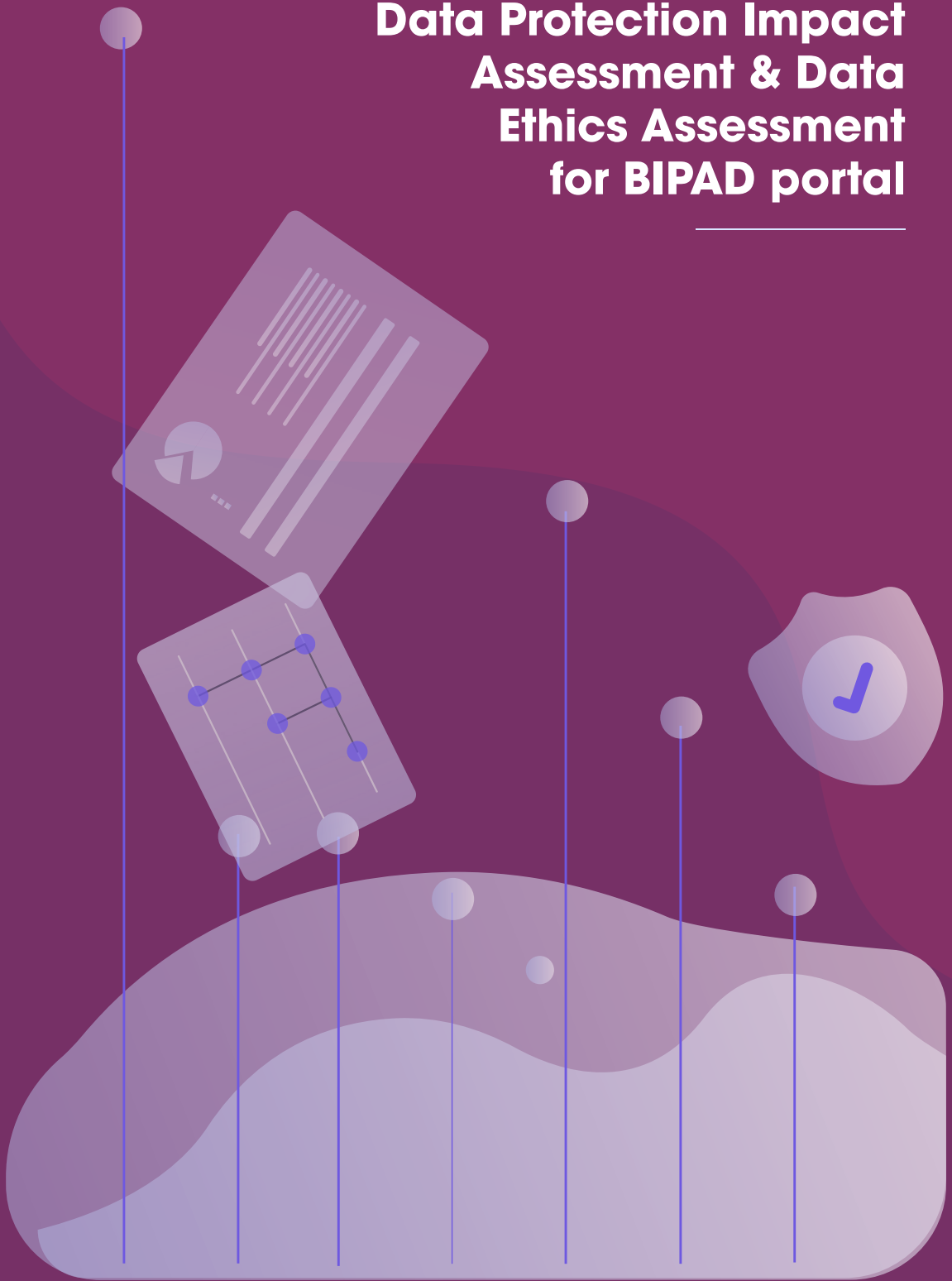
Data Protection Impact Assessment & Data Ethics Assessment for BIPAD portal



Publication Date
March 2021

Published by
Youth Innovation Lab
Banshidhar Marg, Kathmandu 44600
Nepal
Tel: +977 9851115919
Email: info@youthinnovatiolab.org
Website: www.youthinnovationlab.org

Written and Compiled by
Sanchita Neupane
Niroj Panta

Publication Team
Pradip Khatiwada
Sajana Maharjan Amatya
Carolyn O'Donnell
Reena Bajracharya
Pranaya Sthapit
Arnav Upadhyay
Angela Tamrakar
Alina Khatiwada

Designed by
Paras Shrestha

Citation
Youth Innovation Lab (2020). Data Protection Impact Assesment and Data Ethics Assesment For BIPAD portal.

Funded by **UK AID** *with the technical support from the* **Data for Development Programme** *under* **The Asia Foundation.**

CONTENTS

ACRONYMS

BIPAD	Building Information Platform Against Disaster
CBS	Central Bureau of Statistics
CSV	Comma-separated values
DHM	Department of Hydrology and Meteorology
DMG	Department for Mines and Geology
DPIA	Data Protection Impact Assessment
DEA	Data Ethics Assessment
DRR	Disaster Risk Reduction
DRRM	Disaster Risk Reduction and Management
GoN	Government of Nepal
GDPR	General Data Protection Regulation
ICIMOD	International Centre for Integrated Mountain Development
METEOR	Modelling Exposure Through Earth Observation Routines
MoHA	Ministry of Home Affairs
MoU	Memorandum of Understanding
NAP	National Adaptation Plan
NDRRMA	National Disaster Risk Reduction and Management Authority
NEOC	National Emergency Operation Centre
NPC	National Planning Commission
OSM	OpenStreetMap
SFDRR	Sendai Framework for Disaster Risk Reduction
UN	United Nations
UNDRR	United Nations Disaster Risk Reduction
YI-Lab	Youth Innovation Lab

FOREWORD

This report is commissioned by the team of independent consultants and the recommendations made in this report are primarily targeted for BIPAD portal internal team. The report starts with a brief background on data protection, data ethics and data privacy. The report then presents the findings of the data protection impact and ethics assessment, followed by recommendations for strengthening BIPAD's data protection as well as ethical procedures. This report is aimed at identifying gaps and challenges and recommending best practices for the responsible storage, processing and sharing of data for disaster resilience and shaping a framework for data privacy and data protection.

There is a growing trend of collecting and analyzing data on various thematic areas across the humanitarian and development sector. To ensure best practice, the integration of new data with existing sources should adhere to global standards on data privacy and data protection. In today's data initiatives, detailed planning, clear procedures, budget provision and formal allocation of responsibilities are necessary to ensure responsible data practices are implemented from the start.

The analysis on BIPAD portal Data Protection Impact Assessment (DPIA) is based on the review of Nepal government's Privacy Act, 2018 and other international regulations on data protection, such as, OECD guideline, European Union's General Data Protection Regulation (GDPR) guideline. Review of some of the publicly available databases was carried out, specifically the guidelines set out by ICRC on digital data protection and by UN OCHA on humanitarian data management process. While the report takes a reference of EU GDPR specifications for DPIA template it has been tailored to meet the specific needs in the context of data processing explicitly in relation to BIPAD platform only. Hence, the global standard template has been modified and some of the sections that seemed irrelevant to the context are left out.

Considering the minimal level of risk in relation to the data protection in BIPAD portal; the assessment also takes into account the ethical risk associated with collecting, processing and disseminating data and information in the system. However, due to the limitation of time and scope of the document a thorough and systematic assessment of ethical risk has not been carried out acknowledging data ethics being a very broad field. However, several indicators are laid out in the report against which the ethical assessments can be carried out for existing and potential data partners.

Various recommendations are made in this report as a series of bullet points clarifying the actions to make it clear for BIPAD team to set out the data management strategies, policies and protocols. It is recommended for BIPAD team to systematically analyze the risk associated with different data sources from multiple agencies and consider the quality and ethics criteria set out in the report before making agreement with new data partners.

1. INTRODUCTION

This report encompasses the assessments and recommendations emanating from the analytical assessment: Data Protection Impact Assessment and Data Ethics Assessment for BIPAD portal.

The report starts with a brief background on data protection, data ethics and data privacy. The report then presents the findings of the data protection impact and ethics assessment, followed by recommendations for strengthening BIPAD's data protection as well as ethical procedures.

The use of data and evidence for decision making has been a strategic priority for many development related issues and interventions. The use of data and evidence is often recognized as an enabler for meeting the Sustainable Development Goals (SDGs) and other post 2015 development agenda including Sendai framework, Urban Agenda and Paris Agreement among others[1]. The use of data is essential for monitoring development and humanitarian progress, but also for informing critical decisions, planning, advocacy and accountability and to inclusively engage stakeholders at all levels to advance evidence-based policies and programmes. Thus, there is a growing trend of collecting and analyzing data on various thematic areas across the humanitarian and development sector.

The need for integrating new data sources and technologies in humanitarian and development assistance as well as in the process of achieving the SDGs is essential[2]. To ensure best practice, the integration of new data with existing sources should adhere to global standards on data privacy and data protection. In today's data initiatives, detailed planning, clear procedures, budget provision and formal allocation of responsibilities are necessary to ensure responsible data practices are implemented from the start. Working with data comes with data responsibility. Lacking formal policies, procedures and practices on data processing, or handling raw and processed data irresponsibly can cause or be perceived to cause harm to organizations, communities and citizens at large.

Building Information Platform Against Disaster (BIPAD)[3] is an integrated and comprehensive Disaster Information Management System created in line with the DRRM act endorsed by parliament of Nepal in September 2017. BIPAD portal is built upon the concept of creating a national portal incorporating data and information from multiple sources including but not limited to government bodies, non-governmental organizations, academic institutions and research organizations. It comprises six core modules; Dashboard, Incidents, Damage and Loss, Real time info, Profile and Risk Info. The data and information contained in these modules provides an evidence base on all stages of the disaster cycle; mitigation, preparedness, response and recovery. National and subnational governments can make use of the data and information for policy making, resource allocation and informing their disaster risk management plans and actions. The scope of BIPAD portal, however, is not limited to the governments but has potential value for a range of other DRM stakeholders, such as multilateral and bilateral development partners, international and national NGOs, research organizations and civil societies at large.

[1] United Nations Development Group(UNDG), https://unsdg.un.org/
[2] United Nations Global Pulse (UNGP,2016), https://www.unglobalpulse.org/
[3] Government of Nepal, Ministry of Home Affairs, BIPAD portal: https://bipadportal.gov.np/

BIPAD Data Ecosystem

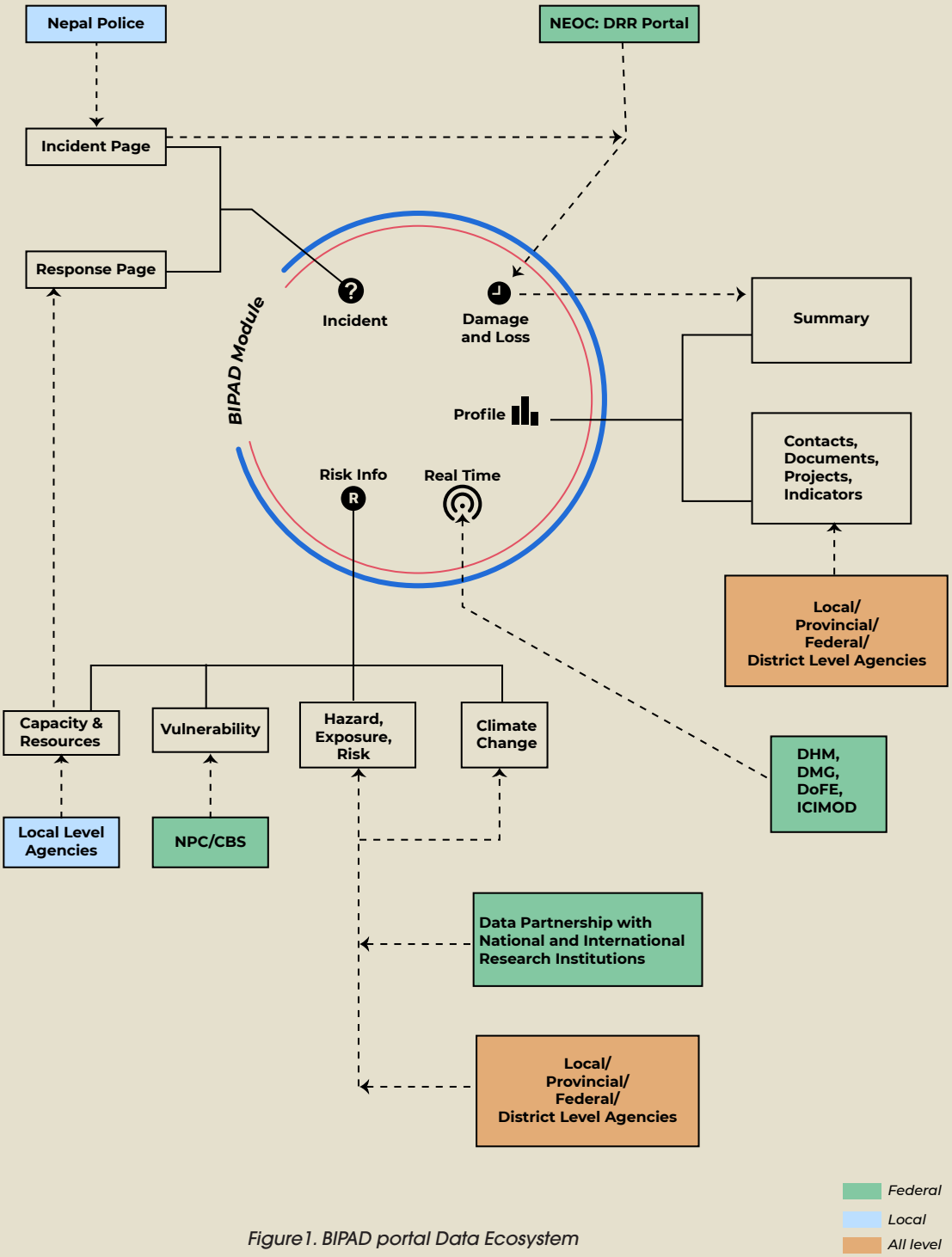


Figure1. BIPAD portal Data Ecosystem

Figure 1 illustrates the data ecosystem within BIPAD portal, especially focusing on sources of data. While BIPAD portal is not a producer of new data, it integrates existing data available from multiple sources. These data sets are either open sourced, published in journal papers, outcome of research projects or government owned data sets that are publicly available. Some of the data sources in existing version of BIPAD portal are-

Sn	Description
1	Data on disaster loss and damage (human and economic) from Nepal Police/Ministry of Home Affairs (MoHA)
2	Department of Hydrology and Meteorology (DHM)'s rainfall and water level data
3	National Seismology Centre (NSC)'s earthquake data
4	Central Bureau Statistic (CBS)'s individual and household data
5	National Planning Commission (NPC)'s socio-economic data
6	Department of Water Resources and Irrigation (DOWRI)'s flood hazard data
7	Department of Forest and Environment (DoFE)'s air pollution data
8	International Centre for Integrated Mountain Development (ICIMOD)'s National Adaptation Plan (NAP) climate change data, forest fire data, and streamline data
9	World Food Program (WFP)'s flood inundation data
10	Durham University's earthquake risk data, landslide hazard data and landslide risk data
11	METEOR's flood hazard, earthquake hazard and landslide hazard data
12	Open source data of critical infrastructures (Health Institutions, Educational Institutions, Financial Institutions, Governance)

DPIA does not have to eradicate the risks altogether but should help to understand risks, minimize risks and assess whether or not remaining risks are justified.

Ethics is particularly more important in the domain of data management, as there has been a rapid development in technical tools compared to instruments that governs their use.

1.1 Background: Why DPIA and DEA for BIPAD portal?

Data Protection Impact Assessment (DPIA) is a tool for identifying and minimizing data protection risk by systematically and comprehensively analyzing data flows and processing. The purpose of DPIA is to identify, evaluate and address the risks to personal data arising from a project, policy, programme or other initiatives.

Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data[4].

DPIA does not have to eradicate the risks altogether but should help to understand risks, minimize risks and assess whether or not remaining risks are justified. DPIA is only mandatory where processing is "likely to result in a high risk to the rights and freedoms of natural persons". BIPAD portal uses information or data that has been collected, or shared lawfully by data partners. Although BIPAD portal is not directly involved in processing of any individual data, it processes a bulk of data related to human vulnerability, poverty, individual access to health and education etc. The database is meant to inform policy and practice for public and private entities but it is important to monitor the use of data and the purpose for which data are downloaded.

[4]European Union, Data Protection under GDPR, https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm

Similarly, there are also a number of ethical concerns associated with data management and analysis for public information sharing. Ethics is defined as the study of what is morally right and wrong, or a set of beliefs about what is morally right and wrong.[5] The role of ethics is essential in the context of disaster risk management where diverse individuals form a range of background come together in a pursuit of a common goal: reducing disaster risk, building resilience and protect people affected by disasters. Ethics is particularly more important in the domain of data management, as there has been a rapid development in technical tools compared to instruments that governs their use.[6]

According to Luciano Floridi and Mariarosario Taddeo, "data ethics can be defined as a branch of ethics that studies and evaluates moral problems related to data (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including artificial intelligence, artificial agents, machine learning and robots) and corresponding practices (including responsible innovation, programming, hacking and professional codes)."[7]

In practice, public sector institutions typically approach data ethics as "a branch of ethics that evaluates data practices with the potential to adversely impact on people and society — in data collection, sharing and use."[8]

BIPAD portal is a public database and the ethical considerations can be accessed on the basis of following indicators[7]:

- **Validity**: Is the data and information representative of what we want to measure? How credible are the data sources and how do we ensure that the data is the accurate reflection of ground reality?
- **Bias and Fairness:** Is there a systematic skewing of the data collected and/or is there any prejudice or favoritism in the data or model? *(For instance, has there been an over- or underestimation of vulnerability and risk or are some members of the population more or less represented than others?)*
- **Transparency and Explainability:** Is there a clear documentation of the data management process and visibility on how the model or algorithm(s) function? *(For instance, can someone not directly involved in the process explain what is happening?)*
- **Privacy and Anonymity:** Can the data or its use reveal the identity of an individual or group of people?
- **Ownership of data and insights:** Are the rights to the data and related insights clearly defined? *(For instance, is it clear how decisions are made regarding how and by whom the data can be used, how problems in or related to the data are rectified, and other related issues?)*

[5]Cambridge Dictionary, available here: https://dictionary.cambridge.org/dictionary/english/ethics
[6]Guidance Note Series Data Responsibility in Humanitarian Action Note #4: Humanitarian Data Ethics, https://centre.humdata.org/wp-content/uploads/2020/02/guidance_note_ethics.pdf
[7]Floridi L., Taddeo M. 2016. What is data Ethics? Phil. Trans. R. Soc. A 374: 20160360. http://dx.doi.org/10.1098/rsta.2016.0360
[8]Open Data Institute. 2017. Helping organizations navigate ethical concerns in their data practices; https://www.scribd.com/ document/358778144/ODI-Ethical-Data-Handling-2017-09-13.

Personal Data means any information relating to an identified or identifiable natural person. A Data Subject is a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to Personal Data.

Personal data: What it means?[9]

Personal Data means any information relating to an identified or identifiable natural person. A Data Subject is a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to Personal Data.[10]

The following list of personal data is taken from the International Organization for Migration's data protection manual. The manual provides a comprehensive list of personal data categorized into different sub sectors. Although the list may not be exhaustive; it contains most of the personal data that can be attributed in the context of disaster risk management and particularly in the context of BIPAD portal.

- **Biographical data** such as name, date of birth, marital status, address or last place of residence, employment, contact details, age, language, sex, gender, sexual orientation, race, ethnic or social origin, nationality, religion, culture, political opinions or other beliefs, membership of a particular group, physical or mental disability and health status;
- **Biometric and genetic data** such as fingerprints, iris scans, hand patterns, facial image, voice recognition, and DNA samples;
- **Background data** such as family and household history, relationships with relatives, community members, and close associates;
- **Images and recordings** such as pictures or photographs, television images, videos, voice and digital recordings, medical X Rays, ultrasound and other medical images;
- **Corroborating materials** such as medical reports, psychological reports, hotline reports, police or other official and unofficial reports; Personal documents such as health records, financial records, bank details, and criminal records or activities;
- **Verification documents** such as originals or copies of passports, identity cards, social security cards, birth certificates, temporary permits, driver's license, visas, marriage certificates, school diplomas, university records, medical certificates, property titles, and employment contracts or recruitment offers;
- **Material circumstances** such as experience of human rights violations and transit details including route taken, education, employment history, work address.

[9]Institute of Migration (IOM) data protection manual; https://publications.iom.int/books/iom-data-protection-manual
[10]ICRC Handbook of Data Protection in Humanitarian Action; https://www.icrc.org/en/data-protection-humanitarian-action-handbook

1.2 Objectives of Assessment

This research is aimed at identifying gaps and challenges and recommending best practices for the responsible storage, processing and sharing of data for disaster resilience and shaping a framework for data privacy and data protection. This allows adopting responsible data practices in BIPAD portal.

The specific objectives of the research are-

- **Identify risks** relevant to BIPAD portal pertaining to data protection or data ethics
- **Suggest mitigation** measures to minimize the identified risks in BIPAD portal
- **Assess** whether the remaining risks are justified
- **Suggest measures** to ensure data protection and avoid ethical risks during system upgrades

2. APPROACH & METHOD

This analysis on BIPAD portal Data Protection Impact Assessment (DPIA) is based on the review of Nepal government's Privacy Act, 2018 and other international regulations on data protection, such as, OECD guideline[11], European Union's General Data Protection Regulation (GDPR) guideline[12]. While BIPAD portal is national level information portal, acknowledging the fact that the data may have been produced outside Nepal, data may be used outside of Nepal and to ensure the portal adheres to global best practices the aforementioned polices and guidance are reviewed in addition to the Nepal Privacy Act.

The assessment framework has adopted the EU's GDPR 2016/679, which is a regulation in EU law on data protection and privacy. GDPR is comprehensive and relevant to a wide range of contexts of data.

Having very little processing of personal data and also, since the data issues in BIPAD portal relate not just to data protection but also have caveats in context to data ethics, the ethical issues need to be understood before the system becomes fully operational. Hence, while using the assessment framework of GDPR for data protection and privacy, the research team has incorporated some aspect of assessment of ethics alongside to provide holistic recommendations around data handling.

2.1 Steps for DPIA

This assessment undertaken for BIPAD portal includes following steps adapted from GDPR's standard template of DPIA-

Based on the assessment, operational recommendations are proposed at the end of the report.

[11] ICRC Handbook of Data Protection in Humanitarian Action, https://www.icrc.org/en/data-protection-humanitarian-action-handbookata.htm
[12] European Union, General Data Protection Regulation (GDPR), https://gdpr-info.eu/

2.2 Legal Provision in Nepal

Article 28 of the Constitution of Nepal, 2015 has declared the right to privacy and protection of information as a fundamental right. Although the Criminal (Code) Act, 2017 has a separate chapter on laws related to offence against privacy, the Privacy Act 2018[13] entails wider issues with the purpose of giving full effect to the constitutional right to the privacy of body, residence, property, documents, data, communication and character of a person.

The OECD Guideline[14] and GDPR define personal data as any information relating to an identifiable person. GDPR states personal data as the identifier that can help to identify the person such as name, identification number, location data, online identifier and other aspects as mental, physical, physiological, genetic, mental, economic, cultural or social identity of the natural person. The Privacy Act, 2018 clearly stipulates the list of information that it considers to be the personal data.

The Privacy Act prohibits collection, storage, preservation, analysis, procession or publication of any personal data without the approval from an authorized person.

While receiving the consent, issues such as time of information collection, subject matter of the information, nature and purpose of data, methodology of information collection and protection of collected information have to be disclosed to the concerned person beforehand. However, the privacy act makes provision for collection/analysis and possession of such data by authorized bodies for specific purposes. For example, Nepal police collect personal data during disaster for rescue and relief.

The Privacy Act also states that the personal information that has been collected by any public body shall be protected by such body

The Privacy Act prohibits collection, storage, preservation, analysis, procession or publication of any personal data without the approval from an authorized person.

and have to make appropriate arrangement 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.

Notably, the Privacy Act states that the following information regarding the person holding a public post shall not be deemed to be his or her personal information:

- His or her post and office address, telephone number or email address through which contact may be established,
- Name of the person signing any letter or document issued or written by a public body, and his or her post, description of job to be performed by him or her and its nature, matters relating to the conditions of his or her service.

[13]The Privacy Act, 2018, http://www.lawcommission.gov.np/en/archives/20722
[14]OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

BOX 1. PERSONAL INFORMATION AS PER PRIVACY ACT, 2018

1. Caste, ethnicity, birth, origin, religion, race or marital status of an individual;
2. Educational qualification of an individual;
3. Address, telephone or email address of an individual;
4. Passport, citizenship number, national identity card number, driving license number, election identity card number or any other details provided by public entity;
5. Letter sent or received by a person which states personal information;
6. Thumb impression, palm lines, retina of eye, blood group or biometric information of a person;
7. Criminal background and punishment served by a person for any criminal offense; and
8. Issues relating to nature of opinion and view presented by any professional or expert presented during a procedure to render any judgment in any decision-making process.

2.3 General Data Protection Regulation

General Data Protection Regulation (GDPR) aims to simplify the regulatory environment for business so both citizens and businesses in the European Union and elsewhere can fully benefit from the digital economy. Under the terms of GDPR, not only do organizations have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it are obliged to protect it from misuse and exploitation, as well as to respect the rights of data owners - or face penalties for not doing so.

GDPR is increasingly seen as a global standard by which most of the data related initiatives comply. Although Nepal does not fall into the GDPR jurisdiction it has been used as a benchmark to access the data protection risk within BIPAD system. DPIA is required under the GDPR any time a new project that is created that likely to involve "a high risk" to other people's personal information. The DPIA template has been tailored to suit the needs of BIPAD portal.

The GDPR sets out seven key principles-

1. **Lawfulness, fairness and transparency:** Any processing of personal data should be lawful and fair. It should be transparent to individuals that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.

2. **Purpose limitation:** Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. However, further processing for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes (in accordance with Article 89(1) GDPR) is not considered to be incompatible with the initial purposes.

3. **Data minimization:** Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum.

4. **Accuracy:** Controllers must ensure that personal data are accurate and, where necessary, kept up to date; taking every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. In particular, controllers should accurately record information they collect or receive and the source of that information.

5. **Storage limitation:** Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

6. **Integrity and confidentiality (security):** Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorized or unlawful access to or use of personal data and the equipment used for the processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

7. **Accountability:** Finally, the controller is responsible for, and must be able to demonstrate, their compliance with all of the above-named Principles of Data Protection. Controllers must take responsibility for their processing of personal data and how they comply with the GDPR."[15]

[15] https://www.dataprotection.ie/en/individuals/principles-data-protection

3. ASSESSMENT & ANALYSIS

3.1 Data Protection Impact Assessment for BIPAD portal

01

IDENTIFY THE NEED FOR DPIA

This section explains broadly what project aims to achieve and what type of processing it involves, summarizing the need for a DPIA.

BIPAD portal (https://bipadportal.gov.np/) aims to become a one stop platform to accessing disaster related data and information across the country. It is built upon the concept of data partnership and sharing among multiple stakeholders. As BIPAD portal entails no processing of personal data, there is no high-risk, however, it is still prudent to conduct a Data Protection Impact Assessment (DPIA) to minimize liability and to ensure that the best practices for data security and privacy are being followed in the system. As set out in EU GDPR, apart from personal data processing, it is still relevant to conduct DPIA in case of using new technologies for such a publicly accessible data platform.

While BIPAD portal aims to be an integrated platform for disaster related data and information, it does not collect any data on its own rather finds an organization that is already collecting the desired data and information. Thus, there is a potential of risk transfer from data partners even though BIPAD portal in its current version, has no processing of personal data and thus no major risks to the rights and freedom of people. Hence, to comprehend the risks that might get transferred from partner agencies, it is essential to understand data collection and processing techniques before making any agreement on data sharing with agencies.

Also, as the system evolves, it might be important to integrate geocoded household data or other personal data in BIPAD portal in future. This indicates the necessity to scrutinize the existing and prospective data on BIPAD portal, conduct DPIA and establish suitable data protection measures beforehand.

The other important reason for conducting DPIA is to ensure that the BIPAD system has been assessed under data ethics, data protection and privacy requirements with recommendation of suitable mitigation measures. This will impart more confidence to DRRM stakeholders and humanitarian actors in using BIPAD.

02

DESCRIBE THE PROCESSING

This section explains how data is collected, stored and shared and if there are any identified potential high risks. The explanation includes nature, scope, context and purpose of the processing.

Nature of Processing: BIPAD portal is not the producer of any humanitarian or disaster related data. The system is designed based on the concept of data partnership and data sharing across multiple stakeholders (government's ministries and departments, academic institutions, non-government organizations including UN agencies).

Currently, YI-lab collaborates with data partners based on mutual understanding, then collects data from source and visualizes the data in BIPAD portal with consensus from data producers/owners. Most data are reserved for the purpose of understanding trends; hence no timeline is defined for data retention. Data details including literature if any and metadata are also collected before using the data. Once the data is visualized, feedback from data producers/owners as well as experts from DRRM sectors are utilized to ensure quality in data visualization.

The raw data received from different partner agencies is being hosted at BIPAD portal and is made publicly available through the portal with visualization. Thus, the data risks are mostly secondary. This means there are risks at source and risks inherited from the producers of data which cannot be managed at BIPAD portal. Some of these identified risks are-

Data Ethics Risk

- Data partners/data producers may not be following the ethical standards while generating data. Issues of data accountability, data gaps, data inaccuracy, and data precision may not have been systematically analyzed.
- At present there exists no legally binding mechanism or agreement such as a Memorandum of Understanding (MoU) with data providers on data use, access and sharing mechanisms.

Data Protection Risk Potential compromise on data security at the backend which possesses personal data transferred from Nepal police.

Scope of Processing: The nature of data in BIPAD portal ranges from loss and damage data, spatial data, population statistics, satellite imageries, data on hazards, vulnerability and risks in the form of maps and tables. These data can be periodically renewed on an ad-hoc basis depending on the availability of latest information.

BIPAD Module	Available data/features
Dashboard	The dashboard module gives the alerts of flood warnings, heavy rain alert, earthquake alert and pollution alert. Alerts in the dashboard are generated when the real-time data for earthquake, river watch, rain watch, air pollution cross the respective threshold limits set. **Data sources:** Flood and heavy rain alert: Department of Department of Hydrology and Meteorology (http://hydrology.gov.np/), Earthquake alerts: Department of Mines and Geology (http://seismonepal.gov.np/home) Pollution alerts: Department of Environment (http://pollution.gov.np/).
Incident	This module displays the geospatial information of the hazard incidents reported by Nepal Police. BIPAD portal has datasets of various reported incidents dated from 2011. This module helps visualize the occurrence of a hazard and its severity. The data on the loss and damage caused by incidents (death, injury, missing, livestock destroyed, infrastructures destroyed, economic loss) is available in the tool tip, which is enabled when clicking on the incidents displayed on the map. It also provides information on resources such as health facilities and financial institutes near the location of the incident.
Damage and Loss	This module provides historical data on the losses and damages. BIPAD portal has datasets of various reported incidents dated from 2011. The data on death, injury, missing, livestock destroyed, infrastructures destroyed, economic loss are visualized through choropleth map.
Real Time	This module provides real time data on rainfall and river watch, earthquake, air pollution, and forest fires along with stream flow forecast. **Data sources:** Rain and river watch: Department of Department of Hydrology and Meteorology (http://hydrology.gov.np/), Earthquake: Department of Mines and Geology (http://seismonepal.gov.np/home) and Pollution: Department of Environment (http://pollution.gov.np/). Stream flow: ICIMOD

Risk Info	The Risk Info module consists of datasets that help understand risk and the associated components of risk. This module is divided into 6 sections; **Hazard:** It consists of various hazard maps such as Flood hazard maps from METEOR and Department of Water Resources and Irrigation, Flood inundation map of 2017 and 2019 taken from World Food Programme, Seismic hazard map, landslide susceptibility and hazard maps from METEOR, Earthquake triggered landslides, and Landslide hazard map from Durham University. **Exposure:** Exposure dimension provides exposure datasets such as building footprints, infrastructures through the visualization of OpenStreetMap data. **Vulnerability:** Visualization of various vulnerability indices such as the Human Poverty Index, Human Development Index, Per capita income, Life expectancy sourced from National Planning Commission (NPC), Remoteness indices from Government of Nepal, USAID / Nepal, SEDAC at Columbia University, datasets on access to education, households with access to water, communication, and toilet sourced from Central Bureau of Statistics (CBS). **Risk:** It consists of risk maps of earthquake and landslide obtained from Durham University. **Capacity and Resources:** Capacity and resources data such as educational institutions, health, government institutions, tourism, cultural sites, industries, and communication. The datasets are in the process of being collected and verified by the respective municipal government. **Climate Change:** This section provides data presented here are a part of Climate Change Scenarios for Nepal report which provides medium-term and long-term climate change scenarios for Nepal, which are modelled representations of an evolving climate. Climate change scenarios (temperature and precipitation data) of Nepal with reference period (1981 - 2010), mid-term (2010 - 2045), long term (2036 - 2065) future scenarios based on RCP 4.5 and RCP 8.5
Profile	Profile module contains the overall disaster profile of the various region in terms of the disaster incidents, damage and loss, project mapping, and monitoring of projects and activities based on national and international mandates and commitments. The objective of this module is to abstract key information related to disasters with minimalistic visualizations. This module is divided into 4 sections; **Summary** gives an overview of resources available, loss information, and demographic profile. **Projects** give information on ongoing projects in the DRRM. **Contacts** contain and allow to manage the records of all the committee and non-committee members related to disaster risk reduction and management. **Document page** is a repository for disaster-related documents such as Acts, guidelines, laws, regulations, and alike.

- **Data Protection Risk:** Some of the data related to the vulnerability component contains information often disaggregated to local levels and are linked to an individual or a group of individuals such as poverty, access to health and education, human development index. etc.

Context of Processing: The primary aim of BIPAD is to harness the use of data and evidence to inform policy related to disaster risk reduction and management. The Disaster Information Management System is a sustainable arrangement within an institution for the systematic collection, documentation and analysis of data about hazard, vulnerabilities, exposure and risk and the associated loss caused by disaster events.

- **Data Ethics Risk:** There is a high dependency on data providers.

Purpose of Processing: The purpose of data processing in BIPAD is to analyze the disaster trends and their impacts in a systematic manner for better visualization. With increased understanding of the disaster trends and their impacts, better prevention, mitigation and preparedness measures can be planned to reduce the impact of disasters on the communities.

- **Potential Data Ethics Risk:** Outdated, inaccurate, biased and incomprehensive data may lead to an ill-informed decision-making process.

03

CONSULTATION PROCESS

This section explains the need and modality of consultation with relevant stakeholders/ data partners and information security experts.

Stakeholder consultation process is one of the key steps in DPIA. For the purpose of this initial research no consultation was carried out with data partners or the data security experts. However, to better understand the data ecosystem, and to operationalize the mitigation measures recommended in this report, wider consultation with governments departments, data providers, and data security experts is needed and thus, recommended by this research.

04

ASSESS NECESSITY AND PROPORTIONALITY

This section explains the lawful basis for processing and if there is another way to achieve the same outcome. This section explains the measures to ensure data quality.

The personal data on BIPAD portal is to be rightly placed in accordance with Nepal's legal provisions, as stated in The Privacy Act, 2018.

Nepal Police is the authorized body for incident data collection. BIPAD portal is owned by NDRRMA, which is also a government entity working for disaster management and thus, has the authority to store personal data. However, it is important for BIPAD portal to ensure security of such data at the backend and restrict unauthorized access. Security of personal data can be achieved through pseudonymisation and encryption, which means personal information are securely hidden at backend of the system and during data transfers to the third party. Similarly, to avoid function creep, it becomes important to ensure clarity on the access privileges to assign, change or revoke backend data. Such mechanisms safeguard the rights of people, and thus, recommended by this research.

For data quality, it becomes important to set up quality assessment procedures and ethical procedures with data partners before embedding any of their data, which is discussed more broadly in recommendation section.

05

IDENTIFY AND ASSESS RISKS

To assess the level of risk, this section on DPIA considers both the likelihood and the severity of any impact on individuals.

BIPAD portal data from each module is assessed as per DPIA template whether the specific data has any likelihood of harm to the rights and freedom of people. And, if there is any such likelihood of harm, whether the data has the potential for minimal, significant or severe harm. The risk is qualitatively assessed, and likelihood expressed in three ways - remote, possible and probable. Then, the overall risk for the module is qualitatively assessed as low, medium or high.

In the current version of BIPAD portal, the incident module stores some personal data at backend, which if leaked could create harm to the affected population. The problem is not the storage of personal data, as NDRRMA being the government entity has the authority to do so but here, the data protection issue is related to security of those data. The BIPAD portal backend needs to be fully secured against unauthorized access. Other modules do not have personal data, and thus there is very little to low risk in other modules.

Risk Identification and Assessment			
Describe source of risk and nature of potential impact on individuals.	**Likelihood of harm (remote, possible or probable)**	**Severity of harm (minimal, significant, severe)**	**Overall risk (low, medium, high)**
1. Incident reports (also covers damage and loss module, relief section) collected by Nepal police is linked to BIPAD portal. This incident data includes personal information of the affected population. *The risks are mostly secondary risks transferred from Nepal Police data collection/transfer procedures.* *These data protection risks are related to security breach at the backend of BIPAD portal system and data ethical risks relate mostly to quality, such as inaccuracy, data gaps, data delay and lack of guiding data principles and standards in the existing Nepal government data collection procedures.*	Possible	Minimal	Medium

2. Real Time data linked to government departments and ministries. *The data risks are mostly secondary risks transferred from these institutions to BIPAD portal. These secondary ethical risks are only related to data gaps, inconsistency, and have no risks of harm to individuals*	Remote	Minimal	Low
3. The Profile module contains documents, contacts, and information related to projects and summary. *The secondary risks are related to ethical issues to data quality and accountability but have no risks of harm.* *The personal Information (including position, email address, phone number, photo) of contact personnel are shown in Profile module. The Privacy Act, 2018 allows sharing of contact information of public officials without consent)*	Remote	Minimal	Low
4. The Risk Info module has no personalized data but indication of disaster risks through sub sections on hazard, exposure, vulnerability, climate change and risk. *These data are acquired through national and international research institutions. The secondary ethical risks relate to quality issues, such as accuracy, data update and others.* *However, depending on the use cases, data related to vulnerability such as poverty, access to health and education facilities could be sensitive in nature and relate to data protection issues.*	Possible	Minimal	Low

06

IDENTIFY MEASURES TO MITIGATE RISK

Existing Data Protection Issues	Necessary Code of Conduct	Assessment of Risks	Recommended Mitigation measures	Conclusion
1. Data limitation and Retention 1. Is all the personal data transferred from Nepal Police incident reports necessary for BIPAD's modules? 2. Is it necessary to keep all of the personal data for processing? For how long? (The Incident section and relief section has storage of personal data related to the affected population. These data are not quite necessary for BIPAD's processing but anyway transferred from Nepal Police's incident reports. The details related to individuals such as name, address, etc. are not necessary for BIPAD portal but the aggregated figures are.)	Processing of relevant data, data security, data retention	1. The current mechanism is such that BIPAD portal has access to the personal data of the affected person at the backend of the system 2. The storage of additional personal data may create a privacy issue for the beneficiaries/ their families/witnesses/ or others if the system is hacked, or otherwise compromised (unauthorized use/disclosure or security breach) 3. The personal data originally transferred without specifying any retention period and is kept for an unlimited period of time	1. Limiting the retention of personal data to what is necessary to fulfill specific, explicit and legitimate purposes. For example, to calculate/display the number of affected people. After retention time, data could be erased from the system 2. Linking the data retention period to the purpose of the data processing operations. An initial retention period could be extended if it is considered necessary to keep the data to fulfill the purpose for which it was originally collected 3. Techniques such as pseudonymization and encryption can be used at the backend for any sensitive data as soon as BIPAD portal receives them from partners 4. If any raw data (incident data/relief data) is to be shared with a third party organization, BIPAD portal to ensure that no personal information is shared . Techniques such as pseudonymization and encryption can be adopted while sharing and internal mechanism to monitor transfer data	Risk accepted and mitigated
2. Information Quality and Accuracy (Incident, Damage and Loss, Real Time, Risk Info, Profile) What processes are in place for ensuring information quality, i.e., that the information is relevant, reliable, accurate, actionable? Is there a policy or procedure in place so that the data partners will notify about updates, data correction and data deletion?	Processing adequate, relevant and updated data Rectification and deletion	The risks are secondary risks stemming from the primary data collectors For example, 1.Nepal police/Nepal government may not have data collection standards/principles 2. Data creators might update their research over time (especially relevant for Risk Info page). There is no standard mechanism or MoU in place that ensures that data creators inform BIPAD portal for any updates/ correction/deletion of research 3. No mechanism to bind the data partners under ethical standards of data related to accuracy/completeness/ reliability/ accountability and responsibility	1. Assess data quality of partners and create and sign MoU with data partners incorporating • Data is accurate and reliable at their best knowledge • Data creators are accountable and responsible for their data • Data creators will inform BIPAD portal on data updates/ correction and deletion • Permission for processing of data for BIPAD portal • Information on ethical standards maintained while collecting/producing data 2. Support Nepal Government to set principles on data collection procedures/standardization	Risks accepted, mitigated and transferred to some extent, however the risks on quality, accuracy and data collection standards are beyond the scope of BIPAD portal
3. Consent (Relevant for contact section in profile page or any prospective personal data in future) Are individuals explicitly informed about their personal data being displayed in an open data portal and how it may be used other than the specified purpose of BIPAD portal? Are individuals able to appreciate the most likely consequences (including negative)? Are they able to refuse to provide some or all information?	Right to Information	The risks are 1. Individuals having no knowledge that their data is being shared through the portal. 2. Unintended use of contact information that might harm the data subjects	1. Inform the individuals that their data is published in BIPAD portal open data portal for specified purpose only and that they have the right to provide access to some or all contact information 2. BIPAD portal cannot be held liable for any other risks arising from sharing the data 3. The Privacy Act allows sharing of information of public officials (their position, contact details). For others, consent would be necessary	Risk accepted and transferred
4. Appropriate security measures Is there a risk of information being stolen / lost / altered / rendered unavailable / system hacked / organization subject to surveillance? What preventative measures are in place to check the unintended use of data? (It is important to consider that context can turn non-sensitive data into sensitive data. The context in which the data is used (e.g. cultural, geographic, religious, the political circumstances, etc.) may influence the effect of the data analysis on an individual(s) or group(s) of individuals, even if the data is not explicitly personal or sensitive)	Security, data breaches, responsibility and accountability Unintended use of data	The risks are 1. Distortion of backend data by external data hackers and users. 2. No mechanism to track the users and the purpose of data downloading	1. Ensure clarity – who has the authority to assign, change or revoke access privileges to backend data. YI-lab is in the process of creating and finalizing this formal document. 2. Develop robust access control protocols which limit access on a 'need to know' basis. Users should only have access to that portion of data they need to carry out their legitimate functions. 3. Set-up data breach notification procedures to inform the authorized data subjects 4. Make provision for login with email address for downloading data to keep track of users. (The user info processing to be based on lawful processing. This is done not to restrict the use of data but to have more information of user and use cases)	Risk mitigated

4. RECOMMENDATIONS

4.1 Protection and Ethical Considerations with Data Partners

As most of the data risks are transferred from data partners, it is prudent for BIPAD portal to engage in ethical considerations with all data partners. This includes conducting ethical assessment based on the indicators discussed in section 1.1 before making any partnership with collaborators.

It will be helpful for BIPAD portal to set up legally binding documents, such as Memorandum of Understanding (MoU) with data partners outlining parameters for data access and handling (e.g. data security, data formats, data transmission, fusion, analysis, validation, storage, retention, re-use, licensing, etc.) to ensure reliable and secure access to data. It will be important to clearly mention the relevant data sources, associated metadata and guidance to use the data/portal. (YI-lab, when collaborating with new partner)

The recommendation is to perform due diligence when selecting data or service provider and ensure their activities comply with the National Privacy Act. BIPAD portal has to keep it in line with the latest legal requirements.

When ministries and departments begin sharing data, policy and legal questions often arise. Some of these issues center on access, privacy, and standards. BIPAD team will need to consider several questions when using any new data source, such as-

Access: Who can view the data? Do some data need to be kept private for security reasons?

Privacy: What the data alone or as a mosaic reveals about others? Does the data reveal information about citizens that needs to be kept private? How can the data be released for DRM purposes in ways that protect citizen privacy?

Standards: What is the national standard for certain data types? Do ministries use formats that are compatible with each other? What is the cost of translating data from one format to another as it now moves from ministry to ministry and outside partners? If there are problems with standards and data translation, what is the standard that BIPAD portal will follow?

Metadata: How can users find the data they need? Metadata provides a common language to describe the data. In this way, experts in various specialties can define their vocabularies and enable others to find the data that they need.

To the extent reasonably possible, data should be validated for accuracy, relevancy, sufficiency, integrity, completeness, usability, validity and coherence, and be kept up to date. This allows sufficient mitigation of data risks and also, legally retains the risks on the partners as BIPAD portal is not in essence liable for their data. This will also allow the data partners to reevaluate and reflect on their data collection, processing and sharing mechanism.

BOX 2 RECOMMENDATIONS

This study recommends the following actions to be taken by YI-lab by 2021 in consultation with NDRRMA:

1. Mechanism in place to assess data quality of partners and ethical standards.
2. Set up legally binding Memorandum of Understanding (MoU) with data partners.
3. All data activities in line with the Privacy Act, 2018 and adapt to changes in legal provisions.
4. BIPAD portal to set up log in feature for downloading data.
5. Add disclaimer in the portal that clearly states that BIPAD portal is not liable for any potential negative outcomes resulting from use and processing of BIPAD portal data.
6. Ensure organizational safeguards are in place to prevent unauthorized access of backend data.
7. Support Nepal Police in standardization of incident reporting platform.
8. If any personal data is acquired, assign retention period to the data and set up mechanism for encryption and pseudonymization.
9. Carry out stakeholder consultation and internal data security audit before fully handing the system to NDRRMA.

4.2 User Information and Consent

BIPAD portal advocates for Open data and thus, cannot truly prohibit the unintended use of disaster data. However, it is possible to monitor the use of data in BIPAD portal by collecting the user details on those who wish to download the data from the system. Information such as the name of the person, organizations, email address and purpose of using the data can be captured. Appropriate consent would be necessary to acquire any such data. Such personal data should be stored safely and not to be shared publicly.

It is also helpful to add a disclaimer in the portal stating clearly that BIPAD portal is not liable for any potential negative outcomes resulting from the use and processing of BIPAD portal data.

Similarly, appropriate consent must be obtained from the data subjects, if in future BIPAD portal intends to process personal data. Such personal data should not be shared publicly.

4.3 Data Security

BIPAD portal has to ensure that reasonable and appropriate technical and organizational safeguards are in place to prevent any unauthorized disclosure or breach of backend data where personal data is accessible. It will be important to set up a mechanism that data is being stored only for the necessary duration and any retention of it is justified.

Security measures include clarity on the authority to assign, change or revoke access privileges to backend data and setting up data breach notification procedures to inform the authorized person. Backend users should only have access to that portion of data that they need to carry out their legitimate functions. Other security measures include pseudonymization and encryption whenever personal data are received from data partners so that those data are secure at the backend of BIPAD portal system.

An internal data security audit is also fruitful before fully handing over the system to NDRRMA.

Government of Nepal