Lab has identified for Nepal to adopt the open government agenda. The OGP challenges in Nepal are related to service delivery, followed by corruption, access to information, lack of citizen participation, lack of data, access to justice/rule of law and lack of private sector accountability, structural challenges like capacity and coordination issues within government, lack of local ownership of the development process, issues of organizational culture and a lack of accountability among civil society.[67][68]

Nepal is eligible to become a member of OGP which would provide a variety of benefits including technical and peer support and international open governance platform and a means to engage civil society. OGP has only been incorporated in the SDGs of Nepal where it supports the idea of integrating open government into monitoring and reviewing implementation of the SDG.

The Open Government Data (the "**OGD**") is a global approach towards sharing government information. It involves systematically sharing government data in a format that allows citizens to download, analyze, and use it freely. The OGD aims to improve the understanding of the citizens about government actions, enhance engagement with decision-makers, and hold the government accountable. It is a proactive approach towards disclosure of raw data on public platforms.[69][70]

To realize the goal of OGD in Nepal, a technical platform for sharing data and promoting data literacy both within and outside of the government must be established and a comprehensive government-wide strategy for OGD must be developed. Such a strategy should be integrated into the existing legal frameworks to provide a structured approach to data sharing in Nepal. In this regard, a centralized open data portal can be established, which could be used as a one-stop

---

65 Accountability lab, available at "https://www.accountabilitylab.org/wp-content/uploads/2020/01/nepalOGP-readinessAssessment-2017sep-v3r0.pdf" (last accessed on 5th October, 2023)

66 "PDF," n.d.

67 ibid

68 "PDF," n.d.

69 Open Nepal, Available at "https://opennepal.net/sites/default/files/doc_briefings/Briefing-Open-Government-Data-(English).pdf"

70 "PDF," n.d.

access point for government database. Additionally. To ensure the success of this initiative, the government should establish clear guidelines on data accessibility, security, and usability. Additionally, fostering collaborations with the private sector, academia, and civil society can help maximize the value of open data, leading to improved public services, evidence-based policymaking, and increased civic engagement.

Therefore, embracing OGP and OGD is a means to enhance transparency, accountability, innovation, and economic growth in Nepal. Although, the OGD and OGP both promote pro-active disclosure of data it is yet to be implemented in practice.

4.3 Right to Information Act

The Right to Information Act, 2064 (2007) (the "**RTI Act**") was enacted to promote transparency and accountability in government functions, ensure easy access for citizens to public information, protect sensitive information affecting national and citizen interests, and safeguard the citizen's right to be well-informed. RTI Act provides for the protection of personal information against unauthorized publication and broadcasting.[71]('Right to Information Act, 2064 (2007).pdf', no date). Further, it also provides that a public body has to keep its information updated.[72]

The RTI Act provides for a reactive approach towards access to information held by the government. It is seen to be reactive since it can only be accessed once a citizen files a request to obtain any information following the given procedure.[73] The interviewee from the National Information Commission, Nepal indicated that the accuracy of information provided by any public body under the use of the RTI Act is generally reliable, although instances of incomplete disclosure are not unusual. However, organizations typically respond promptly to requests for additional or complete information when such discrepancies are brought to their attention.

The RTI also has provisions for proactive disclosure of information as it mandates public bodies to update their information on a regular basis and make it public.[74] Therefore, it has provisions for both reactive and proactive disclosure of information. But for proactive disclosure to be more effective the interviewee suggested that there must be digitization of all governmental records and use of open software's has to be mandated and emphasized that lack of digitization is considered as the biggest problem for the enforcement of RTI. This would increase the access to information for the RTI office as all the data would be readily available and the problem of incomplete disclosure would not be there. The interviewee expressed such thoughts as the use of FOSS can increase transparency, accountability and interoperability, hence increasing the free flow of information and making it more accessible to its citizens.

One of the exceptions provided in the RTI Act for public bodies to withhold informationare the matters pertaining to national security, sovereignty of the nation and matters which have severe effect on commercial and banking interests are information which may not be revealed by the public bodies. Furthermore, the interviewee from the National Information Commission informed us that, regarding information confidentiality, the RTI office makes a claim that when information is withheld or kept confidential, it is not to conceal it from citizens but rather to uphold national security or prevent potential harm if the information were made public.

---

71 Section 28, Right to Information Act, 2064 (2007)
72 Section 5, Right to Information Act, 2064 (2007)
73 Section 7, Right to Information Act, 2064 (2007)
74 Section 4, Right to Information Act, 2064 (2007)

Consequently, information that could potentially incite unrest or conflict among groups or citizens is kept confidential until the situation stabilizes. But it has to be kept in mind that the interviewee from the RTI office is a government officer and their views would reflect the same, hence there is inherent biasness.

Therefore, the RTI promotes transparency and accountability by mandating that public bodies disclose information and respond to citizen requests. However, to enhance efficiency and accessibility, a more proactive approach should be adopted. This can be achieved through the full digitization of government records and the mandatory use of open-source software to ensure cost-effective and secure data management. Additionally, government bodies should proactively disclose updated information online through a centralized platform, reducing reliance on RTI requests and minimizing bureaucratic delays, ultimately strengthening public trust and civic engagement.

The Concept Paper Regarding the Use of AI in Nepal, 2081 (2024) (the "**AI concept paper**")[75] emphasizes the necessity of developing a comprehensive national policy for AI that encompasses cybersecurity, data protection, and user privacy. It highlights the importance of ensuring that these policies align with international standards. The paper underscores the need to draft and implement a National AI Policy, National AI Strategy, AI Act, Data Protection Framework, Data Protection Policy, Data Protection Act, and Sectoral AI Guidelines. Additionally, it proposes the establishment of a dedicated nodal agency for AI research and development, as well as the creation of an integrated national portal for AI-related data exchange.[76]The AI concept paper presents a comparative analysis of AI usage strategies from various entities, including the European Union, United Nations, Nordic-Baltic region, UAE, India, Argentina, Australia, Brazil, Canada, Chile, China, Denmark, Finland, France, Germany, Italy, Singapore, and South Korea.

Therefore, the AI concept paper provides that to effectively integrate AI into national policies, it is essential to[77]:

Formulate a National Policy and Strategy on AI and Data Protection, aligning with international standards and sectoral laws to safeguard user privacy.

Establish a governance structure for AI, ensuring developers comply with national and international standards. A dedicated body should oversee AI use, promotion, and regulation, encouraging self-regulation.

Promote research and development in AI, enhancing transparency, accountability, and cooperation.

Accelerate AI adoption across various sectors by incorporating AI into policy strategies and programs.

Prioritize capacity development through reskilling and upskilling to ensure the availability of skilled manpower, thus fostering AI development and use.

Take public opinions and suggestions through the Ministry's website and other channels, and integrate necessary additions.

---

75 "PDF," n.d.

76 Clause 13, Concept Paper Regarding the Use of AI in Nepal, 2081 (2024)

77 Clause 16, Concept Paper Regarding the Use of AI in Nepal, 2081 (2024)

While the development of an AI policy and strategy is crucial for Nepal, its implementation in a resource-limited environment remains a challenge. To address this, Nepal should foster collaboration with international AI bodies, allowing it to leverage technical expertise, research, and best practices. By engaging with global AI institutions, academic networks, and technology partners, Nepal can gain access to capacity-building programs, knowledge-sharing platforms, and funding opportunities. Such collaborations can help overcome technical and infrastructural limitations, ensuring that AI policies are not only well-designed but also implemented practically in the context of Nepal.

5 Open standards/Open software

5.1 National Cybersecurity Policy and NeGIF

In the National Cybersecurity Policy, 2080 (2023) the use of Open standards is encouraged to facilitate interoperability and data exchange between various information technology systems and services.[78][79]. During the interviews conducted with representatives or interviewee from various government agencies, diverse perspectives emerged on the topic of use or meaning of open standard. The interviewee from the Department of Information Technology (the "DOIT") conveyed that while the National Cybersecurity Policy of 2080 (2023) advocates for open standards, it does not enforce their usage, rather, it encourages the adoption of globally recognized standards and software. Conversely, the interviewee from the Government Integrated Data Center (the "GIDC") and the Ministry of Communication and Technology articulated concerns regarding the utilization of open standards or open-source software. They highlighted potential risks associated with such software, noting that their unrestricted accessibility could heighten vulnerabilities in data protection for the government of Nepal.

The Nepal E-Government Interoperability framework (the "NeGIF")[80][81] was drafted by PricewaterhouseCoopers International Limited (PwC) for the Ministry of Communication and Information Technology, Nepal which was made for the enhancement of the information and communication technology in Nepal. The NeGIF provides a framework for sharing, collaborating and integrating information with the use of common standards. It highly recommends and encourages the use of open standards and open-source software for better interoperability to achieve the goal of better governance, providing faster services and reducing the redundancy of information. It provides for a comprehensive plan and detailed standards with the best practices around the world for the implementation of open source and open standard for interoperability within the government of Nepal (G2G), between the government of Nepal and its citizens (G2C), between government of Nepal and private sector businesses (G2B), between government of Nepal and its employees (G2E).

The NeGIF promotes the use of open standards and highlights its importance to increase access to information by the general public and to increase transparency within the working of the government. The NeGIF has not been implemented so far, despite it being published in 2011 which provided a detailed report showing the advantages and importance of open standard mandates. The failure of implementation of open standard policies is the main reason for the lack of interoperability within various government bodies and overlapping or delay in information sharing in government offices. Through the interviews with various governmental organizations, it has come to light there are no interoperability framework for government bodies and it cannot be seen practice as well. The governmental bodies work with each other based on mutual understanding which can be very subjective.

The NeGIF and National Cybersecurity Policy, 2080 (2023), encourages the use of open standards to facilitate interoperability and data exchange between various information technology systems and government agencies. While they emphasize the technical aspects of data sharing and

---

78 Rule 11.17, National Cyber security Policy, 2080 (2023)

79 National Cyber Security Policy, 2080 (Nepali).

80 ,PWC,'Nepal E-Government Interoperability framework-Main Report', available at "https://nitc.gov.np/assets/img/fileSystem/download/23-07-27-125812-NeGIF%20Main%20Report%20v2.0%20new.pdf" (last accessed on 7th October, 2023)

81 "PDF," n.d.

interoperability, they do not explicitly advocate for proactive data disclosure aimed specifically at providing access to information to the general public. The NeGIF, however, does highlight the importance of open standards in increasing access to information and transparency within government operations, which can indirectly contribute to proactive data disclosure. But, the focus remains more on interoperability and the technical framework rather than on direct public access and proactive data transparency initiatives. However, since both of these instruments are not implemented into practice, its objectives are still needs to be fulfilled.

Therefore, proactive data disclosure mandates should be incorporated into both NeGIF and the National Cybersecurity Policy,2080 (2023) to enhance transparency and public accessibility. Ensuring that data shared between government agencies is also made available to the public at appropriate times will promote accountability, informed decision-making, and trust in digital governance. Clear guidelines should be established to determine what data can be disclosed, when, and in what format, balancing openness with security and privacy considerations.

5.2 Nepal QR Laws

The Nepal Rastra Bank which is the Central bank of Nepal with the aim of standardization of QR codes for electronic financial transactions, has put forward the Nepal QR Standardization Framework and Guidelines, 2077 (2020):[82][83] This framework provides an alternative to cash or debit/credit cards for the convenience of the customers or merchants or citizens of Nepal by promoting digital payments in Nepal. Even though Nepal is a very backward country in terms of technology the adoption of QR based payments has rapidly grown since the enactment and adoption of this QR guideline. Therefore, there was a need for the QR standardization framework and guideline as the QR codes were closed loop and non-interoperable i.e., the QR code could be scanned and paid using only their consumer apps, so multiple apps needed to be downloaded to pay at multiple retailers whose QR code was acquired by multiple providers such as Esewa, Khalti, or any banks. Hence, the Nepal QR Standardization Framework and Guidelines, 2020 was implemented for a standard procedure for payment for interoperability, scalability and security.

The Nepal QR Standardization Framework and Guidelines, 2077 (2020) (the "**QR Guidelines**" prioritizes customer security. It provides for the security and confidentiality of personal data and includes provisions to protect against any anticipated threats or hazards to the security and confidentiality and integrity of personal data. The QR Guidelines also requires that the 'issuer' takes steps to protect against any actual or suspected unauthorized processing, loss or unauthorized acquisition of any personal data, ensure the proper and secure disposal of personal data, and mandates requisite audits and submission.[84] Further it provides for the customer awareness and education.[85]

This QR Guidelines can be seen as a secured step towards digitization of payment methods with an aim to standardize the payment method all over Nepal with interoperability with the Central Bank of Nepal. Therefore, though it provides for the safeguard of the data and interest of the citizens such as risk and compliance measures to be taken by service providers which include

---

82 Nepal QR Standardization Framework and Guidelines, 2020, available at "https://www.nrb.org.np/contents/uploads/2021/01/QR-Code-Guidelines-and-Framework-and-Specifications.pdf" (last accessed on 5th October, 2023)

83 "PDF," n.d.

84 Rule 4.11(7), Nepal QR Standardization Framework and Guidelines, 2020

85 Rule 4.12, Nepal QR Standardization Framework and Guidelines, 2020

following fraud and risk management protocols, building velocity checks at the interface level, annual compliance assessment, etc[86], but it does not proactively promote openness or disclosure of data and must be noted that it uses a proprietary standard developed by a private company EMV Co.

5.3 Nagarik App

The Nagarik App (Operation and Management) Directive, 2078 (2021) was introduced to establish interconnectivity among electronic information systems in public bodies. Its aim is to facilitate the swift, cost-effective, and efficient flow of services and information to citizens through a unified electronic system.

The Nagarik App is defined as a software application designed to function on various electronic devices such as computers, mobile phones, tablets, or any similar electronic device.[87] Registration on the Nagarik App is exclusively for Nepalese citizens, who must register using a mobile phone with a SIM card registered under their name, along with providing their citizenship ID details.[88] The information provided by the applicant will undergo verification against the records stored in the National Identity Card Administration System, Citizenship Management System, Nepali Passport Information System, and the Electoral Roll Management System. Should any discrepancies arise between the provided details and the existing system records, the applicant will be notified accordingly, and their application will be declined.

The interviewee from GIDC also informs us that they are responsible for the management and operation of the Nagarik App and it is their innovation to tackle the problem of lack of interoperability by creating an application that would contain all government record of an individual in a single app. He informed that the collection, usage, disclosure, storage, security and disposal of our personal information and data is governed by the Privacy Act. This can also be considered as an important step towards improving interoperability and interconnection between various government agencies.

However, ensuring robust data security within the Nagarik App is crucial to maintaining the integrity and reliability of government digital services. Implementing strong encryption, strict access controls, and periodic security audits will help protect sensitive information and mitigate the risks of data breaches and unauthorized access. A well-defined security framework within the app is essential to ensuring secure and reliable data exchange between citizens and government services.

[86] Rule 4.9, Nepal QR Standardization Framework and Guidelines, 2020
[87] Section 2 (c), Nagarik App (Operation and Management) Directive, 2078 (2021)
[88] Section 3, Nagarik App (Operation and Management) Directive, 2078 (2021)

6 Decreasing openness

The laws are as follows:

Constitution of Nepal, 2072 (2015), The Privacy Act, 2075 (2018), Individual Privacy Regulation, 2077 (2022), Electronic Transaction Act, 2063 (2008) (the "ETA"), Directives for Managing the Use of Social Networks, 2080 (2023) National Civil (Code) Act, 2074 (2017) The Copyright Act, 2059 (2002) Patent, Design and Trademark Act, 2022 (1965) Telecommunication Act, 2053 (1997) Press and Publications Act 2048 (1991) Unified Directives issued by the Nepal Rastra Bank to "A", "B" and "C" Category Certified Institutions,2079 (2023)[89] Payment System Unified Directive,2079 (2023)[90],and Circular issued by Nepal Rastra Bank regarding Foreign Exchange Transactions,2079 (2023)[91] Right to Information Act, 2064 (2007)

6.1 The Constitution of Nepal

The Constitution of Nepal does not specifically provide for data governance or protection of data but it does provide the right to privacy which is accorded the status of fundamental right under the Constitution,[92][93] where it provides that personal information and data relating to any person shall be protected. In order to safeguard such fundamental rights legislation like the Privacy Act, 2075 (2018) and Individual Privacy Regulation, 2077 (2022) were enacted.

6.2 National Civil Code Act

The National Civil (Code) Act, 2074 (2017) also provides for the right to privacy of a person's body, residence, property, document, correspondence, or information.[94][95] It provides that the right to privacy is deemed to be violated, if any person, without obtaining consent and not in accordance with the law, engages in activities such as entering someone's residence, opening or using their correspondence, recording or listening to their conversations, watching, publishing, or broadcasting their personal activities, taking their photograph, or imitating their name, image, or voice for public dissemination.[96] However, actions taken for literary, artistic purposes, or public interest do not constitute a violation of the right to privacy.

---

89 available at "https://www.nrb.org.np/contents/uploads/2023/02/Unified-Directives-2079-Magh-published.pdf" (last accessed on 3rd October, 2023)

90 available at "https://www.nrb.org.np/contents/uploads/2023/01/PSD_unified-Directive-2079_Letter-combined.pdf" (last accessed on 3rd October, 2023)

91 available at "https://www.nrb.org.np/contents/uploads/2023/04/FXMD-Circular-18_2079.80_Unified-Circular-2079.pdf" (last accessed on 3rd October, 2023)

92 Article 28, Constitution of Nepal, 2072 (2015)

93 "PDF," n.d.

94 Section 20, National Civil (Code) Act, 2074 (2017)

95 "PDF," n.d.

96 Section 21, National Civil (Code) Act, 2074 (2017)

97 Personal information is defined as the following: His or her caste, ethnicity, birth, origin, religion, colour or marital status; His or her education or academic qualification; His or her address, telephone or address of electronic letter (email); His or her passport, citizenship certificate, national identity card number, driving

6.3 Privacy Laws

Privacy Act, 2075 (2018) (the "**Privacy Act**"), defines the term "Personal information"[97] as the information associated with the individual person.[98][99]

The Privacy Act also provides for the privacy of data, where Section 12 of the Privacy Act provides as follows: Every person shall have the right to keep the personal data or details related to him or her confidential. While collecting personal or family data of any person, his or her consent shall be obtained. The data collected by a public body or body corporate upon obtaining the consent of the concerned person shall be used only for the purpose for which such data have been collected. Provided that if any data are demanded for the national security or peace and order, it shall not be deemed to bar to provide such data in accordance with the prevailing law. No person shall, without obtaining the consent of another person, provide the following data related to that person to anyone else or publish, or cause to be published, such data: (a) Details relating to health examination, (b) Details relating to property and income generation, (c) Details relating to employment, (d) Details relating to family matters, (e) Biometric details and thumb impression, (f) Signature or electronic signature, (g) Details relating to political affiliation and election, (h) Details relating to business or transaction. Notwithstanding anything contained in sub-section (4), in cases where it is necessary to provide any personal data or details to the court or the agency or official authorized under law in the course of investigation of any criminal offence, such data or details shall be provided. Notwithstanding anything contained in sub-section (4), if there arises a question as to the issues such as age, qualification, character, sexuality, disability of any person, and the authorized official so demands, the concerned person shall provide such details or documents.

The Privacy Act also defines "Sensitive Information" as (a) His or her caste, ethnicity or origin, (b) Political affiliation, (c) Religious faith or belief, (d) Physical or mental health or condition, (e) Sexual orientation or event relating to sexual life, (f) Details relating to property. It also prohibits processing of such sensitive information by any public body, but it can be processed in the given circumstances (a) In the course of alleviation of disease, public health protection, disease identification, health treatment, management of health institution and providing health service by the licensed doctor in the concerned subject or by the health worker under direction of the licensed doctor, without insulting or letting the concerned person feel inferior. (b) If the concerned person has published the information himself or herself.[100]

The Privacy Act does provide that consent of the concerned person must be taken before processing any data by a public body or body corporate but an exception is provided that an authorized person by the law can collect such data.[101] Unlike GDPR, other exceptions for data processing and disclosure are not provided under the Privacy Act.

---

license, voter identity card or details of identity card issued by a public body; A letter sent or received by him or her to or from anybody mentioning personal information; His or her thumb impressions, fingerprints, retina of eye, blood group or other biometric information; His or her criminal background or description of the sentence imposed on him or her for a criminal offence or service of the sentence; and Matter as to what opinion or view has been expressed by a person who gives professional or expert opinion, in the process of any decision.

98 Section 2 (c), The Privacy Act, 2075 (2018)

99 "PDF," n.d.

100 Section 27, the Privacy Act, 2075(2018)

101 Section 23, The Privacy Act, 2075 (2018)

The Privacy Act provides for a provision for the collection of personal data only with the consent of the subject and to be kept confidential in accordance to the law. The personal data collected should be relevant to the purposes for which they are to be used and kept up to date.[102]

It further provides for the privacy of the personal information, document, correspondence, data or character remained in electronic means and not to contravene by providing such information in an unauthorized manner.[103] It also provides for the protection of processing sensitive information, where the physical and mental health come under the purview of sensitive information.[104]

Further, it provides that any Public Body or Body Corporate can provide the personal information only with the consent of the concerned person, except while collected by or remained under the responsibility or control of the authority for any kind of investigation or moral purpose.[105] One of the interviewee also stated that access to data has to be more restrictive because of the cyber-attacks in Nepal. As per the interviewee the understanding of the government is that restricting data means keeping data safe.[106]

The Individual Privacy Regulation, 2077 (2020) also provides that the details relating to economic, social, religious, physical or mental health of any individual, collected and stored in the digital medium must not be used without the consent of the concerned person.[107] The purpose of collection of personal information pursuant to this Regulations has to be informed to the concerned person prior to the collection of the personal information and has to be used to extent of the purpose for which is collected.[108][109]

The laws of Nepal do not explicitly provide provisions for data controllers however; the personal information received by any public or private sector cannot be stored or shared without the consent of the concerned person. It is the obligation of the public body to make appropriate arrangements against unauthorized access likely to occur to personal information, or against the possible risk of unauthorized use, change, disclosure, publication, or transmission of such information.[110] Therefore, reviewing the current laws, it can be concluded that the personal data relating to health of an individual can be processed as long as prior consent of the patient is taken.

Any action deemed to contravene the Privacy Act is considered a criminal offense as recognized by the National Criminal Procedure Code, 2074 (2017). In such cases, the Nepal Police are responsible for handling the legal proceedings. The punishment for these offenses may entail imprisonment for a term not exceeding three years, a fine not exceeding thirty thousand rupees, or both.[111]

The Privacy Act is the parent act having a broader framework that defines terms such as 'Personal information'. It sets out overarching principles for the protection of any persons right to privacy, whereas the Individual Privacy Regulation is its subordinate legislation only covering some matters relating to a person's individual privacy. In practice, it is essential to look at the

[102] Section 12, The Privacy Act, 2075 (2018)
[103] Section 19 (1) (2), The Privacy Act, 2075 (2018)
[104] Section 27, the Privacy Act, 2075(2018)
[105] Section 26, The Privacy Act, 2075 (2018)
[106] Interview with DOIT, Annex-4
[107] Rule 5, Individual Privacy Regulation, 2077 (2020)
[108] Rule 11 (1) & (2), Individual Privacy Regulation, 2077 (2020)
[109] "PDF," n.d.
[110] Section 25, The Privacy Act, 2075 (2018)
[111] Section 29, The Privacy Act, 2075 (2018)

parent act and the subordinate legislation together to ensure a comprehensive understanding and effective implementation of the legal framework relating to the right to privacy.

To enhance the protection of personal data and safeguard individual privacy rights, the Privacy Act and Individual Privacy Regulation must be amended to include provisions for the right of data subjects, modeled after the GDPR. This inclusion would empower individuals with rights to access, rectify, erase, restrict processing, and object to data processing. It could also introduce mechanisms for data portability and the right to be informed along with the need for explicit consent, aligning the Privacy Act with global best practices in data protection. Adopting these rights will provide individuals with greater control over their personal data and strengthen privacy protections in an increasingly digital world.

6.4 Nepalese legal system versus General Data Protection Regulation (the "GDPR")

When comparing the prevailing laws of Nepal with that of the other internationally practiced data governance regulation such as the GDPR, it can be observed that Nepali privacy laws need to through a set of reforms.

The GDPR was enacted on 25th May 2018, which was designed to safeguard the privacy and personal information of individuals within the European Union (EU). It provides a comprehensive outline for the collection, storage, processing and sharing of personal data by any organization. The GDPR grants individuals enhanced control over their personal information, by empowering them with the right to access, correct and erase their data.

'Personal data' is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[112] Whereas, Consent is defined as "consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".[113]

The GDPR provides for the right to access any data concerning an individual.[114] It allows any person to access any data collected by a company and also to request a copy of such personal data stored which has to be provided to the concerned individual. It also provides for a right to be informed in case any personal data is transferred to a third country or an international organization.[115] Therefore, it allows any person to be informed about the personal data regarding them being processed by any institution which is a fundamental right enshrined under the constitution of Nepal, but such a provision/law is not available in Nepal. It also provides for the right to restriction of processing, so even if personal data is collected an individual has the power or authority to refuse such processing.[116] Though we give our consent for the processing of our persona data, we ourselves cannot see or check the same in any manner.

---

[112] Article.4, General Data Protection regulation (2016)
[113] Article 4 (11), General Data Protection regulation (2016)
[114] Article 15, General Data Protection Regulation (2016)
[115] Article 15 (2), General Data Protection Regulation (2016)
[116] Article 18, General Data Protection Regulation (2016)

The "right to be forgotten"[117] is provided under the GDPR which provides that any company, as well as any other affiliated entities using our data, will be erased. Such data shall be erased when the purpose for which personal data was collected is no longer necessary and also if the person withdraws consent or objects for processing such data. It also provides for the rectification of personal data if it is found that any information pursuant to a person is inaccurate.[118]GDPR provides for the processing of personal data related to criminal conviction and offences. The GDPR establishes a Controller and data protection officer whose main role is to monitor the compliance of GDPR by any organization. The ETA also provides for the appointment of a Controller and deputy Controller, but the role of these entities varies a lot. Under the ETA the main role of the Controller is to monitor the authority which issues license for digital signature certificates.

The provisions outlined in the GDPR highlight comprehensive measures aimed at safeguarding the privacy and personal information of individuals within the European Union (EU). However, upon comparing these provisions with the existing laws of Nepal, it becomes evident that Nepal's legal framework lacks several key aspects crucial for robust data protection. The GDPR grants individuals enhanced control over their personal information, empowering them with rights such as access, correction, and erasure of their data. However, similar provisions ensuring such rights are notably absent in the laws of Nepal. Furthermore, the GDPR defines 'personal data' extensively and emphasizes the importance of obtaining clear and unambiguous consent for data processing. In contrast, Nepal's laws lack clarity and specificity in defining personal data and the requirement of consent though present in the laws such as the Privacy Act, is not seen to be exercised properly. Moreover, the GDPR establishes fundamental rights such as the right to access personal data, the right to restriction of processing, and the right to be forgotten. These rights ensure transparency and accountability in data processing practices, yet such provisions are missing in Nepal's legal framework. The laws of Nepal does provide for the restriction on processing of sensitive information.

The GDPR addresses the processing of personal data related to criminal convictions and offences, ensuring comprehensive protection for individuals. However, Nepal's laws do not provide explicit provisions regarding the processing of such sensitive data.

Furthermore, the GDPR provides for the role and responsibilities of that of a controller and data protection officer in order to monitor compliance with data protection regulations. While Nepal's laws also mention the appointment of a Controller and deputy Controller, their roles primarily focus on monitoring digital signature certificate issuance, lacking the comprehensive oversight provided by GDPR. Even after the adoption of the Privacy Act 2018, many executives remain uncertain about its implications for data storage and usage. A chief technology officer stated that they rely on the General Data Protection Regulation to shape their internal data storage policy, as they perceive a lack of effective implementation or explanation of the Privacy Act 2018 by the government.[119]

In conclusion, the absence of key provisions from Nepal's data protection laws such as the principles for processing of personal data, cross-border transactions, roles of the controller and data protection officer by the GDPR indicates a significant gap in the laws of Nepal when

---

117 Article 17, General Data Protection Regulation (2016)

118 Article 16, General Data Protection Regulation (2016)

119 The World Bank, "Use of data in the private sector of Nepal the current state and opportunities in finance, education and the media" (July 2020) pg.12, available at "https://documents1.worldbank.org/curated/en/805261601023506163/pdf/Use-of-Data-in-the-Private-Sector-of-Nepal-The-Current-State-and-Opportunities-in-Finance-Education-and-the-Media.pdf"

compared to the GDPR. The key gaps to make our data governance structure more secure and enhance data protection standards and ensure alignment with international best practices are:

Lack of definition of Consent Lack of right to be forgotten Lack of right to restriction on processing and right be informed about processing of personal information must be added Lack of right to erasure Lack of right to rectification Lack of responsibilities and duty of Data Controller Lack of Data Protection Officer Lack of laws for data localization Lack of laws governing cross-border exchange of data and trading[120]

The absence of provisions addressing cross-border data transfers, lack of data subject rights, and the absence of data breach notification requirements highlights significant gaps in the legal framework that need to be addressed to bring Nepal's laws in line with global best practices.

Under the GDPR, cross-border transfers are strictly regulated to ensure that data shared with foreign entities remains subject to adequate protection. Without such provisions, Nepali citizens' personal data may be exposed to foreign jurisdictions with weaker data protection laws, increasing the risk of misuse or unauthorized access. To make Nepal's laws more robust and aligned with GDPR standards, it is essential that provisions be introduced to regulate cross-border data transfers, ensuring that data is protected in accordance with local laws even when it is processed abroad. International agreements such as data transfer agreements can help ensure that foreign entities uphold similar data protection standards when handling Nepali citizens' data.

As mentioned above, the legal framework of Nepal currently lacks rights of data subject, including the right to access, rectify, or erase personal data. These rights are fundamental under the GDPR and serve as a cornerstone of data privacy. They empower individuals to control their personal information and protect it from misuse. Without these rights, data of individuals are left vulnerable to unauthorized data processing, which can result in privacy violations. To bring laws of Nepal for data protection in line with GDPR, it is necessary to introduce these rights, as they not only provide individuals with greater control over their data but also foster trust between citizens and both private and public institutions.

Moreover, the absence of mandatory data breach notification requirements represents another significant gap in Nepal's legal framework. GDPR mandates that organizations notify affected individuals promptly in the event of a data breach. This requirement ensures transparency and accountability, helping to mitigate the harm caused by data breaches. To enhance data protection in Nepal, the introduction of a similar legal obligation for timely data breach notifications is critical to ensure that citizens are informed and that organizations are held accountable for protecting personal data.

The above provisions must be incorporated from the GDPR into the laws of Nepal in order to strengthen privacy rights, improve transparency, and bolster accountability in data processing practices, thereby positioning Nepal on par with global standards in data protection.

However, transitioning to a framework like GDPR requires a phased and contextualized approach that considers the country's unique political and socio-economic landscape. While aligning with international best practices is crucial for ensuring robust data protection, a direct adoption without modifications could pose practical challenges. Nepal must first establish a dedicated data protection authority with clear enforcement mechanisms, ensuring regulatory oversight and accountability. Additionally, legal reforms should be introduced in stages,

[120] Interview with DOIT, Annex-4

prioritizing fundamental rights such as data access, rectification, and erasure before expanding to more complex compliance requirements.

Given the economic structure of Nepal, particularly with reference to SMEs and resource constraints within regulatory bodies, capacity-building programs, public awareness campaigns and financial support mechanisms would be necessary to facilitate compliance. A multi-stakeholder approach, involving government agencies, the private sector, and civil society, is crucial to balance privacy, economic growth, and technological advancement. Learning from countries with established data governance frameworks, such as the EU, UK, and Singapore, and engaging foreign experts will help design a system tailored to Nepal's needs while aligning with global standards.

Therefore, by contextualizing the realities within Nepal and drawing from global expertise, Nepal can gradually implement GDPR-aligned standards by avoiding disruptions to businesses or overburdening regulatory bodies. A well-structured roadmap combining legal, institutional and economic factors will ensure sustainable and effective modernization of data protection framework within Nepal.

6.5 Electronic Transaction Act, 2063 (2008) (the "ETA")

The ETA defines "Data" as the "presentation of information, knowledge, fact and concept or instructions in any form, which are kept in a formalized manner in a computer system or computer network and is intended for processing the same, or processed or stored in computer memory."[121][122]. Data includes electronic record as well[123] and it defines "Computer Database as "information, knowledge and concept or presentation of instructions, which are being prepared or have already been prepared in word, image, voice or audio-visual form in a formalized manner or which have been produced by a computer, computer system or computer network, with a view to use in a computer, computer system or computer network."[124]

The ETA also gives legal recognition to electronic records[125] and digital signatures[126].

The ETA also provides that in case there is reasonable grounds to suspect that any provision of the legislation has been violated, the controller shall have the power to have access to such computer system, data, information system.[127] Therefore, government of Nepal designates a government officer for protection against cyber-crimes and data exploitation.

The ETA regulates cyber activity in Nepal, primarily it seeks to protect internet users against cybercrimes. The ETA does not specifically define cybercrimes but does provide for various provisions that deal with the issues about such crimes. Unfortunately, the provisions of the ETA are vague and are not comprehensive enough to address the varied challenges associated with complaints, investigation, prosecution, and adjudication of cybercrimes in Nepal. In this light,

[121] Section 2(k), Electronic Transaction Act, 2063 (2008)
[122] "The Electronic Transactions Act, 2063 (2008).Pdf."
[123] Section 2(v), Electronic Transaction Act, 2063 (2008)
[124] Section 2(e), Electronic Transaction Act, 2063 (2008)
[125] Section 4, Electronic Transaction Act, 2063 (2008)
[126] Section 5, Electronic Transaction Act, 2063 (2008)
[127] Section 28, Electronic Transaction Act, 2063 (2008)

the Government of Nepal has tabled the Information Technology Bill and the Cyber Crime Bill before the Parliament.

The ETA gives protection against cybercrimes but in the process of application of such law, in practice it gives way for the breach of personal data. This is so because in case of investigation of any sort of cybercrimes the device from which such crime is committed or any electronic device related to the crime is confiscated and all the personal information of the accused which is not linked to the particular crime is also investigated by the police officer. For eg: If a person is accused of publication of illegal material[128] via Facebook on their phone, then in such a case the phone is confiscated and even though only the Facebook profile or the particular publication made by the accused should be investigated the police officer has the power or misuses their power to investigate any other content available on the accused's phone. Therefore, the police officer can check their WhatsApp texts, photos, videos etc. which are not linked to the case in any manner. Hence, there is misuse of power by the investigating authority and personal information of any individual is breached.

The process of investigating cybercrimes involves seizing electronic devices. Discussions with multiple government agencies have revealed a concerning issue regarding individual privacy. It has been observed that during these investigations, not only the data relevant to the crime is scrutinized, but all data stored on the device is examined by the investigating authority, posing a significant risk to personal privacy. In the case of Adv. Baburam Aryal vs Office of Prime Ministers and Ors.[129] It was held that for the purposes of granting permission for the access to information necessary in the context of a criminal investigation, the relevant district court must give the order for such investigation.

Guidelines (Procedural) for Access to Information, 2074 (2017)[130] was promulgated in light of the above case to maintain procedural uniformity while accessing private information. The said guideline provides that the information received can only be used for the purposes of investigation and cannot be used for any other purposes.[131] It further provides that, when request for access to information is given it must clearly mention the exact required details such as call details, operational data (BTS, Location, SMS,CDR, User Details, Sim User location, Sim location, Call wise Location, Internet Activities Log, IP Address, etc.).[132] It also provides that confidentiality shall be kept with regard to the information collected which is the most important provision for the protection of privacy of any individual.[133] In case of any discrepancy with regard to the investigation, it provides that the decision of the judge shall be final and if the judge doesn't allow access to such information, it cannot be taken.[134]

The Nepal Telecommunication Authority (the "**NTA**") also has made directives with regard to such criminal investigation. The Directive for Internet Service Providers, 2077 (2021) provides that ISP should make available the information requested by Nepal Police or Law enforcement

---

128 Section 47, Electronic Transaction Act, 2063 (2008)

129 Writ no.069-WO-0268

130 Guidelines (Procedural) for Access to Information, 2074 (2017), available at "https://www.nta.gov.np/uploads/contents/%E0%A4%B8%E0%A5%82%E0%A4%9A%E0%A4%A8%E0%A4%BE%E0%A4%AE%E0%A4%BE_%E0%A4%AA%E0%A4%B9%E0%A5%81%E0%A4%81%E0%A4%9A_%E0%A4%B8%E0%A4%AE%E0%A5%8D%E0%A4%B5%E0%A4%A8%E0%A5%8D%E0%A4%A7%E0%A5%80_%E0%A4%A8%E0%A4%BF%E0%A4%B0%E0%A5%8D%E0%A4%A6%E0%A5%87%E0%A4%B6%E0%A4%BF%E0%A4%95%E0%A4%BE,%E0%A5%A8%E0%A5%A6%E0%A5%AD%E0%A5%AA.pdf"

131 Cause 3 (2), Guidelines (Procedural) for Access to Information, 2074 (2017)

132 Clause 7, Guidelines (Procedural) for Access to Information, 2074 (2017)

133 Clause 9, Guidelines (Procedural) for Access to Information, 2074 (2017)

134 Clause 11, Guidelines (Procedural) for Access to Information, 2074 (2017)

Agency for 365 days 24 hours (basically anytime) and should inform the NTA within 3 days of the same.[135] All licensed ISP shall immediately provide the Internet User Activity Log excluding content for 6 months to the investigation officers for investigation[136] and all licensed ISP will have to provide up to 3 months of internet NAT (Network Address Translation) Record to investigation officers for investigation.[137] Further, all service providers should update the customer's name and address within 24 hours after the customer's service is activated and within 1 week shall update the detailed information along with photo in its database.[138]

The NTA has also issued directives for voice service providers wherein provides for telecommunication service providers to provide 18 months of Operational Data (including SIM/ Call-Wise Location, Cell ID, IMEI, etc) up to 6 months Active (Live) and up to one year Passive (stored).[139] The telecommunication service providers should immediately provide at least 30 days of SMS details and 6 months of SMS logs to relevant agencies for investigation, and provide SMS details of up to 3 months shall be provided within 6 months. It also provides that all licensed ISPs shall immediately provide 6 months of Internet User Activity Log excluding content to the investigating officers. All ISP licensed service providers to provide 3 months of internet NAT (Network Address Translation) Record to investigation officers for investigation. All the service providers should update the customer's name and address within 24 hours after the customer's service is activated and the detailed information including photo within a week in the database of the service providers. Telecommunication service providers to provide the IMEI (International Mobile Equipment Identity) Number of mobile sets of Mobile Users/ Subscribers that have been in use within one year.[140]

Therefore, the ETA lacks a clear and comprhensive definition of cyber-crimes, which creates ambiguity in law enforcement and prosecution. To align with international best practices and ensure consistency in handling cyber-related offenses, the ETA should be amended to explicitly define cybercrimes and outline specific categories such as hacking, identity theft, cyberstalking, financial fraud, and online harassment. Categorizing these offenses will help establish a stronger legal foundation for prosecuting cybercriminals and protecting individuals from cyber-crimes.

Additionally, there is a need to set clear limitations on the scope of data that can be accessed during cybercrime investigations. Investigators should only have access to data that is directly relevant to the case, ensuring that personal information is not unnecessarily exposed. Without proper safeguards, unrestricted access to digital data may lead to violations of privacy rights and potential misuse of sensitive information. To prevent such risks, data access protocols should be established, requiring judicial or regulatory oversight before investigators can obtain personal data. Implementing these safeguards will ensure that investigations are conducted lawfully while maintaining a balance between law enforcement needs and individual privacy rights.

[135] Clause 1, Directive for Internet Service Providers, 2077(2021)
[136] Clause 2, Directive for Internet Service Providers, 2077(2021)
[137] Clause 3, Directive for Internet Service Providers, 2077(2021)
[138] Clause 4, Directive for Internet Service Providers, 2077(2021)
[139] Directive for Voice Service Providers, 2077 (2021)
[140] Directive for Voice Service Providers, 2077 (2021)

7 Directive for Managing the Use of Social Networks, 2080 (2023)

The Social Network Directive was made by the government of Nepal with the exercise of the power conferred by section 79 of the ETA.[141] It aims to regulate social network platform operators along with its users.

It defines 'Social Network' as a "network such as a group, blog and so on which provide facilities for a person, group or organization to communicate interactively with each other accordingly to the facilities and methods provided by the social network platform through electronic means of communication including computer, internet, and so on and the facility to disseminate content created by the users."[142] And defines 'Social networks platform' as the "internet or information technology- based operating systems that are available to the public such as Facebook, TikTok, Twitter, Viber, Pinterest, WhatsApp, Messenger, Instagram, YouTube, LinkedIn, WeChat and so on that allow individuals or organization to exchange idea or information with each other or to disseminate content created by users."[143]

Further, it classifies social network platforms into small i.e. having less than one lakh (i.e., one hundred thousand) users and big social network platforms as those having more than one lakh users.[144]

It provides that any person, company or institution willing to operate social network platform shall enlist the network with the Ministry.[145] Therefore, any social network platform that are not enlisted will be banned from operating in Nepal, except for those platforms which are operational with the sole focus on civic education and social empowerment.[146]

It mandates the operators of social network platforms to establish an office or designate a contact person in Nepal in order to address any grievances[147] and provides responsibilities/ duties[148] of such social media platform operators so they can be held accountable in case of any negligence.

It provides for the prohibition of certain acts committed by social network users which are as follows; (a) creating an anonymous or disguised identity, (b) produce or share content or share others' content or comment on others' content or make calls anonymously or with disguised identity, (c) target any person, community, caste, sex, religion, age, color, class, profession, sect, marital status, family status, physical or mental condition, origin, sexual orientation, language and other groups or category of people protected by law to spread hatred, or share word, audio, visual, picture that harm social harmony and tolerance and to create, publish and broadcast trolls, (d) encourage child labor, human trafficking, polygamy, child marriage, caste untouchability and other activity prohibited by prevailing laws, (e) create offensive words, audio visuals, images, trolls with an intention to bully others and use hateful expressions, insult, or acts that constitute hate speech, (f) perversely modify the photograph of a person by animation montage and other technology through the use of digital media and publish or broadcast such

141 To frame and Enforce the Directives, Section 79, Electronic Transaction Act, 2063 (2008)
142 Section 2 (e), Directives for Managing the Use of Social Networks, 2080 (2023)
143 Section 2 (g), Directives for Managing the Use of Social Networks, 2080 (2023)
144 Section 5, Directives for Managing the Use of Social Networks, 2080 (2023)
145 Section 3, Directives for Managing the Use of Social Networks, 2080 (2023)
146 Section 3 (7), Directives for Managing the Use of Social Networks, 2080 (2023)
147 Section 6, Directives for Managing the Use of Social Networks, 2080 (2023)
148 Section 8, Directives for Managing the Use of Social Networks, 2080 (2023)

photograph, (g) edit, publish and broadcast, without permission, photographs and videos of private matters other than those of public nature, (h) Publish, broadcast or comment in support of obscene word, photograph, audio, video animation, (i) encourage content that harms child and promotes prohibited activities such as child sexual exploitation, sexual abuse, prostitution, (j) publish or broadcast false information, misleading information, misinformation, disinformation, (k) commit act that constitutes cyber bullying, (l) encourage consumption, buying and selling of narcotic drugs, (m) gambling or encouraging gambling, publish or broadcast contents related to terrorism, (o) breach of personal privacy, (p) hacking other's identity and information using social networks, (r) post or share gruesome photograph, video, (s) advertising and transacting goods that are prohibited by prevailing laws, (t) imitate and share activities that are prohibited by the prevailing laws.[149]

It also provides for the responsibilities of social network users[150] and social network operators.[151] The responsibilities of social network users include; (a) they do not commit or cause to be committed such activity or conspire or abet or attempt to commit such activity that causes adverse impact on sovereignty, territorial integrity, national security, national unity, independence, self-respect of Nepal or that causes adverse impact on national interest of Nepal or causes adverse impact on the god relation between federal units or that incites hatred, malice or contempt on the basis of class, caste, religion, region, community, and not to post on social networks such content that undermines harmony between different castes or communities of Nepal, (b) not to publish or broadcast any content or commit any such act that abets caste discrimination and untouchability, shows contempt of labor, incites to commit crime, elicits act that disturbs law and order or publish or broadcast such a content that is prohibited by the prevailing laws to be published or broadcasted or publish or broadcast content that causes adverse impact on the public morality and decent behavior publish or broadcast obscene content, and (c) one shall not knowingly share, like, repost, live broadcast, tag, mention, subscribe and comment or cause to be committed such act on any content published or broadcasted by any other person pursuant this section.

It establishes a Social Networks Management Unit[152] to handle any grievances received by the social network platform operator or its point of contact or the relevant agencies[153] that were not addressed in accordance with this directive or the prevailing laws of Nepal. Thus, the Social Networks Management Unit is the main body responsible for the enforcement of this directive.

The Social Network Directive is a way forward towards regulating social media/network, its users and its operators. It provides a very broad set of guidelines that must be followed by Social Network operators and users. Although it is seen as a way forward towards decreasing immoral and criminal activities done via the use of social network, it also provides the state with ample room for the abuse of power conferred by this directive. The responsibilities of social network users provided in the Social Network Directive gives way for the state to censor any content put up on social network platforms that does not align with the state mentality. Therefore, it can also be seen as a means to control the freedom of opinion and expression,[154] right to

149 Section 4, Directives for Managing the Use of Social Networks, 2080 (2023)

150 Section 9, Directives for Managing the Use of Social Networks, 2080 (2023)

151 Section 8, Directives for Managing the Use of Social Networks, 2080 (2023)

152 Section 13, Directives for Managing the Use of Social Networks, 2080 (2023)

153 'Relevant Agencies' means Department of Information and Broadcasting, Advertisment Board, Press Council and Nepal Telecommunication Authority. Section 2 (d), Directives for Managing the Use of Social Networks, 2080 (2023)

154 Article 17, Constitution of Nepal, 2072 (2015)

communication[155] enshrined under the constitution of Nepal.

7.1 Intellectual Property Laws

The Copyright Act, 2059 (2002) and the Patent, Design and Trademark Act, 2022 (1965), govern and protect Intellectual property in Nepal. Nepal is also a party to the Paris Convention for Protection of Industrial Property,1883, Trade-Related Aspects of Intellectual Property Rights, 1995, and the Berne Convention for Protection of Literary and Artistic Works,1886 which are all treaties and agreements done for the protection of intellectual property in Nepal.

The Copyright Act, 2059 (2002) provides that data or database readable with or without the support of a machine shall be protected under as a copyright under the legislation.[156][157] Further, it also provides that general data shall not be given protection as copyright.[158] It has to be noted that the said legislation does not provide any definition of 'data' or 'database', but it does provide protection for two kinds of work i.e. artistic work and literary work and any computer program comes under the purview of artistic work. The definition of 'general data' is not provided under the Copyright Act therefore, it is not clear whether it captures the concept of meta data and generative AI. Therefore, search engines and generative AI could be considered not covered under the exception of general data' provided in Section 4 of the Copyright Act. The laws of Nepal are silent on the issue of whether generative AI can reproduce copyrighted work as part of the training data for AI.

The Copyright Act provides that the economic and moral rights available to the author under this Act shall be protected throughout the life of the author and in the case of his/her death until fifty years computed from the year of his death.[159]

The exceptions provided under Chapter 4 of the Copyright Act do not address the use of generative AI or whether copyrighted work can be reproduced as part of the training data for AI or as part of the cache for search engines. Consequently, the use of copyrighted work by AI, even for training purposes, can be considered illegal in Nepal since the current laws do not provide for such uses.

The Patent, Design and Trademark Act, 2022 (1965)[160] does not explicitly provide for the protection of data but we have to refer to any patent, design or trademark as the data to be protected which the legislation provides for. Patent[161] is renewable not more than twice for a period of seven years at a time, whereas Trademark[162] is renewable any number of times for a period of seven years at a time, and Design[163] is renewable not more than twice for a period of five years at a time.

The laws governing intellectual property in Nepal are in the nature of decreasing access which seems to be the right approach for such kind of data. It gives protection to the individual's intellectual property and it is not exhaustive in nature as a time limit for protection of such

[155] Article 19, Constitution of Nepal, 2072 (2015)
[156] Section 3, Copyright Act, 2059 (2002)
[157] "The Copyright Act, 2059 (2002).Pdf."
[158] Section 4, Copyright Act, 2059 (2002)
[159] Section 14(1), Copyright Act, 2059 (2002)
[160] "The Patent, Design and Trade Mark Act, 2022 (1965)."
[161] Section 8, Patent, Design and Trademark Act, 2022 (1965)
[162] Section 18D, Patent, Design and Trademark Act, 2022 (1965)
[163] Section 14A, Patent, Design and Trademark Act, 2022 (1965)

intellectual property is provided and conditions for the reproduction[164] or use of such intellectual property are also provided for in the legislation. However, these laws were amended back in 2006 and exhibit a more conventional approach towards the protection of intellectual property which fails to capture the present context of technological advancements and is in need of reform. It has to be noted that these laws are indeed being amended at the moment and a new law governing intellectual property rights in Nepal shall be seen very soon.

While these amendments are forthcoming, it is crucial that they incorporate provisions addressing the legal uncertainty surrounding AI-generated content, metadata, and digital innovations. The absence of clear legal recognition for AI-generated works creates challenges in defining ownership and enforcement, leaving room for disputes. Additionally, the law should explicitly regulate the use of copyrighted works for generative AI models and search engine caches, ensuring a fair balance between innovation and intellectual property rights. As Nepal moves toward modernizing its IP framework, aligning with international standards and technological advancements will be essential to fostering a more secure and forward-looking digital ecosystem.

7.2 Telecommunication and Publication

The Telecommunication Act, 2053 (1997) gives special power to the Government of Nepal where it can control or stop transmission of information in the state of emergency or national security in the country.[165][166]

Although there is an explicit right to communication provision in the Constitution of Nepal, this right can be restricted on some grounds, such as sovereignty, territorial integrity, harmony between communities, public moral, contempt and sedition. The Press and Publications Act, 2048 (1991) provides for restriction[167] and prohibition[168] on publication.[169]

Restriction on any matters which undermines the sovereignty and integrity of Nepal or, disrupts security, peace and order or, creates enmity among the people of various castes, tribes, religions, classes, region, communities and spreading communal disharmony or, hurting decency, morals and social honor of the people generally shall not be published in any books or magazines.[170] It also provides for the restriction on imports of foreign publications on the same lines.[171]

The government can prohibit the publication of any news, information or other reading material relating to any specific subject, event or area via notification in the Nepal gazette.[172]

These legislations provide for the control of mass media and publication in certain situations which was used by the King of Nepal during the Maoist insurgency for security reasons.[173] These

---

164 Chapter 4, Copyright Act, 2059 (2002)
165 Section 19, Telecommunication Act 2053 (1993)
166 Telecommunications Act.
167 Section 14, Press and Publications Act, 2048 (1991)
168 Section 15, Press and Publications Act, 2048 (1991)
169 Press and Publication Act, 2048 (1991) – Nepal Law Commission.
170 Section 14, Press and Publications Act, 2048 (1991)
171 Section 16, Press and Publications Act, 2048 (1991)
172 Section 15, Press and Publications Act, 2048 (1991)
173 Peng Hwa Ang & Ors., 'Shuting down of mobile phone and the downfall of Nepalese society, economy and politics', (2012) PacificAffairs, vol.85 no.3. available at" https://dr.ntu.edu.sg/bitstream/10356/105954/2/Shutting%20down%20the%20mobile%20phone%20and%20the%20downfall%20of%20Nepalese%20society%2C%20economy%20and%20politics.pdf"

can very easily be misused by the now government to push their own ideologies towards its citizens and it can decrease access to information for the citizens of Nepal by suppressing free speecha and critical journalism. While national security and public order are legitimate concerns, the absence of clear legal criteria and judicial oversight leaves room for arbitrary restrictions, potentially undermining the fundamental right to freedom of expression and the public's right to information.

To strike a balance between national security concerns and freedom of expression, it is essential to introduce judicial oversight in cases where publication bans are imposed. Establishing clear legal standards for such restrictions would ensure that limitations on publications are applied only when necessary and proportionate, preventing potential government overreach. Strengthening procedural safeguards within the legal framework would promote transparency, accountability, and media independence, aligning the telecommunication and publication laws of Nepal with international human rights standards and reinforcing democratic principles

7.3 Banks and Financial Institutions

The Unified Directive issued by the Nepal Rastra Bank to "A", "B" and "C" Category Certified Institutions,2079 (2023), Unified Directive no. 14/2079, Rule 6 provides for mobile banking services where in Rule 6(13) provides that the networking and database should be totally secure, wherein if hindrance occur during deposit or payment transactions which might result in damage of the database then the bank and financial institutions are to be liable for such damages. Rule 7 (10) also provides for the (Live) data transfer to the nearest branch or central office to exchange information immediately in the central information system and appropriate backup, shall be arranged at least 2 days a week at a designated location.

Under the Unified Directive no. 19/2079, Rule 2 provides that the customer must be identified and verified before any transaction through geographical location and account through digital platforms. It also provides for the use of goAML (Anti-Money Laundering) software developed by the United Nations Office on Drugs and Crime (UNODC) for prevention of money laundering and terrorist financing.[174] Unified Directive no. 20/2079, Rule 11 provides for privacy and data protection or confidentiality of the customers business information. It also provides a research paper which also highlights some importance of data accuracy, confidentiality and protection of data through risk management and regular reviews.[175][176]

Payment System Unified Directive, 2079 (2023) provides for the operation and security of electronic payment systems which include hardware and network security, computer virus and malware protection, authentication of System Access by customers, customer data privacy, confidentiality, backup and archival.[177][178] It further mentions transaction and equipment security through protection of payment system firewall, antivirus/malware detection software, intrusion detection/prevention system, monitoring, log analysis tools/techniques, cryptographic system, Disaster Recovery Plan(DRP), etc.[179] It further provides for the security measure that a Payment

[174] The Unified Directive no. 14/2079, Rule 19 (11), Unified Directives issued by the Nepal Rastra Bank to "A", "B" and "C" Category Certified Institutions, 2079 (2023),

[175] Schedule 1, Unified Directives issued by the Nepal Rastra Bank to "A", "B" and "C" Category Certified Institutions, 2079 (2023)

[176] "PDF," n.d.

[177] Rule 3 (1) (ii), Unified Directive no.3/079, Payment System Unified Directive,2079 (2023)

[178] "PDF," n.d.

[179] Rule 3 (2) and (3),Unified Directive no.3/079, Payment System Unified Directive,2079 (2023)

System Provider (PSP) can adopt for better functioning and for data security with regular monitoring transactions, updating systems as needed, and testing database and transaction security systems.

The Circular issued by Nepal Rastra Bank regarding Foreign Exchange Transactions, 2079 (2023) provides for monitoring of foreign currency payments and the use of the database structure provided to ensure data entry and monitoring of the same is as per the rules of the bank and financial institutions. It does not directly violate the Privacy Act and the Individual Privacy Act because an exception is provided under such legislations that if it is authorized by the authority, institution, or consent of a person related to it under law then the government can collect such data.

The Unified Directives provides a framework for banks and financial institutions and payment system operators to better function according to international standards and also provides for better data governance of such institutions.It provides for the security of confidential information of their customers as well as data related to business transaction etc. It provides the use of data protection software for the same. The data protection regime of Banks and financial institutions are comparatively safer as higher degree of compliance and monitoring is done. But it is unclear as to the uniformity in data governance structure amongst the banks and financial institutions in Nepal.

7.4 Right to Information

Some of the provisions in the RTI Act also decrease access to data. It contains provisions for the classification of information[180] and keeping information confidential for a maximum period of 30 years.[181]

With power given under the RTI Act the government of Nepal tried to classify 87 types of information as confidential information.[182][183] Classification of such information is a necessary step towards protection of sensitive information and for national security as well, but this sort of a blanket classification would prove to be harmful to the people's right to information.

The classification was done in such a way to hide more government data or information from the general public which would decrease transparency of the government, but due to a revolt from the Payment Service Providers, Payment Service Opertators, private companies, citizens and other stakeholders this classification is put on hold for now.

Therefore, this classification of information is seen to be a regressive as it was done without the consultation from all stakeholders and there was no factual reasoning or justification for the categorization of such information. There has to be due accountability on the part of the government with respect to the classifications made.

---

180 Section 27, Right to Information Act, 2064 (2007)

181 Section 27(5), Right to Information Act, 2064 (2007)

182 Tika R Pradhan, 'Government backtracks on information classification, The Kathmandu Post, (31 January 2023), available at "https://kathmandupost.com/national/2023/01/31/government-backtracks-on-information-classification" (last accessed on 6th October, 2023)

183 Pradhan, *Government Backtracks on Information Classification.*

8 Data Localization

The laws of Nepal are silent on data residency or data localization. As of now, there are no laws that govern any data residency or data localization that prevent the export of personal, healthcare, or other data out of the jurisdiction. Further, there are no specific laws concerning special requirements for data transfer and/or data storage out of jurisdiction, including sharing it with affiliated companies and vendors that may be located in other countries. However, the Individual Privacy Regulation, 2077 (2020) does illustrate that no one shall collect, store, process, analyze, process or distribute any personal information unless authorized by the authority, institution, or consent of a person related to it under the law,[184] but in practice it is not seen to be followed

The government of Nepal is seen to be more inclined towards data localization for the collected data of the citizens of Nepal. There was a cabinet decision highlighting the same, wherein it states that all the data and information technology of the government of Nepal shall be stored and managed in the Government Integrated Data Center (**GIDC**) along with the Disaster Recovery Center located in Kathmandu and Hetauda respectively.[185]Those centers shall be operated in full capacity with 24-hour networking and cyber security monitoring. It provides to develop and upgrade technical and human capacity of GIDC. Further, it provides for the regular technical and security audits of information technology systems operating in government agencies, to remove software that does not meet the security standards operating in the agencies, only to use genuine software, prohibits the sharing of software source code which are used by government agencies and any software without source code shall not be used.[186]

The Cabinet decision also does not explicitly talk about data localization, but while interviewing various government personnel it has come to light that the intent of the government of Nepal is to store data collected in Nepal shall be stored within the territory of Nepal.

Nepal lacks explicit laws governing data localization and cross-border data transfers for both personal and corporate data. To address this gap, comprehensive data localization laws should be introduced to ensure that both government and private sector data are stored and processed within Nepal unless explicit cross-border transfer permissions are obtained. Regulations must establish clear requirements for the transfer of personal, healthcare, and financial data outside Nepal's jurisdiction while ensuring that data sovereignty is maintained.

The absence of such data localization laws creates economic and operational challenges for businesses operating in Nepal, particularly those that rely on international data flows. While localization requirements can strengthen national security and data protection, they may also impose financial burdens on companies that must develop local storage infrastructure. Striking a balance between regulatory compliance and business feasibility is crucial to prevent unnecessary barriers to innovation and foreign investment. Moreover, given Nepal's increasing engagement in global markets, restrictions on data flow could affect trade relations and international business operations, making it necessary to implement measured policies that align with both economic interests and data protection standards.

Data localization policies also have significant implications for privacy rights, especially in the context of international data-sharing agreements. Without a structured framework, there is a risk that Nepali citizens' data may be processed under foreign jurisdictions without adequate

[184] Rule 10, Individual Privacy Regulation, 2077 (2020)
[185] Table S.No.9, Decision of the Council of Ministers Meeting held on 2079/11/15 (27th February, 2023)
[186] Letter dated 2079/11/17 (1st March, 2023), Ministry of Information and Communication

safeguards. Therefore, it is essential to establish legal clarity on cross-border data transfers, ensuring that privacy protections remain intact when data is shared across borders.

To implement an effective data localization framework, private-sector stakeholders, including telecommunications companies, banks, and internet service providers, must be actively involved in policy development. Clearly defining the obligations of private entities will help streamline compliance mechanisms while providing guidelines on secure data storage and processing practices within Nepal. A well-defined legal structure will not only enhance data protection and national security but also create a regulatory environment that supports digital transformation and aligns with international best practices such as the GDPR.

9 Deep Dives

Right to Information vis-a-vis Right to Privacy**

Nepal is one of the few countries which has constitutionally guaranteed the right to information and the right to privacy as fundamental rights. Nepal serves as an example for implementing legislation to uphold the enforcement of such fundamental right, namely the Right to Information Act and Privacy Act because it is one of the few contries to have both those rights guaranteed under the constitution.

The RTI Act has defined 'information' as "any written document, material, or information related to the functions, proceedings thereof or decision of public importance made by a Public Body".[187] Similarly, the preamble of the Privacy Act provides for the right to privacy relating to data and promotes the safe use of any personal information held by any public body.

On one hand, the right to information necessitates the disclosure of information, ensuring transparency and accountability in governance. This means that public bodies are obligated to provide access to information upon request, promoting openness and accountability in public affairs. The preamble of the RTI Act emphasizes the importance of transparency and accountability within the democratic system. The objective is to ensure that the functions of the state are open and accessible to citizens by providing easy access to information held by public bodies and also aims to empower citizens and protect their rights to be well-informed. Additionally, it highlights the need to safeguard sensitive information that could adversely affect the nation or its citizens. In summary, the legislation is intended to promote transparency, accountability, combat corruption and citizen empowerment while balancing the protection of national interests and sensitive information.

On the other hand, the right to privacy seeks to protect individuals' personal information, bodily privacy, mental condition, biological identity from access or disclosure, safeguarding their privacy and autonomy. This involves limiting the collection, use, and dissemination of personal data by public bodies to ensure individuals' privacy rights are respected. However, the data held with the government data serves as a vital resource across various sectors, including media, finance, and education. While stakeholders recognize the importance of data for decision-making, there is limited awareness among executives regarding the role of data analytics teams and specialists in utilizing existing data effectively.[188]

The tension between the right to information, which mandates the disclosure of information, and the right to privacy, which seeks to safeguard personal information and privacy, underscores the delicate balance required in legislation and policy-making.

Executives across various governmental sectors are still unaware of the potential benefits internal data can offer in enhancing their operations, making better policies and fostering growth. Although stakeholders emphasize the importance of disaggregated and timely data, underscoring their critical role in maximizing the utility of government data across different domains,[189] only the finance and education sectors have established mechanisms to collect data

---

187 Section 2 (b), Right to Information Act, 2064 (2006)

188 The World Bank, "Use of data in the private sector of Nepal the current state and opportunities in finance, education and the media" (July 2020) pg.19-22, available at "https://documents1.worldbank.org/curated/en/805261601023506163/pdf/Use-of-Data-in-the-Private-Sector-of-Nepal-The-Current-State-and-Opportunities-in-Finance-Education-and-the-Media.pdf"

189 The World Bank, "Use of data in the private sector of Nepal the current state and opportunities in finance, education and the media" (July 2020) pg.19, available at "https://documents1.worldbank.org/curated/en/80526

as part of their routine operations, awareness of gathering internal data remains limited to these two governmental institutions and is not practiced by any other governmental bodies. This is because in all sectors, there is a notable deficiency in both infrastructure and human resources dedicated to data analysis and management. Leaders within organizations acknowledge this lack of capacity to effectively analyze and manage data. Moreover, leaders across the finance, education, and media sectors identify three primary areas for increasing investment in data: management (including gathering, storage, and retrieval), analysis, and synthesis (particularly visualization) of data.[190]

The government is the main repository and producer of individual data and leveraging these data can address public policy challenges. However, access to this data is restricted due to the confusion regarding data privacy rules and laws, the limited awareness among executives regarding the role of data analytics teams and specialists in utilizing existing data effectively, low investment in data and analytics skills and infrastructure. A significant portion of professionals in the finance and education sectors lack awareness or have limited understanding of the Privacy Act 2018.[191] Conversely, professionals in the media sector are generally familiar with the act and perceive it as the government's responsibility to classify information to encourage a culture of data sharing. Therefore, the overlapping mandates of RTI Act and Privacy Act has resulted in notable gap in the availability and capacity to utilize data effectively.

There is also a provision in the RTI Act to prevent unauthorized disclosure of personal information.[192]The only conditions where personal information can be disclosed are instances where disclosure is necessary to prevent a serious threat to life, public health, or security; when mandated by existing laws; or when required to address corruption offenses. There is no public interest exception under the RTI Act of Nepal. The Right to Information Act of India used to have a provision wherein a public authority may disclose information if the public interest in such disclosure outweighs the potential harm to protected interests.[193] Similarly, Sri Lanka also adopts a similar public interest override clause. However, it's notable that the laws of Nepal do not include such a clause. This absence can be seen as advantageous for the protection of individual privacy in Nepal, but if data are not shared or cannot be accessed the engagement with local communities and decision making is negatively impacted. Without a public interest override clause, while the legal framework of Nepal emphasizes safeguarding personal information, the overarching aim of benefit of data for the goal of national development is hindered. Therefore, a public interest override clause should be adopted to ensure that digital innovation is not hindered by any privacy laws and security frameworks.

The provisions within the RTI Act that allows the classification of data into classified/ confidential information impedes the objective of access to data. This classification is based on factors such as national security, criminal investigations, economic interests, social harmony, and individual privacy and security.[194] The committee comprising of Chief Secretary of Nepal, Secretary of Ministry of Communication and Information Technology, and an expert assigned by the National Information commission is mandated to classify information as confidential at policy level.[195] The RTI Act does not prescribe any criteria for this committee to abide by or

1601023506163/pdf/Use-of-Data-in-the-Private-Sector-of-Nepal-The-Current-State-and-Opportunities-in-Finance-Education-and-the-Media.pdf"

190 ibid.

191 ibid

192 Section 28, Right to Information Act, 2064 (2007)

193 Section 8 (2), Right to Information Act, 2005 (India)

194 Section 3, Right to Information Act, 2064 (2007)

195 Section 27, Right to Information Act, 2064 (2007)

follow for classifying information resulting in classification being subjective and opaque. Therefore, this subjectivity in classification of information undermines the transparency and accessibility goals of the RTI Act, as it may lead to inconsistent interpretations and challenges in determining the appropriateness of the classification decisions. The government had proposed to classify the information and tried to classify 87 types of information as confidential information.[196][197] Classification of such information is a necessary step towards protection of sensitive information and for national security as well, but this sort of a blanket classification would prove to be harmful to the people's right to information. The RTI Act also provides that, if a person disagrees with the classification of information made by a committee under the RTI Act, they can submit a review petition to the National Information Commission requesting the information to be made public.[198] Upon reviewing the petition, if the commission determines that the information does not need to be kept confidential, it will issue an order for its disclosure. Information classified under the RTI Act can be kept confidential for a maximum of thirty years, depending on its nature. However, every ten years, the committee must review whether the classified information still needs to be kept confidential.

The interviewee from the National Information Commission mentioned that formal classification of information at the national level remains incomplete in Nepal. While some organizations have conducted their own classification processes, these classifications lack official recognition. As a result, the accuracy of such classifications cannot be conclusively determined. For instance, Loksewa Ayog (Public Service Commission) categorized its information according to what could be disclosed under the provisions of the RTI Act and what must remain confidential. However, the RTI office contested Loksewa Ayog's classification, suggesting that it was either inaccurate or unacceptable.[199]

Therefore, one of the major reforms required in the RTI Act is the establishment of of set criteria for the classification of information as confidential information anddefining the conditions under which disclosure is permitted. While government-held personal data, such as medical records, tax filings, and biometric information, must be strictly protected to safeguard individual privacy, information related to public interest matters, government decisions, and public spending should remain accessible to promote transparency, accountability and prevent corruption.

A well-defined exemption system is necessary to differentiate between information that must remain confidential due to privacy concerns and information that should be disclosed in the public interest. Legal safeguards, such as judicial oversight and independent regulatory bodies, should be implemented to review cases where privacy and transparency come into conflict. Additionally, data protection laws must ensure that government agencies and private entities handling sensitive information adopt strict security measures to prevent data leaks and unauthorized disclosures.Technological solutions such as data anonymization, encryption, and controlled access to information can further aid in achieving this balance. By implementing robust legal and policy mechanisms, Nepal can ensure that citizens' right to privacy is protected without undermining the fundamental principles of transparency and accountability. As right to information and the right to privacy are both fundamental rights provided under the constitution of Nepal. These two fundamental rights are complementary to each other, yet

---

196 Tika R Pradhan, 'Government backtracks on information classification, The Kathmandu Post, (31 January 2023), available at "https://kathmandupost.com/national/2023/01/31/government-backtracks-on-information-classification" (last accessed on 6th October, 2023)

197 Pradhan, *Government Backtracks on Information Classification.*

198 Section 27(3), Right to Information Act, 2064 (2007)

199 Interview with the National Information Commission, Annex-2.

sometimes conflicting principles. While right to information facilitates access to information, the right to ensures the protection of personal information. There is a need to balance the two principles in order to ensure transparency and accountability in governance while also respecting individual privacy rights. This requires developing clear guidelines and mechanisms to address situations where the two rights intersect, ensuring that access to information serves the public interest without unduly compromising individuals' privacy. The challenge lies in finding a balance between these two fundamental rights. While transparency and access to information are essential for democratic governance and accountability, protecting individuals' privacy rights is equally crucial for preserving autonomy and dignity. Legislation and policy-making must navigate this tension by establishing clear guidelines and mechanisms for accessing information while also implementing robust data protection measures to safeguard individuals' privacy. This delicate balance ensures that both rights are upheld in a manner that respects the principles of democracy, transparency, and individual autonomy.

10 Key Findings

The information processed and collected pursuant to the Statistics Act is published in the website of the National Statistical Office. Upon initial inspection of the website it seems to have missing data and is faces retrieval challenges hard to retrieve all data. Following an interview with the interviewee from the Central Bureau of Statistics, National Statistics Office, it was determined that not all required information is readily accessible to them and that the published data on the website is the summarized version of a larger set of micro-data. This type of limited accessibility of only summarized data has significant implications for decision-making and public trust. It hampers the ability of policymakers, researchers, and businesses to make informed, evidence-based decisions and undermines public confidence in the government's transparency. To address this, the government should ensure full data accessibility, including detailed micro-data, on public platforms. Regular audits should also be conducted to ensure that missing data is promptly addressed, thereby fostering a culture of transparency and accountability and supporting more informed policy development.

Data processed under the Statistics Act is published on the National Statistical Office website, but accessibility issues and missing data hinder comprehensive retrieval. Interviews reveal that the published data is a summary, with the full dataset not readily available.

The Statistics Acts sets out the common standard to be followed in case of demographic indicators.

The Supreme Court of Nepal has initiated the publication of case laws on its website, while daily court hearings are also listed on the platform for public access.

The annual fiscal budget is presented by the Minister of Finance in Parliament, with detailed information published by the Ministry of Finance, including the Expenditure Details (Red Book). Additionally, provincial and local governments also publish their respective budgets, accessible to the public through the Ministry of Federal Affairs and General Administration's website.

The Government Website Management and Operational Guidelines, 2078 (2021) mandate a uniform format for all government websites.

The GIDC, serves as a centralized repository for managing and storing government data. It facilitates the sharing of information among different government bodies or ministries and hosts all government websites.

Credit Information Bureau of Nepal releases a list of borrowers and affiliated individuals, firms, or companies who have been blacklisted in accordance with the laws of Nepal.

The Office of Company Registrar regularly updates and publishes real-time statistics on the total number of registered companies. The Office of the Company Registrar and Tax office are the only two government bodies that have an interoperability framework amongst both offices, their systems work in harmony with each other and no overlap is there in the process. This is not done through any interoperability framework but it is done with the mutual understanding between the two governmental bodies so that the duplication of information is avoided and making it easier for the citizens and government employees both by making it a shorter process.

The Department of Industry hosts a website where it discloses a catalog of registered industries and those endorsed for foreign investment, as well as information regarding the registration of industrial property, including patents, designs, and trademarks.

The Department of Land Management and Archives operates the Land-service Center, allowing access to all land-related data within Nepal's territory for entities holding a license.

The National Cybersecurity Policy, 2080 (2023) and NeGIF both, promote the adoption of open standards, although they do not enforce this requirement, which negatively impacts the effectiveness of this policy.

The Archives Act outlines 'prohibited records' which can only be accessed by authorized individuals.

The Social Network Directive outlines a set of responsibilities that social network platform operators are required to adhere to.

The RTI Act mandates public bodies to maintain updated information while also ensuring the protection of personal information from unauthorized disclosure or broadcasting.

The Nepal Rastra Bank, has implemented the Nepal QR Guidelines to standardize QR code usage.

The Government Integrated Data Centre (GIDC) introduced the Nagarik App to establish interconnectivity among electronic information systems in public bodies. The aim of the app is to facilitate the swift, cost-effective, and efficient flow of services and information to citizens through a unified electronic system. GIDC is responsible for the management and operation of the Nagarik App.

The Constitution of Nepal provides for the right to privacy as a fundamental right which includes protection of personal information and data relating to a person.

The Privacy Act mandates the protection of personal data and sensitive information, requiring consent for the collection of such data.

Nepal's data protection laws exhibit significant disparities when compared to the GDPR, including the absence of a defined framework for consent, provisions for the right to be forgotten, regulations regarding the right to restrict processing and be informed about processing of personal information, as well as stipulations for the right to erasure and rectification. Additionally, there is a lack of clarity on the responsibilities of Data Controllers, requirements for appointing Data Protection Officers, legislation on data localization, and laws governing cross-border data exchange and trading.

The ETA defines 'Data', encompassing electronic records, and provides safeguards against cybercrimes. However, in its practical application, the ETA inadvertently exposes personal data to breaches. As during investigations of cybercrimes, law enforcement authorities confiscate electronic devices linked to the offense, leading to the scrutiny of all personal information stored on these devices, even if it is unrelated to the specific crime under investigation.

The NTA has also made directives with regard to such criminal investigation provides that ISP should make available the information requested by Nepal Police or Law enforcement Agency for 365 days 24 hours should inform the NTA within 3 days of the same. NTA has also issued directives for voice service providers wherein it provides for telecommunication service providers to provide 18 months of Operational Data (including SIM/Call-Wise Location, Cell ID, IMEI, etc) up to 6 months Active (Live) and up to one year Passive (stored). But there seems to be a gap in its implementation as service providers do not have the capacity to store such data and retrieve it easily, only when the court orders such service providers, only after that such record is stored.

The Social Network Directive is a way forward towards regulating social media/network, its users and its operators. It provides a very broad set of guidelines that must be followed by Social Network operators and users. Although it is seen as a way forward towards decreasing immoral and criminal activities done via the use of social network, it also provides the state with ample room for the abuse of power conferred by this directive. Therefore, an independent review mechanism must be put in place to oversee the implementation of the Social Network Directive to mitigate the risk of infringement on freedom of expression.

The definition of 'general data' is not provided under the Copyright Act therefore, it is not clear whether it captures the concept of meta data and generative AI. Therefore, search engines and generative AI could be considered not covered under the exception of general data' provided in Section 4 of the Copyright Act.

The laws governing intellectual property in Nepal are in the nature of decreasing access which seems to be the right approach for such kind of data. It gives protection to the individual's intellectual property and it is not exhaustive in nature as a time limit for protection of such intellectual property is provided and conditions for the reproduction[200] or use of such intellectual property are also provided for in the legislation.

The telecommunication and publication legislations provide for the control of mass media and publication in certain situations, which can very easily be misused by the government to push their own ideologies towards its citizens. Therefore, it can decrease access to information for the citizens of Nepal.

Some of the provisions in the RTI Act also decrease access to data. It contains provisions for the classification of information[201] and keeping information confidential for a maximum period of 30 years.

The laws of Nepal are silent on data residency or data localization. As of now, there are no laws that govern any data residency or data localization that prevent the export of personal, healthcare, or other data out of the jurisdiction. Therefore, a comprehensive legislation for data localization, that mandates the storage of sensitive data within the jurisdiction of Nepal must be introduced for greater data sovereignty and security.

Nepal is one of the few countries which has constitutionally guaranteed the right to information and right to privacy as a fundamental right. Nepal serves as an example for implementing legislation to uphold the enforcement of such fundamental right, namely the Right to Information Act and Privacy Act.

The tension between the right to information, which mandates the disclosure of information, and the right to privacy, which seeks to safeguard personal information and privacy, underscores the delicate balance required in legislation and policy-making. The provisions in the RTI Act regarding the classification of information, coupled with the absence of a public override clause, hinder the right to access information.

It is seen that Nepal is still in the early stages of establishing a robust data governance system. While explicit tradeoffs have not yet been recognized, Nepal being a developing nation aiming for rapid economic growth and digitization, must balance ensuring data protection and privacy with promoting digital innovation and economic growth. To improve its data governance structure, Nepal seems to learn from the experiences of developed countries. Currently,

---

200 Chapter 4, Copyright Act, 2059 (2002)

201 Section 27, Right to Information Act, 2064 (2007)

challenges such as a lack of experts, technological advancement, and gaps in the laws hinder the complete implementation of data governance initiatives. These challenges also limit the participation of government officials in international rule-making or norm-setting processes related to data governance.

To overcome these obstacles, Nepal should encourage citizen engagement in data governance by training young and mid-career researchers and professionals, providing education and awareness programs, and promoting capacity-building initiatives. Collaboration with civil society groups, offering incentives, and fostering online platforms for debate and collaboration are also crucial steps. By addressing these challenges and fostering an inclusive approach, Nepal can build a more effective and resilient data governance framework that supports its goals of economic growth and digitization.

11 Preliminary Findings

There are no laws with regard to Open standards in Nepal. There is vagueness and ambiguity with respect to the control or the right to govern data generated from Nepal. There are still concerns with regard to storage of data and who has access to such data especially when a foreign entity is involved.

The existing data governance policies are fragmented across multiple laws, lacking a unified source of legislation that comprehensively governs data as a whole. Present regulations inadequately address data protection and governance, only partially aligning with international best practices or standards.

The Policies have been developing to meet the engagement of public discourse and discussion on data governance with a multi stakeholder approach involving government agencies, civil society, academia and private sector, and yet the legislation seems to have overlooked to recognize recommendations from the stakeholders. The existing laws on data governance do not properly address the problems such as cross border data transmission, national data storage and protection, national cyber security issue, lack of open standards, etc.

There is no regulation for the mandate of a common procurement standard in construction and development projects. But in case of procurement of medicines common procurement standards are used making it easier to identify medicines and compare it with other jurisdictions.

The flow of data needs to be streamlined within the government and interoperability framework must be followed which is lacking in the current data governance structure of Nepal.

There are no provisions or facility for internet surveillance in Nepal. The only way government can stop the access to any websites is by providing a list of websites to the Internet service providers then they can restrict access of such websites for their customers. But then again, there are no resources available for the surveillance on the customer browsing and track the web history of each citizen. For eg; the government has banned porn websites in Nepal, but since a new website comes out every now and then it is hard for the government to put a ban on them all as the list has to be updated and provided to the internet service providers continuously. Therefore, a total ban cannot be placed for such illicit websites as envisioned by the government of Nepal.

There are more than 5 types of identity cards provided by the government of Nepal to identify its citizens.[202][203] The identity comprises of Permanent Account Number (PAN), Driving License, Citizenship, National Identity card, Passport, Voter Identity card, etc. It has to be noted that these different types of identity card prescribed by the government are not interoperable with each other and creates duplication of data. All the information provided while making a driving license including the bio metrics scan of hand and eyes has to be given again while making the National Identity card. This type of multiple data stored in different government departments with regard to identity of the same person is more vulnerable to breach of data and privacy. An integrated system to manage such identification data of its citizens has to be made so that the data of citizens can be securely stored and government agencies can also function more efficiently putting lesser burden on its citizen to provide the same information again and again

[202] Samajha Bk, 'Too many identity cards are burdening Nepal with big money and citizens with redtape: time to rethink?', OnlineKhabar, (16 September 2022), available at "https://english.onlinekhabar.com/many-identity-cards-nepal-problem.html" (last accessed on 6th October, 2023)

[203] *Too Many Identity Cards Are Burdening Nepal with Big Money and Citizens with Red Tape. Time to Rethink?*

to the same government. Therefore, the lack of interoperability between various government bodies or offices is the main reason for such problem of duplication of work.

In the case of Adv. Bhaktiram Ghimire v. Government of Nepal Prime Minister's Office, Ministry of Physical Infrastructure and Transport and ors.[204][205] a writ petition was filed in the Supreme Court for the breach of the right to privacy[206] enshrined under the constitution of Nepal. The electronic driving license or smart license issued by the Ministry of Physical Infrastructure and Transport in Nepal is made and printed by Madras security printers Ltd which is based in India. The writ petition was filed claiming that the personal details of the citizens of Nepal are sent to an Indian company where it can very easily be breached, which would result in the breach of privacy of Nepalese citizens. But the writ petition was quashed by the SC claiming that Nepal does not have the technology or resources for the printing of such smart driving license, hence it had to be outsourced to a foreign company where such company was chosen through a competitive bidding process and since the company has not used such data for its personal benefit or with malicious intentions it cannot be said to be a breach of privacy which is a fundamental right enshrined under the constitution. This case also showcases that Nepal lacks resources for technological growth in and a reason as to why the country has to be dependent on foreign service provider to risking data of individuals.

There are no data centers in Nepal for commercial storage of data. All the private sector companies store and process data through foreign entities. This is so as the cyber security in Nepal is very weak and companies find it safer to use foreign service providers to store and process their data. Though the GIDC created a system to store government data, it is not considered safe as it recently faced cyberattacks which affected the data of as many as 60 different government bodies including Airport authority Kathmandu, Public Service Commission, Department of Passport, Department of Immigration, etc. Some of the data of 10-15 different government agencies could not even be recovered like that of the Public Service Commission of Nepal where data of 85000 candidates who had filled in their details and filed for applications for examinations are missing.[207][208]

Nepal Telecommunication Authority is a regulator for internet and telecommunication service providers in Nepal. It provides license for Network Service Providers[209], GSM Cellular data[210], VSAT, Basic telecommunication Services, internet with email[211], GMPCS, International truck telephone, rural VSAT services, basic telephone service and Rural ISP.

The Interviewee representing NTA informs us that, while the Directives published by the NTA outlines the storage of data by service providers, in reality, it's observed that they lack the necessary system or infrastructure to do so. Even if they possess such capabilities, data storage is not implemented in practice. Data can only be stored or recorded from the date of a court order for an investigation. This poses a challenge during investigations as even with a court order, obtaining or accessing such data becomes difficult. Despite regulatory guidelines set by the

---

204 Adv. Bhaktiram Ghimire v Government of Nepal Prime Ministers Office, Ministry of Physical Infrastructure and Transport and ors., NKP 2079 (Decision no. 073-W0-1097)

205 "Smart License_Privacy.Pdf."

206 Article 28, Constitution of Nepal, 2015

207 Rabindra Ghimire, 'Digital loss in Nepal is troubling Nepal in front of the helpless government', OnlineKhabar (8 May 2023), available at" https://english.onlinekhabar.com/digital-data-loss-nepal-helpless.html" (last accessed on 6th October, 2023)

208 *Digital Data Loss Is Troubling Nepal in Front of the Helpless Government - OnlineKhabar English News.*

209 There are total of 27 such service provider in Nepal.

210 There are only two GSM celluar data provider which are Ncell and Nepal Doorsanchar Company limited.

211 There are total of 122 such providers with largest players being worldlink, subisu, vianet, etc.

NTA, compliance with these laws is not feasible or is not practiced in reality by licensed service providers. Even when questioning an interviewee from one of the largest telecommunication service providers, namely Nepal Doorsanchar Company Limited (NTC), they indicated that in practice, they do not retain personal data or call records of individuals. The data stored is solely for billing purposes for their clients. Consequently, obtaining call records of any accused, even with a court order, is exceedingly difficult and often not feasible due to the lack of retrieval mechanisms.

Through an interview with the director of the Central Bureau of Statistics Mr. Manohar Ghimire, it has come to our knowledge that there exists a micro-data catalog for storing and maintaining all data. Initially, all data are stored in their raw form as micro-data. These micro-data are available for purchase, with anyone able to buy them. However, online purchases or international transactions for such data are not feasible due to the absence of an international payment gateway in Nepal. Therefore, international entities interested in purchasing such micro-data must submit a formal letter and conduct a cash transaction. However, there is no documented or formal procedure for this process, and buyers must approach the thematic authority directly. Even if a governmental organization requests such data, there is no established protocol for its provision. The general practice with regard to sale/purchase of such data is done by submitting a formal letter to the concerned office and make the payment for the prescribed fees.

Nepal lacks dedicated data banks or processing centers; instead, data are stored on flash drives, CDs, or physical books. While an e-library exists for data storage, it only contains selected portions of the raw data. Despite the absence of a data recovery process, data loss incidents have never occurred incase of the data collected and stored by the Central Bureau of Statistics. If such data is lost there is no recovery process for the same, but Mr. Ghimire says that luckily such data has never been lost till now.

Mr. Ghimire informs us that, in Nepal, all micro-data[212] or collected data are in the possession of the 150 employees of the National Statistics Office (the "**NSO**"), with only 3-4 individuals having access to the raw data. Consequently, these few individuals serve as the primary security system or guardians of the collected data in Nepal. Remarkably, there have been no reported incidents of data breaches or individuals selling data, possibly due to the limited market demand for such data and the employees' lack of understanding regarding the data market. Concerning privacy protection, the Statistic Act sanctions any breaches of data or misuse of power/trust by NSO employees. There is no established practice of reuse of data, once data serves its intended purpose, it is either discarded, never used again, or becomes inaccessible. For example, data collected by the Health or Education ministry is processed, and only a summarized or general overview is published on their websites mostly in a single table format. Subsequently, this data is not reused for any other purpose and remains inaccessible to external entities.

Although it is customary within the NSO to retain data for at least 20 years, this practice is not codified anywhere in the laws of Nepal, it is rather an informal convention. Further Mr. Ghimire informed us that in case of retrieving data older than 15 years for study purposes is challenging, as it may not be readily available.

The main hurdle for Nepal in its aim to build a rigid data governance structure is the lack of resources and trained personnel in the information and technology field having expertise on such aspect.

[212] By 'micro-data' the interviewee refers to all raw data collected or the initial set of information collected, such as national surveys.

There is no open standard mandate while publishing data for construction work in Nepal. An initiative was taken by the government by making the bidding process online and more transparent. But even though such process was made to create a standard for publishing such data but it has taken a step backwards, due to the ongoing system or norms of corruption in Nepal. It was seen that the contractors bidding for such construction contracts usually collude and monopolize such infrastructure projects. It was seen that the contractors even collude with the government officials and such government officials make the bidding criteria in such a way that only those contractors are eligible for that contract.[213][214] It was seen that only few contractors used to get the bidding contract and this trend lasted for a long time and still continues but it was only exposed once bidding was done through online portal and such data could be compared.

[213] Rudra Pangeni, 'Cartel of contractors in cahoots with government officials swindle billions of rupees, govt report reveal', Centre for Investigative Journalism (15 January 2018), available at "https://cijnepal.org.np/cartel-contractors-cahoots-govt-officials-swindle-billions-rupees-govt-report-reveals/"(last accessed on 7th October, 2023)

[214] Pangeni, "Cartel of Contractors in Cahoots with Government Officials Swindle Billions of Rupees, Govt Report Reveal."

12 Conclusion

12.1 What is common, and what is nationally specific, in the emerging data governance architectures in South and Southeast Asia? What are the explanations?

Nepal does not have a unified open data portal as stated. but there are guidelines and legislations promoting the use of open standard and open source software such as the Digital Nepal Framework (2019), National Cybersecurity Policy, 2080 (2023) and Nepal E-Government Interoperability framework.

The government seems to encourage both proprietary and open-source solutions, but through our interviews we identified two prevailing perspectives from the government officials where the government discourages adopting open-source software due to security concerns, while others believe open source signifies globally recognized software.

The hesitation towards open-source solutions in Nepal stems from perceived security risks, reflecting a broader trend where cybersecurity is a major priority.

12.2 What are the implications of the emergent nature of the governance architecture? Because there is no overall design that envisions how the parts fit together, it is likely that there will be friction points and even contradictions. How are these being worked out?

The data governance policies are fragmented into various laws and do not have a single unified source of law that govern data as a whole. And the present legislations do not comprehensively provide for data protection, its governance and only partly aligns with international best practices or standards. Therefore, it can be said that the data governance architecture of Nepal is fragmented, limited, ambiguous and has its own challenges towards its enforcement.

The Archives Preservation Act, 2046 (1986) outlines 'Prohibited records' which are safeguarded by the National Archives to ensure restricted access.[215] Only authorized individuals are permitted to view, move, or copy such records for a specified or unspecified duration.[216]

The RTI Act includes provisions for proactive disclosure, requiring public bodies to regularly update and make their information publicly accessible.[217] However, it also allows public bodies to withhold information on matters related to national security, national sovereignty, and those that could severely impact commercial and banking interests. Unfortunately, these exceptions

[215] Section 9, Archives Preservation Act, 2046 (1986)
[216] Section 10, Archives Preservation Act, 2046 (1986)
[217] Section 4, Right to Information Act, 2064 (2007)

are sometimes misused to conceal information, undermining the legislative intent of increasing transparency.

12.3 The emerging governance architecture involves tradeoffs among objectives such as greater accountability of powerholders, economic growth including creation of employment and wealth, resilience of systems, etc. How have different societies

(a) explicitly recognized the tradeoffs or not; and (b) handled them?**

The existing laws on data governance do not address the problem of cross border data transmission, national data storage and protection, national cyber security issue and more. The laws are not consistent with the GDPR. Compared to the GDPR, Nepal's privacy laws lack key elements, including definitions of consent, the right to be forgotten, rights to restrict processing and to be informed about processing, the right to erasure, the right to rectification, responsibilities and duties of data controllers, the requirement for a Data Protection Officer, laws for data localization, and regulations governing cross-border data exchange and trading.

Nepal is not a party to the Open Government Partnership.

Therefore, it can be said that the tradeoffs have not been recognized at all.

12.4 Are there legislative or policy innovations with potential for replication? What are the modalities of sharing experiences? Are developing countries learning from each other, or are they learning from the developed countries?

Nepal recognizes the right to privacy as a fundamental right under its constitution. To protect this right, it has enacted the Privacy Act, 2075 (2018), and the Individual Privacy Regulation, 2077 (2022). However, these laws are not sufficiently robust to protect people's privacy effectively and fall short of international best practices. The National Cybersecurity Policy, 2080 (2023), and NeGIF both promote the adoption of open standards, although they do not enforce this requirement. If such a framework for transparency is enforced properly in Nepal, it can stand out as a model for potential replication and which will influence the development of open data policies.The same can be replicated by sharing experiences with neighboring countries like India, which has more robust national cybersecurity policies and open standard mandates.

Another example where Nepal learned from a developed country is the use of the NagarikApp. The Government Integrated Data Centre (GIDC) introduced the Nagarik App to establish interconnectivity among electronic information systems in public bodies. The aim of the app is

to facilitate the swift, cost-effective, and efficient flow of services and information to citizens through a unified electronic system. GIDC is responsible for the management and operation of the Nagarik App. Such an integrated system for procuring all official records and relevant data of a citizen in Nepal can be accessed by Nepal. Such an integrated system for procuring all official records and relevant data of a Nepalese citizen can be accessed by Nepal.

Nepal's Privacy Act was greatly influenced by the Personal Data Protection Act, 2012, enacted by Singapore which governed the collection, use, and disclosure of personal data by organizations. This demonstrates that Nepal is learning from developed nations like Singapore. Singapore later enacted the Personal Data Protection Act, 2020, which added provisions like mandatory data breach notifications by organizations suffering data breaches, but such provisions and other provisions from international best practices like that of GDPR are yet to be incorporated into the prevailing laws relating to data governance in Nepal.

12.5 How were the laws and bills developed? What expertise was brought to bear? How open were the procedures? How receptive were drafters to suggestions and criticisms?

The pre-legislative procedure follows this order: policy identification and subject analysis, preparation and approval of the bill proposal, bill drafting, review of the draft bill, presentation to the Bill Committee at the Council of Ministers, and final discussion and approval by the Council of Ministers.

In the legislative phase, a member of parliament introduces the bill in either the House of Representatives (HoR) or the National Assembly (NA). The bill is then referred to the relevant parliamentary committee for scrutiny. The committee may hold public hearings and invite experts to provide their views. After thorough review, the committee submits its report and recommendations to the parliament. The bill is then debated and voted on in parliament. If passed, it is sent to the President for assent. The President can either assent to the bill or return it to the parliament with a message for reconsideration. If the parliament passes the bill again, it becomes an Act of Parliament.

A bill can be introduced by any member of the parliament, including the Prime Minister, ministers, and ordinary members. It must be in writing and must be accompanied by a statement of objectives and reasons. The bill is then referred to the relevant parliamentary committee for scrutiny. The committee may hold public hearings and invite experts to give their views on the bill. The committee then submits its report to the parliament, along with its recommendations. The bill is then debated and voted on in the parliament. A bill can be passed by a simple majority of the members present and voting. If the bill is passed by the parliament, it is then sent to the President for assent. The President may assent to the bill, or may send it back to the parliament with a message for reconsideration. If the parliament passes the bill again, it becomes an Act of Parliament.

The Law Commission of Nepal, which is responsible for drafting new laws and reviewing existing ones, also solicits feedback from the public before finalizing its proposals. For example, the Law Commission invited public comments on a draft bill that would amend the country's criminal code and received comments on the same some of which were incorporated in the final version of the bill.

There have been instances where the drafters of bills in Nepal have been less receptive to suggestions and criticisms. For example, the government of Nepal has been criticized for its handling of the recent protests against the Citizenship Amendment Bill. However, overall, the drafters of bills in Nepal have shown a willingness to listen to feedback and make changes to their proposals when necessary.

In the case of drafting the laws relating to personal data protection, privacy and electronic transactions, public consultations were held but there were not many experts involved in the field to conceptualize the broader framework of the legislation and the implications it would have in the future. There have been multiple debates about the arbitrary classification of information done by the government under the RTI Act. To date, this classification of information has not been completed.

Only recently during the drafting of the concept paper on AI by the Ministry of Communication and Information Technology public consultation and experts were hired but even then, the concept paper claims that the knowledge of the experts was limited and no expert from foreign developed countries was hired to finalize the concept paper. Therefore, it can be said that there are lack of experts in the field of AI and Data governance in Nepal.

12.6 How were capacity challenges addressed

by simplifying the laws or by tolerating incomplete implementation?**

The government agencies are open to capacity-building training, which is often supported by foreign aid.

There have been many instances where incomplete implementation of data governance laws has taken place as due to lack of experts, lack of technological advancement, gaps in the laws, etc. These have been a hurdle for the implementation of the data governance laws. There has been so many instances of cases relating to cyber crime or data breach which has not been settled till date due to a lack of understanding by the judges or the lack of technical requirements to even identify the problem.

On one hand, there is a desire to bring in investment and make the government more transparent and accountable. On the other hand, there is a push for stronger control by the state. These competing priorities create a perception that there isn't enough capacity to implement policies effectively, when in reality, the real issue might be the lack of political will and clear focus.

13 Bibliography

Statutes:

- Archives Preservation Act, 2046 (1986)
- Copyright Act, 2059 (2002)
- Company Act 2063 (2006)
- Concept Paper Regarding the Use of AI in Nepal, 2081 (2024)
- Directives for Managing the Use of Social Networks, 2080 (2023)
- Directive for Internet Service Providers, 2077(2021)
- Directive for Voice Service Providers, 2077 (2021)
- Electronic Transaction Act, 2063 (2008)
- Government Website Management and Operational guidelines, 2078 (2021)
- General Data Protection Regulation (2016)
- Guidelines (Procedural) for Access to Information, 2074 (2017)
- Individual Privacy Regulation, 2077 (2020)
- National Civil (Code) Act, 2074 (2017)
- National Cyber security Policy, 2080
- Nagarik App (Operation and Management) Directive, 2078 (2021)
- Nepal QR Standardization Framework and Guidelines, 2020
- Patent, Design and Trademark Act, 2022 (1965)
- Press and Publications Act, 2048 (1991)
- Right to Information Act, 2064 (2007)
- Statistics Act, 2079 (2022)
- Telecommunication Act 2053 (1993)
- The Constitution of Nepal, 2015
- The Privacy Act, 2075 (2018)
- Unified Directive no.3/079, Payment System Unified Directive,2079 (2023)
- Unified Directives issued by the Nepal Rastra Bank to "A", "B" and "C" Category Certified Institutions, 2079 (2023)

Articles, Journals and Reports:

- Accountability lab, available at "https://www.accountabilitylab.org/wp-content/uploads/2020/01/nepalOGP-readinessAssessment-2017sep-v3r0.pdf" (last accessed on 5th October, 2023)
- Adv. Bhaktiram Ghimire v Government of Nepal Prime Ministers Office, Ministry of Physical Infrastructure and Transport and ors., NKP 2079 (Decision no. 073-Wo-1097)
- Available at "https://dolma.gov.np/office/dept/content/description-of-public-access-module-1634724366"
- Available at "https://merokitta.dos.gov.np/"
- Available at "https://mofaga.gov.np/lgbudget"
- Available at "https://ocr.gov.np/"
- Availablt at "https://nkp.gov.np"
- Available at "https://www.nrb.org.np/contents/uploads/2023/01/PSD_unified-Directive-2079_Letter-combined.pdf" (last accessed on 3rd October, 2023)
- Bipin Adhikari, Constitutional Foundings in Nepal: Experience with Changing Parameters in Kevin YL Tan & Ridwanul Hoque, Constitutional Foundings in South Asia 165 (Hart Publishing 2021).
- Blacklist, Central Investigation Bureau, available at "https://cibnepal.org.np/assets/upload/block/blacklist_upload_2080-12-01_05_30pm.pdf"

- Digital Nepal Framework, 2019, available at "https://drc.gov.np/storage/backend/pages/resources/others/D8lp6S0TBuokqwXB7V90hB9a0dF4v6qTLGzUvN7M.pdf"
- Fiscal Budget, available at "https://www.mof.gov.np/site/publication-detail/3249" (last accessed on 5th October, 2023)
- Industrial Satistics 2079/80, available at "https://doind.gov.np/detail/218"
- Interim Const. Of Nepal, 2063, art. 107 (1) (2); Const. Of The Kingdom Of Nepal, 2047, Art. 88.
- Letter dated 2079/11/17 (1st March, 2023), Ministry of Information and Communication
- National Data Profile, National Statistics Office, available at "http://nationaldata.gov.np/"(last accessed on 1st October, 2023)
- Nepal Times, 'Open season on Hacking into gov.np' (29 Jan 2023), available at "https://nepalitimes.com/news/open-season-on-hacking-into-gov-np" (last accessed on 5th October, 2023)
- Open Nepal, Available at "https://opennepal.net/sites/default/files/doc_briefings/Briefing-Open-Government-Data-(English).pdf"
- Peng Hwa Ang & Ors., 'Shuting down of mobile phone and the downfall of Nepalese society, economy and politics', (2012) PacificAffairs, vol.85 no.3. available at" https://dr.ntu.edu.sg/bitstream/10356/105954/2/Shutting%20down%20the%20mobile%20phone%20and%20the%20downfall%20of%20Nepalese%20society%2C%20economy%20and%20politics.pdf"
- Prithvi Man Shrestha, 'Singha Durbar server continues to face cyberattacks', The Kathmandu Post,(30 January 2023), available at "https://kathmandupost.com/national/2023/01/30/singha-durbar-server-continues-to-face-cyberattacks" (last accessed on 5th October, 2023)
- PWC,'Nepal E-Government Interoperability framework-Main Report', available at "https://nitc.gov.np/assets/img/fileSystem/download/23-07-27-125812-NeGIF%20Main%20Report%20v2.0%20new.pdf" (last accessed on 7th October, 2023)
- Rabindra Ghimire, 'Digital loss in Nepal is troubling Nepal in front of the helpless government', OnlineKhabar (8 May 2023), available at" https://english.onlinekhabar.com/digital-data-loss-nepal-helpless.html" (last accessed on 6th October, 2023)
- Rudra Pangeni, 'Cartel of contractors in cahoots with government officials swindle billions of rupees, govt report reveal', Centre for Investigative Journalism (15 January 2018), available at "https://cijnepal.org.np/cartel-contractors-cahoots-govt-officials-swindle-billions-rupees-govt-report-reveals/"(last accessed on 7th October, 2023)
- Samajha Bk, 'Too many identity cards are burdening Nepal with big money and citizens with redtape: time to rethink?', OnlineKhabar, (16 September 2022), available at "https://english.onlinekhabar.com/many-identity-cards-nepal-problem.html" (last accessed on 6th October, 2023)
- Supreme Court of Nepal, available at "https://supremecourt.gov.np/web/" (last accessed on 1st October, 2023)
- Table S.No.9, Decision of the Council of Ministers Meeting held on 2079/11/15 (27th February, 2023)
- The Himalayan Times, 'Open season on Hacking into gov.np' (29 Jan 2023),available at "https://nepalitimes.com/news/open-season-on-hacking-into-gov-np" (last accessed on 5th October, 2023)
- The World Bank, "Use of data in the private sector of Nepal the current state and opportunities in finance, education and the media" (July 2020) pg.12, available at "https://documents1.worldbank.org/curated/en/805261601023506163/pdf/Use-of-Data-in-the-Private-Sector-of-Nepal-The-Current-State-and-Opportunities-in-Finance-Education-and-the-Media.pdf"

- Tika R Pradhan, 'Government backtracks on information classification, The Kathmandu Post, (31 January 2023), available at "https://kathmandupost.com/national/2023/01/31/government-backtracks-on-information-classification" (last accessed on 6th October, 2023)
- Writ no.069-WO-0268
- Writ No. 01 063-00001 of the year 2063 B.S. (2006)
- Writ No. 3561 of the year 2063 B.S. (2006)

14 Annexure-1:

Interview with director of the Central Bureau of Statistics, Mr. Manohar Ghimire:

The following points were articulated by Mr. Manohar Ghimire, Director of the Central Bureau of Statistics:

The process of collecting survey data and that the first step of the process is that the questionnaire for the survey has to passed by the cabinet. it is a 5yrs project, There is a micro-data catalog where all the data are stored and kept. All raw data are stored as micro-data. These micro-data are kept for sale- anyone can buy such data- but such data cannot be bought through an online portal or through international transaction as there is no international payment gateway available, therefore any international entity wanting to buy such micro-data has to write a formal letter and then through cash transaction buy such data. But there is no written or formal procedure for the same. The buyer has to go the thematic authority. Even if any governmental organization asks for such data there is no formal to give the same. There are no data bank for storage of data in Nepal- no data processing center. The data collected is stored in flash drives or CDs or physical books. There is an elibrary for the storage of data but only selected or a portion of the whole raw data is kept in such library. If such data is lost there is no recovery process. But this has never happened In Nepal the micro-data or all the data collected are with the 150 employees of the NSO- the raw data are in the hands of 3-4 people in Nepal. Therefore, in Nepal those 3-4 people are the security system or guardians of the data collected. There has not been any incidents of such data being breached or such people selling data. This might also be because of the lack of market for such data and lack of understanding of the employees with regard to such data market. With respect to protection of privacy the Statistic acts provides for the sanction of any breach of data or for the misuse of power/trust by any employee. There is no practice of reuse of data- once data is used for a purpose it is removed or never used again or lost. For eg: the Health or Education ministry collects data with regard to it field of study, then that data is processed and only its summary or general overview of that used and published in a single table on its websites, then such data is never reused again for any purposes and it is not accessible to any outside body. The practice in NSO is that data is retained for at least 20 years, but this is not written anywhere in the law, it is just a practice and old data is stored. But if any information of 15yrs old is to be taken out and studied such data can not be given or found. Only the micro-data can be bought which is again 10% of the raw data collected. With respect to openness of data or data transparency- the NSO is of a very conversative nature with regard to such transparency as is the thought of most other governmental authorities. But as per Manohar Ghimere sir; he suggests that we should have a separate privacy law, a formal written process in our law for data sharing or sale, we need a law for data protection. The practice in the NSO for now is enough for the protection of data as we have not faced any issue of data breach or illegal sale of data, but there are chances that the people who are in charge of the data might breach their trust or once those people are no more in charge of the same the data might fall in the wrong hands. Since it has not happened yet there are no issues raised with regard to this but precautions must be taken. The information collected with regard to Finance, Industry and some parts of Census are kept confidential. Expensive software's of high quality are bought by the government of Nepal. But its use is yet to be seen.

15 Annexure-2:

Interview with the National Information Commission:

First RTI was enancted in Sweden, Then, later 136 countries followed the same. Formal classification of information at the national level remains incomplete in Nepal. While some organizations have undertaken their own classification processes, these classifications are not officially recognized. Consequently, the accuracy of such classifications cannot be definitively determined. For instance, Loksewa Ayog (Public Service Commission) classified its information according to what could be disclosed under the Right to Information (RTI) Act and what could not. However, the RTI office challenged Loksewa Ayog's classification, indicating that it was either incorrect or unacceptable. The RTI Act itself stipulates penalties for organizations that withhold information. The RTI office rigorously enforces these provisions, issuing warnings and further notices if an organization fails to comply initially. Regarding information confidentiality, the RTI office emphasizes that when information is withheld or kept confidential, it is not to conceal it from citizens but rather to uphold national security or prevent potential harm if the information were made public. Consequently, information that could potentially incite unrest or conflict among groups or citizens is kept confidential until the situation stabilizes. While information provided under the RTI Act is generally accurate, instances of incomplete disclosure are not uncommon. However, organizations are typically responsive to requests for additional or full information when such discrepancies are brought to their attention. He informs that there are three preconditions for a full-fledged enforcement of the RTI Act. Firstly, there must be digitization of all governmental records and use of open software's has to be mandated. This is considered as the biggest problem for the enforcement of RTI. Secondly, all governmental organizations and public body must have high ethical value as it is seen in practice that all government employees hesitate to give complete information and would rather not give any information if possible. Lastly, there is lack of awareness amongst the citizens of Nepal and the Media also needs to play a more proactive role in spreading awareness and providing information. With respect to publication of any information though the RTI Act provides for it to be published in local languages as well, but in practice it is seen that it is published only in Nepali and only in rare cases in local languages. There are no cases of information being misused or information being corrected. There only instances of information being incomplete wherein full information is given again. The RTI provides for the punishment incase of misuse of information. Section-35 The RTI also provides for the punishment incase any governmental body tries to withhold information and it was reiterated that the National Information Commission takes such an offence very seriously. If any government officer repeatedly tries to withhold information then the National Information Commission writes a letter against such an officer then the departmental action taken against such an officer is very strict. Therefore, since the sanction for the same is strict there have not been any instances of information being withheld. Though the RTI provides that information shall be given within 15 days by the information commissioner, it is true in most cases but it takes more time to collect information form any other authority, hence more time is taken in practice to provide the information to any citizen. Our RTI is also similar to that of Sri Lanka as our RTI also has an overriding affect. Though, it is not explicitly mentioned in the RTI regarding this effect, it is true in practice that RTI shall prevail over other subordinate legislations.

16 Annexure-3:

Interview with GIDC:

GIDC is the government data center. All government data is stored in this office and in recovery in Hetauda. GIDC and GRDC (Hetauda) are linked through fiber cable which means even if one data center has some problem all the working can be done through the data of another center. Nagarik app was created by GIDC to integrate govt profiles. Even if data is lost there is a backup storage to recover the data. But each data or information is classified by its importance or according to its criticality and then sent for storage. For security- Web application firewall, End point security, automated system, encryption. There are various methods for storage and backup of data, the first time it takes time as data is very large then it is synced to backup. According to the criticality of a data such as financial data it is migrated in real-time. Payment systems operators do not come under GIDC. Only NCHL, NEPSE, and a few trading house Share market data is migrated in time. GIDC only looks after the data of the government and public entities, GIDC's policy doesn't allow to store private data of private entities. As per IRD- Financial data should not go abroad or should stay in Nepal. It is mandatory for billing systems. Passport office has their own data center. The Website Management Act- Discussion is going on to make a new privacy and data protection related legislation. Talking about the security of data- firstly lets talk about the physical presences of GIDC which is located inside Singhadurbar which is a highly secure place so no one can access the physical location of the data center. Then we have Domain: Mercantile- .np is the top server, .gov.np server are with the GIDC, Mercantile has authority to give name server of .np, Eg; someone sends request for ABC.gov.np to be registered, then GIDC directs Mercantile to point to the name server then again GIDC makes the Domain. Therefore, Mercantile just points to the There are no laws to govern data localization. But there is cabinet decision to store government data in GIDC. E-governance master plan- it says that SOA (service oriented architechture) Enterprise Service Bus (ESB)- it promotes interoperability framework among organization API gateway- for interoperability There are no laws mandating interoperability of any organization. Incase of GIDC they save data logs for a period of 3 years. It is different as per organization and in international GIDC is not a governing body of private entity or data of private company but GIDC has been acting as a bridge between gov and private entity in PPP projects. There are no laws for protection of privacy. Incase of confidentiality it is guided by the contract done between the parties GIDC does MOU and puts condition for privacy and non-disclosure agreement is also done. No laws to erase or amend data. In practice it is seen that if any entity asks to delete its data GIDC will delete it. No laws for cross boarder data flow There is a need for an umbrella legislation which cover all aspects related to data which will mandate us to comply to data protection. E-Governance Committee (EGC) – in Estonia Europe data of its citizen is only collected. The policies should define the process of collection, use and storage of data and then the technology should also be developed in such a way. The laws of Nepal provide for

17 Annexure-4:

Interview with Department of Information Technology (DOIT):

GIDC is the main data center, and in Hetauda we have a data recovery center which stores all the back up of GIDC. There is a problem of repetition of data. This problem has been addressed to the Ministry of Information and Communication multiple times. There are no laws or regulation for interoperability in Nepal and in practice such coordination or data sharing between various government agencies are done on the basis of mutual relation between those agencies. Common standards are used in all government websites There are no practice or laws with respect to cross boarder data exchange or trading. Incase of license, it is made in India which is done in a contractual basis and for the protection of our data and privacy before giving any work to foreign company a non-disclosure agreement is mandatorily signed Social media regulation was made for government organization, to handle their social media page. Social media is the most vulnerable platform from which most cyber attacks are seen. For the protection of privacy, we have 24hr monitoring of traffic and prevention is done by the cyber department of the Ministry of Information and Communication, other than that we can file a complaint with the cyber bureau as per ETA. But for the protection of individual privacy there has not been any progress. Open standards- it means globally recognized standards. Data is not traded from Nepal, we can only provide data for specific work if needed. There is a concept of transparency which is applicable for any government organization, it must be followed to the extent possible depending on the type of data, as some information has to be classified and some might have a negative effect if made public. Therefore, it depends on the type of data. Data has to be restrictive as there are more cyber attacks than laws in Nepal. Restricting data means keeping data safe which is also applicable in countries like USA as well. The social media regulation was also made not to restrict a users personal thoughts and views but it was made to regulate illegal activities. Majority of the population in Nepal do not have the awareness about the use of social media or the internet, and this is true for well educated people as well. This is because no one reads the terms and conditions given in any website, we automatically give our consent for the same without knowing the repercussions for the same. There are no laws in Nepal which are coherent with the GDPR. There are no laws for modification, processing or erasing of data. But the IT bill tries to include such laws.

18 Annexure-5: Gender Questions

Q.1 To what extent and how do the policies/laws/strategies relating to data governance mention/recognize the importance of gender disaggregated data? How is this enforced? For example, do national statistics and open data policies make gender disaggregated data available for all data points ? Is this legally mandated? Under which laws?

The importance of gender disaggregated data is shown in the Gender Equality and Social Inclusion Strategy, 2021 (2077) where it emphasizes the importance of collection and analysis of disaggregated data which is then used for the planning, budgeting, monitoring and reporting by the local provinces.[218]

However, aside from the mentioned strategy, there are no specific laws in Nepal that mandate the comprehensive availability and enforcement of gender disaggregated data across all data points in national statistics and open data policies.

Q.2 Is there legal recognition in the data for categories other than the traditional male vs female? . If so is this implemented in practice? i.e. collection and reporting both allow for categories beyond male and female, and might include "other", or more detailed options like "transgender". For example think in India immigration forms allow male, female and 'other' ([219] could you please check this), so this must be backed up by some change in law at some point?

In the case of Sunilbabu Panta v. Office of Prime minister, Government of Nepal[220] the Supreme Court held that non-cisgenders should also be identified and ordered that citizenship cards should have another option as "other" for all non-cisgender identifying people.

The Central Bureau of Statistics also distinguishes three types of gender i.e. male, female, and other gender (consisting of all genders and sexual minorities) while collecting the data for the census report.[221] The form which needs to filled out also mentions another category

In the case of Pinky Gurung v. Office of the Prime Minister and Others[222] same-sex marriage was legally recognized for the first time and the court issued an interim order to maintain a separate registry for the registration of such marriages.

Q.3. Is there a provision in the law or a general practice that enables self identified genders (i.e. instead of just the "assigned at birth" categories of usually male vs female, or in some countries as male vs female vs 'other')?

The Constitution on Nepal also provides that the right to equality shall be provided to "gender and sexual minorities"[223].

The Privacy Act also defines one's sexual orientation as 'sensitive information'[224].

---

218 Gender Equality and Social Inclusion Strategy 2021 (2077)Available at" https://plgsp.gov.np/sites/default/files/2023-02/PLGSP%20Gender%20Equality%20and%20Social%20Inclusion%20%28GESI%29%20Strategy%202021%E2%80%932023.pdf"

219 **Pranesh?**

220 Writ no.0287 of the year 2070 B.S (2013) (Decision No.9875)

221 National Population and Housing Census, 2021, available at "https://censusnepal.cbs.gov.np/results/downloads/national"

222 Writ No.079-WO-1382

223 Article 18 (3), Constitution of Nepal, 2072 (2015)

224 Section 27 (e), Privacy Act,

Therefore, while there are legal recognitions and certain strategies that highlight the importance of gender disaggregated data, the enforcement and comprehensive legal framework mandating its collection and availability are limited in the context of Nepal.

References

OECD. *Going Digital Guide to Data Governance Policy Making*. OECD, 2022. https://web.archive.org/web/20231116075558/https://www.oecd-ilibrary.org/science-and-technology/going-digital-guide-to-data-governance-policy-making_40d53904-en. https://doi.org/10.1787/40d53904-en.