EdTech Hub

Clear evidence, better decisions, more learning.

HELPDESK RESPONSE 44

Data Access and Protection Laws in Pakistan

A technical review

Date July 2022

Authors Waqas Halim
Arjun Upadhyay
Caitlin Coflan

DOI 10.53832/edtechhub.0098

UKaid from the British people

THE WORLD BANK

unicef for every child

About this document

Recommended citation

Halim, W., Upadhyay, A., & Coflan, C. (2022). *Data Access and Protection Laws in Pakistan: A technical review* (Helpdesk Response No. 118). EdTech Hub. https://doi.org/10.53832/edtechhub.0098
Available at https://docs.edtechhub.org/lib/GV4MKFZH.
Available under Creative Commons Attribution 4.0 International, https://creativecommons.org/licenses/by/4.0/.

Notes

EdTech Hub is supported by UK aid (Foreign, Commonwealth and Development Office), Bill & Melinda Gates Foundation, World Bank, and UNICEF. The views expressed in this document do not necessarily reflect the views of UK aid (Foreign, Commonwealth and Development Office), Bill & Melinda Gates Foundation, World Bank, and UNICEF.

Reviewers

Tom Kaye, Imdad Baloch, Björn Haßler

About the EdTech Hub Helpdesk

The Helpdesk is the Hub's rapid response service, available to FCDO advisers and World Bank staff in 70 low- and lower-middle-income countries (LMICs). It delivers just-in-time services to support education technology planning and decision-making. We respond to most requests in 1–15 business days. Given the rapid nature of requests, we aim to produce comprehensive and evidence-based quality outputs, while acknowledging that our work is by no means exhaustive. For more information, please visit https://edtechhub.org/helpdesk/.

Contents

Figures

Tables

Abbreviations and acronyms

AEPAM	Academy for Educational Planning and Management
API	Application Programming Interface
DPA	Data Protection Authority
DPO	Data Protection Officer
EMIS	Education Management Information System
FCDO	Foreign, Commonwealth and Development Office
GDPR	General Data Protection Regulation
ID4D	Identification for Development Initiative
IT	Information technology
KP	Khyber Pakhtunkhwa
KREMA	Khyber Pakhtunkhwa Education Monitoring Authority
LMIC	Low- and middle-income country
MEITY	Ministry of Electronics and Information Technology
NCPDP	National Commission for Personal Data Protection
NEAS	National Educational Assessment System
NEMIS	National Education Management Information System
PIE	Pakistan Institute for Education
PITB	Punjab Information Technology Board
PMIU	Programme Monitoring and Implementation Unit
RTI	Right to Information
SABER	Systems Approach for Better Education Results
UNOCHA	United Nations Office for the Coordination of Humanitarian Affairs

1. Introduction

The advancement of technologies has supported an exponential rise in the collection and use of data. Data, when used appropriately, can support better decision-making and inform innovation (↑OECD, no date). Data has value to entrepreneurs and innovators who seek to design products that respond to user needs. However, the widespread collection and use of data have also spawned concerns about individual rights and data privacy (↑World Economic Forum, 2021). Issues related to collection, usage, dissemination, and access to data have also come to the forefront. To address these concerns, many countries across the globe have introduced data protection laws (↑UNCTAD, 2022). However, policymakers across the world face serious challenges in striking a delicate balance between regulating data privacy and enabling innovation.

In the education sector, stakeholders require timely and accurate information to make informed decisions (↑Human Rights Watch, 2022). Emerging evidence suggests that EdTech has a key role to play in the expansion of data systems in low- and middle-income countries (LMICs). But as with data in general, the education sector faces challenges of data availability, usability and uptake, and minimising potential harm that can come from misuse, abuse, or inadequate data protection (↑Hennessy et al., 2021). Likewise, the benefits of the usage of data in policymaking are well documented. Particularly in the education sector, where data access offers several growth and productivity advantages (↑Gruen et al., 2014). One common policy framework, which addresses both access and protection issues in the education domain, is the set of ↑Principles for Digital Development (no date). The Principles are based on nine guidelines and offer guidance on a user-based focus, open data, relevance to the context, collaboration, scalability and sustainability, reusability, protection, and coordination at different stages of a digital project focused on development goals, including education.

This policy brief identifies and analyses global best practices in data protection and data access. It is developed in response to an inquiry related to data and research in the education sector, specifically in Pakistan. The brief explores the potential practical challenges in the enforcement and implementation of global good practices in the context of the data protection environment in Pakistan; it proposes a set of key recommendations for the Government of Pakistan, provincial

governments, development partners, and other education-related ministries and public departments.

1.1 Purpose of this brief

This brief summarises international good practices for establishing and implementing:

- **data access protocols**, to ensure that the appropriate people have the appropriate access to data for decision-making when they need it;
- **data protection laws**, including child protection and the collection of sensitive data.

For this brief, we focus our analysis on data access and protection. It is important to note, however, that there are other stages in the data management lifecycle that we do not cover explicitly, such as data collection, storage, and analysis (↑World Bank, 2021). The brief is intended for various stakeholders in the education sector — particularly policymakers in Government agencies in Pakistan.

It is important to mention that access and protection are not the only aspects of a data lifecycle, and several different stages of an education data lifecycle include data collection, usage, storage, transfer and destruction, besides access and protection (↑Romadhoni, 2020). While the focus of this brief is on data access and protection, it touches on few other stages of the data lifecycle. However, it does not specifically cover other stages, which can be future pathways for further research.

1.2 Methodology

The main research methods for this brief include desk research, case studies, and expert interviews. Desk research included a review of select countries' data protection and privacy legislation, published white and grey literature, and documents from international organisations, as well as those from governments and other key stakeholders.

The authors also conducted three semi-structured interviews with key informants working on data protection and privacy. The key informants included:

1. A representative from Social and Policy Sciences, a research centre in Pakistan specialising in education technology data;

2. Global experts on data protection from the World Bank Group and EdTech Hub's Specialist Network, to identify country cases and success stories.

Case studies were developed to highlight good practices from countries with similar governance structures to Pakistan. The report draws on Malaysia and India's experiences for recommendations on data protection, and on the examples of Sierra Leone and India for data access. Countries were selected with the intention of drawing out lessons that are applicable to Pakistan. These countries have some similarities to Pakistan in terms of socio-economic development and colonial legacy, as well as challenges they face in their executive and legal systems. Sierra Leone is an example of an effective education-related data sharing mechanism with policymakers, and India is one of the first countries to introduce a data access(ibility) policy and has a similar socio-political and legal background to Pakistan. Likewise, Malaysia is considered to be a highly robust data protection regime, and India is one of the low- and middle-income countries that has a similar federal system to Pakistan, offering useful insights for Pakistan.

Our analysis is largely informed by the literature available on data protection and data access in general, without any focus on a specific sector. However, where possible we have highlighted and mentioned education-related data protection good practices, guidelines and policies, which are implemented in different parts of the world in the brief. To make our analysis and recommendations relevant to Pakistan, we have tried to find references from countries with similar structures, history and development trajectories, and for those countries, it is even difficult to find any literature. Where we identified the limited literature that exists in the context of low- and middle-income countries, we have cited examples of high-income countries to draw lessons.

2. Overview of key definitions

For the purposes of this brief, we define data access as making appropriate data accessible for use by the public, policymakers, and other stakeholders in the education sector. However, data access is a complex subject, and not all stakeholders can have the same level of access. Considering this, the brief addresses data access, sharing, and usage by the public, policymakers, teachers and parents, or third parties like private companies or startups, separately to highlight the nuances that must be taken into consideration. Appropriate data adheres to the principles of data integrity, including protocols related to open data and special measures for the protection of sensitive information related to children and marginalised groups, which are discussed further in detail. However, elements of data quality, including reliability and verification, fall outside the scope of this brief.

Data protection refers to the "systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy regarding the collection, storage, use, disclosure and any other type of processing of personal data" (↑European Commission, 2015).

3. Context for data protection and data use

This section includes an overview of the global landscape on data protection and access and contextualises the current position of Pakistan. We also examine progress and challenges in this area in detail.

3.1. Landscape of data protection and data access regulations across the world

Although there is growing acknowledgement of the importance of protecting data rights, the robustness of regulatory frameworks related to data protection and access varies considerably across the globe. To address these concerns, 137 out of 194 countries across the globe had some form of data protection legislation in place until December 2021 (↑UNCTAD, 2022). However, our research suggests that only a limited number of countries have robust institutional or legal frameworks and processes for data protection in place (↑DLA Piper, 2022). Different countries introduce different kinds of legislation that suit their political and bureaucratic systems.

Robust data protection regulation is difficult to enforce. The European Union data protection law, formally known as the General Data Protection Regulation (↑GDPR, 2016), is viewed as the gold standard in the protection of information and data. However, while it is considered to be stringent, it is difficult to apply when it comes to data collection and processing by governments and private organisations alike. However, for research purposes, the GDPR extends several privileges to research bodies and allows various exemptions that include sensitive data processing, right to data erasure, and lenient requirement of seeking consent — provided that such bodies have necessary safeguards in place (↑Maldoff, 2016). Malaysia, Egypt, Tunisia, and Algeria are among the few LMICs that have passed robust legislation (↑DLA Piper, 2022). However, there are vast gaps in enforcement and implementation. India has not yet passed a data protection law, although a draft data protection bill has been introduced by the government.

3.2. Data protection and access: Progress and challenges specific to Pakistan

The Personal Data Protection Bill 2022 in Pakistan (↑Ministry of Information Technology and Telecommunication, 2021) marks a significant transition for Pakistan in granting rights to data subjects and setting up legal and accountability mechanisms for any breach of privacy and security. The Personal Data Protection Bill was recently approved by the Federal Cabinet on 28 February 2022. As a next step, it will be debated in Parliament (↑OneTrust DataGuidance, 2022). The Personal Data Protection Bill builds on the Prevention of Electronic Crimes Act 2016 (↑Ministry of Information Technology, 2016), which instituted a regulatory framework for data breaches but did not have provisions for privacy rights, which are guaranteed as a fundamental right in the Constitution of Pakistan.

The Personal Data Protection Bill has its own merits and shortcomings. Some analysts suggest that the bill is made up of a patchwork of similar legislation drawn from across the globe. Most notably, the bill has features of India's 2019 Data Protection Bill (↑Government of India, 2019), Malaysia's 2010 Data Protection Law (↑Parliament of Malaysia, 2010), the UK's 2018 Data Protection law (↑UK Data Protection Act, 2018), and the EU's GDPR legislation(↑GDPR, 2016). Although it borrows extensively from ↑GDPR (2016) and UK Protection Law 2018 (↑UK Data Protection Act, 2018), the Personal Data Protection Bill differs from these in that it prioritises certain privileges for the state over the protection of citizens (↑Shahani, 2020).

The following are some of the salient features of the Pakistan Personal Data Protection Bill, 2022:

1. Establishment of a Supervisory Commission: A commission is mandated to operate as a supervisory authority at a federal level, known as the National Commission for Personal Data Protection (NCPDP).
2. Rights to the Data Subject: The following key rights have been conferred to data subjects:
    - the right to access personal data;
    - the right to correct personal data;
    - the right to withdraw consent;

- the right to prevent processing that is likely to cause damage or distress;
- the right to erasure.[1]

1. Data localisation provisions to ensure that a 'copy of personal data' is retained by all businesses in Pakistan.
2. Roles and obligations of 'data controllers' (entities that determine the purpose of data) and 'data processors' (entities that process the data) are established.
3. Accountability mechanism on misuse of data: the bill provides an accountability mechanism and process to follow in the event of data breaches.
4. Fines and penalties for data breaches are established (↑Ministry of Information Technology and Telecommunication, 2021).

However, there are several limitations to the Personal Data Protection Bill that have been highlighted in analyses by Bolo Bhi, a research-based organisation (↑Bhi, 2020), and MediaMatters for Democracy, a policy research initiative (↑Kalyar, 2021). They include the following:

1. *Unclear definitions*: The bill offers no efforts to define a key term of what is considered a 'data subject' when requests for data access are made. Likewise, definitions of the terms 'state' and 'authorities' are unclear, which makes it difficult to understand if the law will be applicable to government authorities. The lack of clarity of the terms used in the bill, in particular, the terms 'critical personal data' and 'some sensitive data', also make planning difficult for businesses (↑Ali, 2021).
2. *Extensive discretionary powers and vague penalties*: Substantial discretionary powers afforded to the state limit the scope of the bill. The bill allows departments of state governments wide-ranging exemptions from the accountability measures set out in the bill (↑Bhi, 2020).
3. *Lack of autonomous oversight and clear accountability*: Similar to the Indian Personal Data Protection Bill, the Personal Data Protection Bill in Pakistan also allows the federal government to

[1] 'Erasure' refers to ideas that are also known as the 'right to be forgotten'.

intervene in the annual report of the supervisory authority, the appointment of commission members, and other similar key decisions. The federal government is given the power to appoint a member in the committee, control the funds, as well as hire employees and determine their salaries (↑Kalyar, 2021).

4. *Lack of coverage of non-personal data*: In its current form, the bill only focuses on the processing of personal data and does not cover non-personal data, which is data that does not contain personally identifiable information.

3.3. Challenges of education data collection, storage, processing, and dissemination in Pakistan

During the in-depth interviews, the key informants provided an overview of problems related to demand and access to data in the education sector of Pakistan. Based on the insights, the following challenges were identified for data collection, access, and protection across Pakistan:

1. **Lack of coordination among data collection agencies**

   Multiple agencies at the provincial level are tasked with data collection on a number of indicators for education. According to a key informant, at one time, there were 16 different education-related datasets that were collected without centralisation or coordination. Examples of the agencies that collect education data at the provincial level include the Programme Monitoring and Implementation Unit (PMIU) in Punjab and the Khyber Pakhtunkhwa Education Monitoring Authority (Independent Monitoring Unit).

2. **Minimal safeguards in place for marginalised groups**

   In Pakistan, a wide range of data is collected from refugees, persons with disabilities, internally displaced people, individuals who identify as transgender, and minorities. The main reasons for collecting this data typically relate to planning, such as identifying which students will and will not get Nazra[2] textbooks and identifying teachers who can teach Nazra to Muslim students. However, in the absence of any

[2] Nazra refers to Quran recitation courses offered to Muslim students (↑Punjab Curriculum & Textbook Board, 2021).

specific protocols targeted at safeguarding data for marginalised groups, the collection of this data can leave non-Muslims and other groups vulnerable to malicious intent. Data on these already vulnerable groups could be subject to misuse or abuse.

3. **Weak formal systems and mechanisms for data sharing**

   Historically, in Pakistan, the Academy for Educational Planning and Management (AEPAM) has been the federal body in charge of collecting and collating education data. However, AEPAM lacked a clear legal mandate to collect data from the provinces. The academy worked with provincial-level agencies that manage Education Management Information Systems (EMISs) through the coordination committee, resulting in the creation of a National Education Management Information System (NEMIS). The NEMIS outlines data standards for provinces to gather and integrate data on education. Another important collector of education data, the National Educational Assessment System (NEAS), only covers public school data and does not gather data on private schools. In March 2022, AEPAM and NEAS were merged into a new organisation known as Pakistan Institute for Education. How the institute consolidates and shares education data going forward remains to be seen.

   In addition to the coordination challenges within government and across levels, Pakistan also lacks formal mechanisms for sharing data with third parties such as EdTech business and data analytics companies. Civil society organisations are, however, able to apply for the Right to Information Act (RTI) provision in order to access data. One provincial-level example of the RTI is ↑The Punjab Transparency and Right to Information Act (2013).

4. **Limited use of data by policymakers for insights and decisions**

   Education policymakers and administrators in Pakistan generally use data on a limited scale for insights and decision-making for policymaking, planning, allocation of resources, and procurement.

3.3.1. Examples of security measures introduced by different departments

Key informants also identified a few measures that different provincial departments have introduced to protect data.

1. **Sharing summarised information on request under the Right to Information Act**

   One of the measures that are deployed by the education agencies is to share summarised information on request to ensure confidentiality and privacy. For example, the Programme Monitoring and Implementation Unit (PMIU) in Punjab and Independent Monitoring Unit, Khyber Pakhtunkhwa only share summarised information on request under their respective Right to Information Acts.

2. **Restricting access to data by requiring special permission**

   The Punjab RTI further restricts access to data by requiring special permission from the executive-level managers if data is directly requested from the relevant education department. The School Information System in Punjab restricts access to back-end data; even teachers and principals have limited access to data when they enter information for each student in the school.

3. **Encrypting data for security**

   The Punjab Information Technology Board (PITB) encrypts data of all kinds, which provides greater security than data in its raw form. Likewise, Khyber Pakhtunkhwa Information Technology Board uses data encryption to secure data.

The extent to which these measures are rigorously applied requires additional research. One key informant suggested that although education data collection authorities claim to ensure rigorous compliance with the established data security measures, there are issues in practical implementation that leave data management systems vulnerable to potential external attacks and leaks of personal information.

There is significant variation in the robustness of data regimes in place across different provinces in Pakistan. Punjab has historically been advanced in terms of instituting systematic approaches in the education sector and hence has a more sophisticated data regime compared to other provinces.

The following are the main features of data regimes across different provinces:

The education departments in all provinces (Punjab, Khyber Pakhtunkhwa, Sindh, Balochistan) collect and disseminate data on education. The School Education Department Punjab, the Khyber Pakhtunkhwa Education Monitoring Authority (KPEMA) and others used to hold vast repositories of data that were previously stored in spaces at PITB and the Khyber Pakhtunkhwa IT Board respectively. However, through the PMIU, the Punjab School Education Department has recently established a data warehouse to consolidate the processing and storage of data from various sources under its own premises, which ensures improved data security. Personnel, including experts on data security, need to be hired in order to operate the centre effectively. Khyber Pakhtunkhwa also has a data centre. In Sindh and Balochistan, where data collection is typically done manually, there are no data centres.

The PITB has an elaborate privacy policy and claims to follow it in practice, however, it is less clear what privacy policies, if any, are in place in other provincial IT government bodies.

Punjab has a well-functioning open data portal, known as ↑Punjab School Monitoring (no date). While the Khyber Pakhtunkhwa School Education Department does not have an open data portal, the Independent Monitoring Unit does release aggregated education statistics on its website. Likewise, all four provinces (including KyberPakhtunkhwa, Sindh, and Balochistan) operate EMIS systems with varying levels of expertise. Punjab has a well-structured EMIS, which is linked to open data. However, only selected indicators are shared on the open data portal. In Punjab, education data includes sensitive personal information such as addresses, phone numbers, and information on the identities of parents, teachers, and children. Thus, effective data protection measures are required to strengthen the security of the EMIS back end, and the front end, which is shared on an open data platform. Both Sindh and Balochistan have functioning EMISs. Furthermore, open data systems for education exist in Punjab (through PMIU) and Khyber Pakhtunkhwa through the Education Monitoring Authority but they do not exist in Balochistan and Sindh.

According to one key informant, apart from the basic education-related indicators, there is not much duplication of information collected, and by and large, the data collection functions are divided between different education-related agencies within each province.

4. Data access protocols and policies: Good practices

Data access refers to making appropriate data available for public and government use. Putting in place appropriate protocols for data access is important for improving accountability and service delivery. In the education sector, data access protocols can help enable the establishment of administrative roles, data ownership procedures, and other security protocols. Data access is also very important for public participation, sound governance, and the improvement of service delivery through civil society evaluation (Lateral Economics, 2014). One of two examples of data access protocols is the Data Accessibility and Use Act in India, a federal government policy that aims to consolidate data access and data sharing efforts in the country (↑Ministry of Electronics and Information Technology, 2022). The second example is the Data Availability and Transparency Bill 2022 in Australia (↑Markham, 2020), which provides a legal framework for certain data authorisations and principles.

Through a rigorous analysis of data protection practices around the world, interviews with key informants, and focusing on the main challenges regarding data access, we identified three key effective practices for data access protocols and policies that include:

1. Establishing specific protocols for access to children's data and data from marginalised and disadvantaged groups.
2. Facilitating open data for accountability and transparency, with protocols specifying acceptable uses of such data, and setting up interoperable education data systems.
3. Defining mechanisms for data sharing across government, with teachers and administrators, and with third parties.

This review identifies three major good practices for responsible data access based on lessons from across countries and regions including Australia, the EU, India, Punjab province in Pakistan, the UK, and the US.

4.1. Good practice #1: Establish protocols for access to sensitive data

The first good practice relates to sensitive data of children and marginalised and disadvantaged groups as these groups are more vulnerable to manipulation and discrimination. Government departments must ensure the privacy of these groups and implement security measures, which we highlight below in light of examples of effective mechanisms in other countries.

4.1.1. Establish protocols and rules for consent for collection and access to children's data

Policymakers, government officials, parents and teachers can use data to track the academic performance of children. Data can also be used to track children in the event of transfers between schools or even migration to different parts of the country. Personal identity data (gender, age, religion, language, etc.) can inform policies required to improve education access and quality for groups that have been marginalised. However, there are serious risks of misuse of such data. Location and health data can be used in ways that could cause severe damage to a child's mental and physical life.

In this regard, the GDPR has established the same rights for children as for adults regarding the processing of their personal data. For children below the age of 16, parents or caregivers need to provide consent on their children's behalf. GDPR places additional safeguards on children's personal data since children are underage and less aware of the potential risks and consequences of sharing data. In cases where children can give consent, the language of policies must be easily understandable for children. Moreover, children must be educated on the risks involved and their rights through different engagement programmes. Schools should create awareness about data security risks and protection mechanisms, such as stronger passwords and sharing devices, among others (↑GDPR, 2016). Kenyan data protection law prohibits the collection of data without parental consent and data protection law in Ghana categorises children's data as sensitive (↑UNICEF, 2021).

When it comes to data collection, the US Department of Education has specific guidelines in Standards for Education Data Collection and Reporting (↑SEDCR, 1991) for collecting data through a rigorous process in

education settings. The Standards highlight the need for building data collection infrastructure and planning, identifying data purpose and value, developing data processing systems, and creating robust management processes, among others, to address issues of management, accuracy, confidentiality, quality, and capacity building.

4.1.2. Foster an enabling environment for protecting children's data

Multiple global frameworks outline policy recommendations for enabling a safer environment for children online and ensuring data protection in cyberspace. In "The Case for Better Governance of Children's Data: A Manifesto", ↑UNICEF (2021) introduces key action items for data protection. These include:

- prioritising children's rights in data collection to take a child-centred data governance approach;
- ensuring no marginalised child is left behind;
- providing protection measures to all children, even below the age of 18;
- minimising the use of profiling and surveillance.

It also recommends governments develop guidelines for children's data protection at national as well as sub-national levels. Other proposed recommendations include:

- developing guidelines for the private sector;
- developing impact assessment instruments for compliance with children's data protection rights;
- thoroughly introducing regulatory frameworks for children's data protection.

Likewise, the organisation Responsible Data for Children has established a set of principles for handling children's data. It emphasises the importance of purpose, participation, prevention of any harm, and the protection of children, among other principles for the protection of children's data to ensure data security (↑RD4C, no date).

Although ↑UNICEF's (2011) 'Child Safety Online — Global Challenges and Strategies' report focuses on the ways governments can inform children

about internet safety and provide assistance in the event of harm. It also identifies policy measures for children's online security. These include recommendations for government departments to ensure a safe online environment. The recommendations include the need to develop policy and regulatory frameworks and IT solutions to take down abusive content immediately and to strengthen legal and reporting mechanisms

4.1.3. Examples of legal frameworks to safeguard children's online data

The UK, USA, European Union, and recently, India, have introduced legal frameworks to safeguard children's online data.

In the UK, the recently proposed Online Safety Bill 2022 has special provisions to protect children's rights in cyberspace. It empowers the media regulator to regulate social media platforms, content producers, search engines, and other digital applications to ensure the protection of children and remove any content that may cause them harm. Some of the punitive measures for non-compliance enshrined in the bill include fines of 10% of companies' global revenue, blocking sites, and forcing sites to improve their mechanisms (↑UK Parliament, 2022).

Likewise, the 2021 Indian Accessibility and Use Policy also emphasises the protection of children's rights and the importance of ensuring that data security measures are in place when processing children's data. It restricts data processors from "profiling, tracking, behaviourally monitoring children's data or targeted advertisements or any processing that may cause harm to children" (↑Khaitan and Co., 2022).

In the US, while different laws have been introduced to ensure children's rights, protection of these rights in digital spaces has not as yet been fully regulated. One existing law is the Children's Online Privacy Protection Act of 1998 (COPPA), which restricts access to any harmful content online by minors under the age of 13 and protects children's privacy online (↑COPPA, 1998).

An example of established data access protocols at the sub-national level is the Australian Data Access Protocol, which operationalises the Information Act in the Children and Education Department for the Northern Territories, 2013. It focuses on public access and protection of personal and sensitive information and establishes protocols for the provision of data in the education sector (↑Department of Education Children Services, 2013). The

protocol emphasises that data will be only used for the purposes for which it was specifically collected, and requires consent from subjects for disclosure to third parties.

4.1.4. Examples of legal frameworks to safeguard data on marginalised and disadvantaged groups

Special attention must be given to protecting the data of marginalised groups because the abuse of data can lead to discrimination, persecution, profiling, and surveillance. In Pakistan, data from transgender schools, people with special needs, religious and other minority groups, and even data on female children, can be considered sensitive. According to one key informant, the Khyber Pakhtunkhwa government collects and records data on Afghan refugee children and internally displaced people. Although collecting this data can be seen as a positive step in terms of the inclusion of marginalised groups in the educational system, there are no known safeguards in place to secure the data or the rights of the children from whom it is collected.

Research indicates that the following principles are crucial when establishing data access protocols to protect marginalised groups:

1. **Principles of non-exclusion and non-discrimination**

   A country's identification card (ID) ecosystem must not leave out any ethnic, gender, religious, or other kinds of minority groups and must not discriminate against them. This principle is practised in India for the legal inclusion of minority groups such as unskilled workers, the disabled, women, older people, tribal people, and others, to avoid any discrimination against them (↑World Bank, 2019).

2. **Principle of retention**

   Under Malaysia's 2010 Data Protection Law, data should not be kept or stored after the purpose for which it was originally collected has been fulfilled (↑Parliament of Malaysia, 2010). This principle ensures the deletion of data after its intended use has been met. Malaysia's 2015 Personal Data Protection Standard mandates the development of a schedule for the disposal of any inactive personal data within 24 months (↑Ping, 2021).

3. **Data security measures**

   Data security measures ensure the protection of files and data through different controls, protocols, and restrictions of access to information through techniques including encryption, anonymisation, and setting up firewalls, among others. Governments should ensure that data of marginalised groups is anonymised and encrypted, adhering to effective practices for data security described elsewhere in this brief. For more details, please refer to Section 5.3.

4. **Improving training and awareness**

   One key informant suggested that awareness and training sessions focused on data protection laws and access protocols in the education sector should be conducted to enable a proper regime of data protection for children and marginalised groups.

One fundamental principle laid out in the guidelines of the Principles for Digital Development[3] is the focus on the user. It is essential to consider children, the disabled, or those affected by conflict, etc., and ensure that traditionally disadvantaged communities are included in databases and also considered in the design and implementation of child-related projects.

4.2. Good practice #2: Facilitate open and public access data protocols

4.2.1. Open data can facilitate accountability, transparency, and productivity

Open data is data that is "freely available, used, re-used and redistributed" by anyone, without requiring any kind of licence (↑Open Data Handbook, 2022). Global evidence suggests that open data leads to improved accountability and transparency. The World Bank's 2019 working paper notes examples of the importance of open data in education, including a strong association of open data with increased stakeholder involvement in monitoring, resulting in improved education (↑Jelenic, 2019; ↑Barr et al., 2012). It also includes examples of the dissemination of school budget information, which led to enhanced teaching efforts and a reduction in absenteeism (↑Pandey et al., 2008). Furthermore, open data can bolster business prosperity and enable productivity gains through providing

[3] See: https://digitalprinciples.org/

better data on reducing costs, offering new services, and improving quality (Lateral Economics, 2014). Facilitating access to open education data requires governments to establish well-functioning EMISs. We discuss this further below. Open data does not necessarily mean access to all information. Open data should be guided by robust data sharing principles such as removing or minimising the sharing of personal information. This nuance is discussed further in Section 4.3.

A 2018 UNESCO case study on Punjab's Programme Monitoring and Implementation Unit (PMIU) offers lessons on using open school data to improve transparency and accountability (↑Khan, 2018). Based on surveys of and interviews with teachers and principals, the case study highlights how PMIU provided teachers and principals convenient access to data, who then used it to track the performance of their schools. It also underscores that open data enabled civil servants to make better decisions and helped to restructure the chain of accountability by making data collection efficient in the short term. The case study notes that the system still requires improvement to address wide gaps in the consumption and communication of data by and to the right stakeholders, including parents and civil society.

Box 1. *Background on the PMIU.*

The PMIU collects school-level data to ensure the continued involvement of district offices, school leaders, and teachers in Punjab. It reports on student learning outcomes at the school level to assess the performance of teachers and schools overall. The PMIU database then translates into an open data platform, which provides statistics to the district, *tehsil* (sub-district), and schools (↑Open Data Punjab, 2022). According to one key informant, the PMIU used to report data on learning outcomes, but recently this practice has been disrupted due to political interference.

To facilitate the process of open data, several countries have enforced and implemented legislation on access to information (↑UNESCO, 2019). Such legislation provides context and precedent for the development of contemporary data laws. However, Pakistan's Right to Information Act is only applicable to public interest information and only summary information is provided. Further regulation of private sector uses of more detailed data needs to be developed.

4.2.2. A robust EMIS can facilitate open data access

One important aspect of facilitating access to open data is the development of EMISs, as they typically hold back-end data. An effective EMIS requires strong coordination between the different departments of state and central governments. The World Bank's Systems Approach for Better Education Results (SABER) report identifies four key areas for effective EMIS development and implementation: a robust ecosystem, system soundness, data validity, and usage of data for insights and meaningful decision-making (↑Abdul-Hamid, 2014). Among low- and middle-income countries, Malaysia is an example of a country with a well-established EMIS that integrates and consolidates multiple government sources of data, enabling the tracking of individual children through the system (↑UNICEF, 2020).

One key informant identified two factors as major enablers for a successful implementation of an EMIS system: interoperability and identification. Interoperability refers to the ability of two or more IT systems to mutually exchange and interact to attain certain outcomes (↑Adam et al., 2021). Ideally, various government IT systems must be interoperable at the back end and provide a single entry point for the public at the front end through one-stop portals. The transition towards interoperable digital data architecture requires open data and standardisation (↑World Bank, 2019).

At the federal level, the Pakistan Institute of Education (PIE)[4] is responsible for coordinating and collating datasets from all provinces. Historically, AEPAM has published this data in the Pakistan Education Statistics Report and the National Education Management Information System (NEMIS) — the database that compiles and centralises education data from the provinces. However, NEMIS does not contain updated information and needs data verification through the support of provincial departments. Furthermore, EMIS 2.0 is still being developed in Pakistan, with the ambition of consolidating and better integrating teacher and student data and exam results.

[4] The Pakistan Institute of Education was established through a cabinet decision in 2022 through the merger of AEPAM and NEAS (see Section 3.3). However, its structuring will take some time to properly establish its systems. The Data and Research in Education programme is supporting the institute to strengthen its structure and functions.

Box 2. *How a functioning EMIS unlocks open data sharing.*

The Education Department in the US state of Massachusetts can be considered a benchmark when it comes to providing opportunities for data access to the public and disseminating information. The Massachusetts Department of Elementary and Secondary Education aggregates data on different education indicators at state, district, and school levels (↑Massachusetts Department of Elementary and Secondary Education, no date). Most of this data is available freely online. The department prepares reports, which are also available online. In addition, it provides information to improve accountability and work towards improved learning and teaching in public schools in the state. Still further, the department provides detailed information on request to researchers who are affiliated with a recognised organisation.

4.2.3. Licensing for open data reduces uncertainty

An important effective practice is the use of the legal instrument of licensing for open data via the Open Data Commons to access and publish data online. Licensing eliminates the element of uncertainty in the use of open data and provides a legal cover (↑Open Knowledge Foundation, no date). Moreover, the process facilitates the interoperability of different databases and helps to nurture data sharing and integration.

4.2.4. Global open databases and frameworks

There are several open databases which are maintained by different international organisations. One such portal containing the aggregation of various global open databases for education is maintained by the United Nations Office for the Coordination of Humanitarian Affairs (UNOCHA) known as the Humanitarian Data Exchange. The database gathers information from different databases of the United Nations Development Programme (UNDP), UNICEF, and UNESCO under one platform. Additionally, it provides information on education in emergencies and in some cases, databases from the national education ministries, with limited access (↑Humanitarian Data Exchange, no date). The World Bank's Microdata Library goes a bit further and freely provides national and sub-national survey data related to education among other datasets in its repository online (↑World Bank, 2022). All these open databases help policymakers and other stakeholders anticipate and better understand educational needs.

The UK Foreign, Commonwealth and Development Office (FCDO)[5] follows an open access policy and compels researchers and experts to make the findings of research conducted under its auspices freely available for the use of the public, and where possible, to translate them into relevant languages (↑DFID, 2013). This policy offers a good lesson for other countries that can make the research available to enhance its uptake and help others benefit from its value.

The ↑Principles for Digital Development (no date) offer nine areas for guidelines on data collection, access, and usage. Relevant tenets to open data access include:

- ensuring that the definition of 'openness' in the context is clear
- the adoption of open standards
- minimising personal data collection to protect privacy, contextualise the risks, get informed consent where applicable, and document all potentially sensitive data.

4.3. Good practice #3: Establish data sharing mechanisms and principles

Data sharing can expand the possibilities for increased collaboration and greater transparency and thereby result in improved educational outcomes. The introduction of data protection laws across the world has posed a challenge that has made it difficult for the data to be shared among three key parties: government, school-level actors (e.g., teachers and administrators), and third-party stakeholders. Based on a review of the Australian Availability and Transparency Bill 2022 and the data sharing protocols of the UK Government, establishing data sharing mechanisms can help increase collaboration and use of data (↑The Parliament of the Commonwealth of Australia, 2022; ↑UK Information Commissioner's Office, 2021). The following paragraphs discuss issues pertaining to the above-mentioned three parties.

4.3.1. Cross-governmental and inter-departmental data sharing

Data sharing agreements between federal and state governments and other states are crucial for the seamless exchange of information and data.

[5] Formerly known as the Department for International Development (DFID).

In Australia, a new data sharing mechanism under the Data Availability and Transparency Bill, 2022 facilitates sharing of public sector data across state and federal governments and public institutions (↑The Parliament of the Commonwealth of Australia, 2022). Australia's Bill is a sound instrument that allows for sharing government data for the purposes of providing government services, informing government policies and projects, and conducting research and development.

Some of the salient features of the recently passed Data Availability and Transparency Bill, 2022 in Australia (↑The Parliament of the Commonwealth of Australia, 2022) include:

1. Establishing a data sharing mechanism to facilitate different state-level entities to share public sector data with other states and federal governments, as well as public organisations in Australia.
2. Sharing of only government data in order to provide government information, inform government policies and projects, and conduct research and development.
3. Establishing data sharing principles, such as data minimisation and output principles, that must be followed. (For further information, see Box 3.)
4. Appointing a National Data Commissioner who performs oversight functions of the implementation of the regulation, and ensures compliance with best practices in data sharing.

At the time of writing, in Pakistan, no formal mechanisms have been established to transfer data between different levels of government — a key obstacle in developing a nationwide EMIS 2.0 system. Data sharing mechanisms between different departments and government agencies will facilitate the proper and timely transfer of data.

4.3.2. Data sharing at the school level

In education, sharing data with teachers, public officials, and administrators to help them track the progress of educational indicators can lead to improved results. Research from EdTech Hub in Ghana and other LMICs found that the sharing of monitoring and student tracking data can enhance efficiency, including reducing teacher absenteeism. Furthermore, the findings show that the use of data-enabled

improvement in transparency and civil society participation (↑McIntyre et al., 2021).

4.3.3. Third-party data sharing

Access to data by startups and private companies can spark innovative products and services and help create significant economic value (↑OECD, 2020). However, regulatory frameworks must simultaneously ensure the protection of the rights of data subjects to avoid any manipulation by third parties.

Many current data protection regimes do not allow for data sharing with third parties. Third parties are entities that are authorised to process personal data but that do not have a direct connection with the data user. Even the GDPR, owing to data profitability and competitive laws, does not allow the use of data-driven approaches by the private sector.

However, recently, India introduced a Data Accessibility and Use Policy 2022, and the European Union has introduced a similar bill known as the Data Governance Act 2022 for voluntary data sharing across the European Union (↑Council of the EU, 2022). Unlike previous data protection laws, which did not cover data sharing extensively and precluded third-party access to data, this recent development may help balance data sharing processes with security protocols.

Overall, data protection and sharing legislation needs to balance rights and data access. A holistic reform of data infrastructure, including developing transparency mechanisms, institutional change and elaborate legislation and policies, would be required to enable active data sharing with the private sector (↑Australian Government Productivity Commission, 2017).

4.4. Data sharing principles

Some high-income countries have introduced data sharing principles and even legal frameworks to ensure data protection and privacy rights. The Australian Availability and Transparency Bill 2022 (↑Markham, 2020) provides a framework for robust data sharing protocols. The data sharing principles highlighted in the Australian Availability and Transparency Bill 2022 comprise the following:

Table 1. *Data sharing principles highlighted in the Australian Data Availability and Transparency Bill 2022* (↑The Parliament of the Commonwealth of Australia, 2022).

1	**Project principle**	Data sharing is for an ethical purpose and is done in the public interest and with the consent of the individuals
2	**People principle**	Data is only shared with 'appropriately qualified' people
3	**Setting principle**	Data is shared in a secure environment where standards are established
4	**Data principle**	Only essential data is shared — with the 'minimisation' of sharing personal information
5	**Outputs principle**	Data custodian and the user are aware of the purpose of data sharing

One of the best illustrations of data sharing mechanisms of non-personal data to third parties is provided in the EU Data Governance Act 2022 (↑Council of the EU, 2022) — a licensing scheme for data intermediaries. Data Intermediaries are businesses that facilitate economic transactions between data custodians and data users but do not contribute value to the data themselves. As per the law, the data intermediaries are required to comply with licensing requirements that maintain their independence and limit their data / metadata re-use. This step is taken to leverage the data potential for analytics and new innovations and ensure security.

An important initiative to understand and map the databases that exist in the education domain across sub-Saharan Africa is the Unlocking Data Initiative, to which EdTech Hub has made a significant contribution. It serves as a community of practice and a learning resource for policymakers, civil society organisations, and national statistical authorities (↑Unlocking Data Initiative, no date). Such efforts are essential for learning from the experiences of different countries on how the access and use of data can be made available to the public and other stakeholders to improve the performance of governance and improve learning outcomes. More notably, it helps to identify and strategise about the gaps and challenges in the education space (↑Unlocking Data Initiative, no date).

4.5. Data access protocols and policies: Case studies

We have selected India and Sierra Leone as case studies with the intention of drawing lessons that are applicable to Pakistan. Both countries have some similarities to Pakistan in terms of socio-economic development and colonial legacy, as well as challenges they face in their executive and legal systems. India and Sierra Leone also have relatively robust data protection legislation from which lessons can be drawn (↑DLA Piper, 2022).

4.5.1. Case Study #1: Third-Party data sharing regulation in India

The Data Accessibility and Use Policy in India (↑Ministry of Electronics and Information Technology, 2022) offers valuable lessons for facilitating and enhancing data accessibility and establishing protocols for data sharing with third parties through policy action.

Context

At the time of writing, there is no legislation for data sharing with third parties in India. However, in February 2022, the Ministry of Electronics and Information Technology (MEITY) issued the draft India Data Accessibility & Use Policy, 2022. The objective of the policy is to enable access of third parties to public data through the sale of the data (↑Ministry of Electronics and Information Technology, 2022). The main objective of data accessibility policies is to grant access to selected databases to the private sector for commercial purposes since the private sector potentially can accelerate economic value creation from the use of data.

Institutional framework and key provisions

The institutional mechanisms that will enable the operationalisation of the policy include:

1. Establishment of an India Data Office under MEITY: It is mandated with the task of coordinating with different departments for the consolidation of datasets and sharing repositories across different agencies.
2. Appointment of a Chief Data Officer by each government entity. The Data Officer will be responsible for ensuring the provision of requested high-value data and monitoring its implementation

3. Formation of the India Data Council, which will serve as a consultative body for tasks that include the finalisation of standards (↑Ministry of Electronics and Information Technology, 2022).

Merits of the policy

According to experts, the policy holds certain merits, including:

1. Potential for data-driven economic growth and innovation through data licensing to the private sector.
2. Enhanced accountability of the government by providing citizen data related to different public services.
3. Easing of inter-governmental departmental data exchange.
4. Preparation of sector-specific metadata and data standards, which will comply with open standards policy and interoperability frameworks (↑Choudhury, 2022).
5. Increased trust in data sharing to facilitate processes and reduce costs.

Limitations of the policy

Salient limitations of the policy include:

1. Unclear mandates: The mandates are quite vague and general and require further elaboration on what subjects will be covered (↑Jain, 2022).
2. Lack of frameworks for privacy-related grievances: India does not have a data protection law at the moment. In the absence of such a law, privacy rights cannot be guaranteed, and in particular, grievances, cannot be addressed.
3. Potential threats of surveillance and profiling include the collection and sharing of data through open government data portals, which comprise data from all departments. This may potentially result in the creation of extensive profiles and lead to excessive surveillance (↑Alliance for Digital India Foundation, 2022).
4. Danger of re-identification despite anonymisation: Research has shown that anonymisation is not a safe process and can be abused

through re-identification. Hence, there is a need for additional safeguards (↑Jain, 2022).

Implications

EdTech startups and private companies in India would benefit greatly from the initiative, as their ability to access the data will be optimised. However, the policy makes no mention of data protection, raising serious concerns about how data security and protection would be handled. To balance these concerns about the potential benefits of data sharing with EdTech companies, the government will have to introduce data protection mechanisms and establish other standards by amending the policy. The example of India is quite pertinent to Pakistan since it also lacks any data sharing legal instrument.

4.5.2. Case study #2: Data sharing with policymakers in Sierra Leone

This case study of Sierra Leone demonstrates the effectiveness of consolidating data in one place to provide insights to policymakers. (↑Fab Inc., 2021). It offers several lessons for data integration and access in Pakistan.

Context

A lack of synchronisation of data collection and datasets in Sierra Leone used to pose challenges to the development of effective data architecture. Policymakers did not have a systematic way of using education data for decision-making. To address this, Fab Inc., a social enterprise consultancy specialising in education data, undertook a project with Edtech Hub to integrate various datasets, including enrolment data, annual school census data, and Ebola case data into one database (↑Fab Inc., 2021). The database enables trend analyses that provide insights into geographical and economic factors affecting education access in Sierra Leone.

Database design and implementation

The initial dashboard includes data on key indicators such as enrolment (by district, levels, grades; enrolment growth and enrolment rates; repetition; radical inclusion including gender parity and children with disabilities), teachers (by gender, pay source, qualifications; subject specialisms and specialist shortages), facilities (schools, classrooms; additional classroom construction and repair needs); Water, sanitation, and

hygiene (WASH) facilities including latrines and water sources and a school map.

Fab Inc.,[6] a group of international education advisors, developed a step-by-step guide for other countries to follow to integrate disparate education databases and create a subsequent dashboard. Three key factors led to improving the systems:

1. Involving key stakeholders in the process
2. Understanding the needs of intended users for it to be effectively executed
3. Creating a demand for information use at different levels of the information chain, including schools (↑Fab Inc., 2021).

Merits of the data integration and sharing project

The key advantage of the database and dashboard is the ability to track changes over time, which makes it possible to identify areas where progress is made. It also allows policymakers to draw lessons about schools where progress is slower. More importantly, it enables policymakers and experts to tell stories with clear visuals to engage stakeholders. Another benefit of such a centralised database during the Covid-19 pandemic was that it allowed policymakers and experts to track progress and better understand the impact of Covid-19 on school closures. Policymakers needed an integrated database and an interactive dashboard to access the right information — particularly to assess the consequences of Ebola on student enrolment. Based on data analysis of school closures during the Ebola epidemic, policymakers were better prepared to assess the aftermath of school closures caused by the epidemic. Some of the benefits that resulted from the introduction of data architecture were the policy-level ownership of the database, the possibility of displaying the dashboard publicly and informing policy development and implementation based on data access and use. The refined data architecture allows for the consolidation of data in one place and sharing of data to gain insights (↑Fab Inc., 2021).

There are two main pre-conditions to enable the use of an effective data architecture system:

[6] See: https://fabinc.co.uk/

1. Unique Identification — every person has a unique non-duplicable ID in the entire system.
2. Interoperability — the ability of information technology (IT) systems and databases to exchange information (↑Fab Inc., 2021).

The database was initially developed for research purposes, but Fab Inc. is working with the Sierra Leone Ministry of Education to hand over and build capacity to operate and maintain the database, as well as training ministry staff and others in using the dashboard to support decision-making. Furthermore, the dashboard has not as yet been made public, but Fab Inc. is working with the ministry of education to do so.

Some privacy measures to secure data protection and limit access are in place. One such measure is that no personal level data is accessible or visible on the dashboard. The back-end database does have some limited personal information, but only one person has access to the main database. Furthermore, the database is password protected to ensure data protection.

Implications

Sierra Leone is a successful example of a country with limited resources that has sought to build a robust data architecture in education to enable policymakers to make meaningful decisions. The integration of fragmented datasets into one comprehensive data architecture has facilitated access of data to the right policymakers, enabling them to anticipate emergency situations and track the impact of a health emergency on key education indicators. Although Punjab has a well-functioning EMIS system and an open data system, there are several lessons that can be learned from Sierra Leone - particularly data-driven decision-making in education.

5. Data protection laws: Effective practices for data protection

A common theme identified across multiple frameworks that address data privacy and protection is the putting in place of data security measures. The OECD lays out policy prescriptions for data governance, privacy, and digital security and highlights the need for a balanced approach between protection and digital opportunities (↑OECD, no date). It also provides recommendations to improve the security of data in open-source databases through the use of data security mechanisms such as password hashing.[7] All of these procedures provide viable solutions to data security concerns (↑OpenEMIS, 2019). Likewise, a recent UNICEF publication underscores the importance of end-to-end encryption in digital services, which can protect the privacy and security of all people — including children, minority groups, and vulnerable communities (↑Kardefelt-Winther et al., 2020).

Based on an in-depth review of publications mentioned above, analysis of several country case studies focused on data protection, extracting common themes among them, interviews with global experts, and identifying the need for various measures in Pakistan, we have narrowed down a list of effective practices for data protection to include the following:

1. Establishing institutional and legal arrangements.
2. Developing a systematic approach to data governance.
3. Establishing technical safeguards and building the capacity of, and providing resources to, staff and administrators.
4. Engagement with the public and civil society organisations.

[7] Password hashing converts text passwords into a complicated string of characters using algorithms. Applying a hash to a password makes it very difficult for a cyberattacker to retrieve the original password.

5.1. Good practice #1: Establish institutional and legal arrangements

At the national level, the government should establish a rigorous institutional framework for data protection. There is a wide array of frameworks that exist across the world. Some of the examples of good practices in legal and institutional arrangements, drawn from the experiences of Malaysia and India, are as follows.

5.1.1. Develop a cohesive framework under the federal system and establish sub-national authorities.

Malaysia is a country with a federal political system and has effectively delegated data protection laws to sub-national authorities to protect rights and handle data breaches. One of the factors that enabled implementation is the development of cohesive legal frameworks under the federal system. More discussion on federal government and state government relations is provided in the case studies in Section 5.5.

5.1.2. Ensure the supervisory authority is independent and well-funded

The key institution for a sound data protection regulatory framework is a supervisory authority at the federal level. However, the mandate and composition of these authorities vary considerably from country to country. A supervisory authority needs the allocation of dedicated resources for its proper functioning. The independence of the authority is central to its ability to execute its role effectively; lack of independence due to political interference is one of the most common reasons why authorities fall short of their expected roles. In Malaysia, the supervisory authority is called the 'Personal Data Protection Department'. It is headed by a Commissioner and operates under the Ministry of Communications and Multimedia.

5.1.3. Hire technical staff to implement data protection policies

A combination of expertise from privacy lawyers, constitutional IT security experts, data protection specialists, and data analysts is needed to help

decision-makers ensure that data protection mechanisms are established properly.

5.1.4. Establish an appeals tribunal

Another important institution in Malaysia is the Information and Data Protection Appeals Tribunal, which hears appeals against review decisions by the Data Protection Commissioner to ensure grievances are heard. At the time of writing, in the Pakistan Bill, the High Court is mandated to deal with appeals, which may additionally burden the existing backlog.

5.1.5. Develop standards and guidelines for each sector

Under Malaysia's Data Protection Law 2010, the Commissioner established standards according to the specific needs of each sector. Moreover, different sectors in Malaysia, including the financial and banking sector have developed specific guidelines and policies to improve the adoption of protection policies by all stakeholders and establish regulatory obligations by different authorities. Sector-specific guidelines helped the effective adoption of data protection rules and regulations according to the nuanced challenges of each industry. The Personal Data Protection Department facilitates the implementation of effective data protection policies and standard operating procedures across organisations. Likewise, various data user forums were formed for all industries, and each industry was directed by the authority to create its own codes of practice for adherence by data users (↑Parliament of Malaysia, 2010).

5.1.6. Adopt consultative processes when drafting legislation

A consultative process ensures compliance and ownership of the legal arrangements by stakeholders. Malaysia undertook a participatory approach to drafting legislation and establishing a stringent monitoring regime. Creating incentives for data sharing by taking the concerns of different stakeholders into account can also help promote their compliance.

5.1.7. Require education programmes to conduct a data protection impact assessment

The GDPR requires different organisations working in education to conduct extensive data protection impact assessments to identify and minimise risks before initiating programmes or projects. An independent supervisory authority should help organisations understand laws and regulations and run courses and workshops to enable organisations to conduct these assessments. The supervisory authority should also be responsible for overseeing assessments and ensuring compliance.

5.1.8. Establish user rights and obligations for data processors

Although not as comprehensive as the eight rights of data subjects under GDPR (presented in Box 4 below), the Indian Draft Data Protection Bill 2019 and Malaysia's 2010 Data Protection Law both confer substantial legal rights on data subjects and address data breaches by making it obligatory to report leaks to the supervisory authorities. Extending a full range of user rights to citizens can help build trust with data subjects and generate buy-in (↑The Personal Data Protection Bill, 2019; ↑Parliament of Malaysia, 2010).

Table 2. *The Eight Rights of Data Subjects enshrined in GDPR* (↑GDPR, 2016).

1	The Right to Information: The right to know whether data concerning the data subject is being processed
2	The Right of Access: The right to know who has access to the data
3	The Right to Rectification: The right to get inaccurate data corrected
4	The Right to Erasure: The right to remove personal data
5	The Right to Restriction of Processing: The right to limit the use of a subject's data

6	The Right to Data Portability: The right to transfer data from one IT system to another
7	The Right to Object: The right to decline the processing of a subject's data
8	The Right to Avoid Automated Decision-Making: The right to avoid profiling

5.1.9. Establish a clear data breach mechanism

As per India's Data Protection Bill 2019, data fiduciaries (processors) must notify the Data Protection Authority (DPA) of any breach of personal data. The notification to the DPA must include the nature of the personal data breach, the number of data principals affected and the consequences of the breach.

5.1.10. Categorise significant data processors separately

The Indian Data Protection Draft Bill 2019, empowered the DPA to categorise significant data processors separately based on factors such as the volume and sensitivity of personal data processed. It places additional obligations on data processors based on the potential harm that can be caused by their data processing activities.

5.1.11. Regulate the intermediaries in social media

The Indian Data Protection Draft Bill 2019 suggests that all social media platforms which do not act as intermediaries be treated as publishers and held accountable for the content they host. It also recommends a mechanism be devised whereby social media platforms can be held accountable for content from unverified accounts.

5.1.12. Appointment of Data Protection Officers

Under the Indian Data Protection Draft Bill 2019, the Data Protection Officer (DPO) should be the states' senior-level officer in the government's case, whereas, in the case of a private company, the DPO should be any

executive personnel. The bill recommends every organisation appoint a DPO for addressing all issues relating to data protection and ensuring compliance. The DPO's role is to monitor compliance, advise the organisation on its data policies and data impact assessments, and act as a focal person between data subjects and the supervisory authority.

5.1.13. Develop mechanisms for data transfer

Under the Indian Data Protection Draft Bill 2019, the Data Protection Authority is required to consult the government when authorising a contract to engage in cross-border data transfer. The data of the data principal cannot be shared with any foreign government / agency without the approval of the Indian government. However, data localisation requirements in the Indian bill (requiring data to be stored and copied in India) diminish the chances of innovation and growth.

5.1.14. Establish rules for the regulation of non-personal data

The 2021 draft version of the Indian Data Protection Draft Bill 2019 mandates the central government to regulate non-personal data as well as personal data by establishing a Data Protection Authority.

Box 3. *Seven data processing principles under GDPR (↑GDPR, 2016).*

There are seven data processing principles that are not legal measures but guiding principles that embody the spirit of the law:

1. Lawfulness, Fairness, and Transparency: Purpose is legal, clean, and open
2. Purpose Limitation: Ensure that reasons for processing are clear and open
3. Data Minimisation: Ensure only data that is adequate, relevant, and limited is processed
4. Accuracy: Data that is accurate, kept up-to-date and 'erased or rectified' when inaccurate
5. Storage Limitation: Controllers and processors set limits based on the purpose of processing
6. Integrity and Confidentiality: Controllers and processors must ensure appropriate security measures
7. Accountability: Controllers and processors take responsibility for their processing activities and comply with data protection principles

5.2. Good practice #2: Develop a systematic approach to data governance

The United Nations Department of Economic and Social Affairs defines 'data governance' as a systematic approach to foster a data ecosystem that encompasses strategies at the national level, data infrastructure policies, the legal and regulatory framework for data, various related institutions as well as leadership for institutional coordination (↑Yao & Park, 2020). Data protection is increasingly tied to data governance and the effectiveness of the ecosystem under which the data protection mechanisms will operate. Hence, it is essential to work towards an improved data governance system to ensure proper data protection (↑OECD, 2019). The OECD Data Governance Frameworks Report highlights the significance of data protection vis-a-vis data governance. It highlights that data protection needs not only holistic data governance frameworks but also that those frameworks are complemented with data policies and regulations as well as instruments like data infrastructures and data standards that can facilitate the advancement of data systems in the public sector of any country. The OECD has identified three different levels of data governance, which ensure a systematic approach. Each is discussed in turn below.

1. **Strategic level**: At the strategic level, leadership, vision, and responsibility to effectively execute policies are crucial. This includes developing and implementing national and sub-national data strategies. This clarity of direction helps define expectations, roles, and goals. National data strategies in countries like Ireland, the UK, and the USA as well as Netherlands' National Data Agenda are some examples (↑OECD, 2019).
2. **Tactical level**: At the tactical level, the following two factors are important:
    i. Capacity for coordinated implementation: Committees, skills and training, funding resources, data-led innovation, data stewardship
    ii. Regulation: Legal framework and regulatory environment and setting out rules and procedures (↑OECD, 2019).
3. **Delivery level**: At the delivery level, the most important factors to ensure proper apparatuses and instruments are in place include:

i. Data Architecture: Standards, interoperability, and relationships

ii. Data Value Cycle: Data management tools, competence of different actors, coordination between the actors, and linkage of data flows

iii. Data Infrastructure: Data infrastructure, including integration tools such as equipment for storage and security, like cloud services, Application Programming Interfaces (APIs) etc. (↑OECD, 2019).

The US State Department of Education's established framework for good data governance practices in education organisations and schools include the following:

1. Security of sensitive data
2. Data vulnerability and risk management
3. Compliance with regulatory requirements
4. Establishing roles and responsibilities of parents and administrators
5. Organisational decision-making authority about who has access and devising other protocols (↑U.S. Department of Education, 2015).

Likewise, the US Department of Education has developed a comprehensive guide (↑SEDCR, 2021) for implementing strategy in different departments and agencies including clarity of purpose, strengthening the culture of valuing data, data governance and managing it, and promoting efficiency in data usage.

5.3. Good practice #3: Establish technical safeguards and develop capacity of staff and administrators

The ↑Principles for Digital Development (no date) also offer valuable guidelines on data protection and security. Relevant tenets on data protection include:

- clearly identifying roles and responsibilities related to data sovereignty, access, data ownership, and who decides the purpose of the data
- ensuring the provision of rights of data subjects

- undertaking risk-benefit comparisons, and conducting risk assessments of data; facilitating minimum use of collection
- tracking all sensitive data collection
- ensuring data consent is sought and restricting access to the data.

Policy measures related to technical safeguards include interoperability, introducing unique identifiers, data encryption techniques that are used to secure data, and capacity-building measures. We discuss each in turn below.

5.3.1. Interoperability

Interoperability ensures the protection of privacy by making it convenient for data subjects to control who can access their data and for what purpose it is used. It also ensures administrative efficiency and consolidation of data, which is essential for identity management systems (↑World Bank, 2019).

5.3.2. Unique identifier

The second most important technical factor for the seamless implementation of a data protection regime is assigning a unique identifier to every person. Through its Identification for Development Initiative (ID4D) the World Bank provides the most comprehensive guidelines involving different actors. It outlines recommendations on legal frameworks including placing safeguards and enablers, ensuring public engagement, privacy and security measures, administration, data, IT Systems, registration and coverage, credentials and authentication. It also recommends other mechanisms for interoperability, and standards like institutionalising legal and governance mechanisms, ensuring user consent and authenticated use of the systems, and control access (↑World Bank, 2019).

5.3.3. Data encryption and other methods of de-identification

The third most important action to take in establishing technical safeguards is to establish system-wide data security measures. This essentially translates into fully protecting education data in any form. All information gathered, stored, and transmitted, needs to be fully encrypted. However, it is crucial to build the capacity of personnel to fully enable all

security measures. There are different data methods for de-identification of personal data, such as data encryption of personal data, anonymisation, deletion, data masking and generalisation. Additional methods include pseudonymisation,[8] which is recommended by the ↑GDPR (2019).

5.3.4. Capacity development

We recommend that the Government of Pakistan develop capacities to integrate data security best practices as a system-wide policy framework. It requires establishing and implementing policies, standards, and other accepted procedures — especially where protection of marginalised groups and children's data is required.

Some of the capacities include developing roadmaps to replace inefficient IT systems and incorporate cybersecurity measures including utilising a high-level Intrusion Prevention System and hiring information security personnel for robust practices in data centres (↑Verizon Data Breach Investigations Report, 2022).

Besides the technical measures mentioned above, it is essential to ensure sharing of best practices and developing a strategy to train public service employees to sensitise them and get buy-in from the stakeholders working within the public sector. Specific capacity-building sessions on data literacy, strengthening data security and data governance mechanisms, data protection laws and their social implications, data integration and usage of insights for improved decision-making are some of the areas where training can be designed and delivered. Further, opportunities for mentorship, coaching, and networking must also be provided. Security experts argue that human error contributes significantly to breaches of data privacy and protection. Hence, it becomes more important to build the capacities of employees at every level.

5.4. Good Practice #4: Engage with the public

The World Bank highlights the significance of involving the general public and other stakeholders in the conversation at different stages of the policy process (↑World Bank, 2019), and is mentioned as one of the good practices to develop a culture and awareness about data protection.

[8] Pseudonymisation is a method in which a personally identifiable information record is replaced with an artificial identifier, whereas anonymisation encrypts or erases the identifiable information.

The role of civil society in India is often highlighted as quite proactive and participatory when it comes to the discussions on the Right to Information Act and the provision of data for the evaluation of government performance (↑Sharma, 2004). One step that can be taken is to enhance the interface between data activists and civil society organisations working on human rights and monitoring the performance of the government in different sectors. In one of our interviews with key informants, it was mentioned that Malaysia is one example where a civil society organisation proactively took part in the initial consultation before the data protection legislation in Malaysia was drafted. Public engagement with the industry partners ensured their buy-in to the whole process, and continuous dialogues with the industry partners enabled their compliance.

5.5. Data protection laws: Case studies

The case studies in this section are intended to highlight the challenges that Pakistan faces in the implementation of data protection laws. Through the examples of Malaysia and India, we identify different pathways that Pakistan could potentially adopt to address these problems.

5.5.1. Case Study 1: Effectiveness of implementation of Malaysian data protection law

Context

Malaysia has been a pioneer among low- and middle-income countries in the introduction of data protection law. It is an example of a country with a dedicated data privacy and protection act, the Malaysian Personal Data Protection Act (2010), which was introduced to restore consumer trust in the use of data in the face of excessive credit card fraud. Legislation concerning data privacy and protection is consolidated, accessible, and structured under the act, which contains relevant subsidiary legislation. A coordinating body, the Commissioner, develops and enacts standards and guidelines. Under this guidance, specific sectors (industries) generate their own Codes of Practice, which are tailored to the needs of each sector but conform to the overarching standards and guidelines (↑Ping, 2021).

Enabling factors for proper implementation in Malaysia

Based on our analysis of the Malaysian data protection regime (↑Ping, 2021), and our interview with a global data protection expert, we have

identified the following key features of the Malaysian legislation (and overall ecosystem).

1. Robust, rationalised, and well-structured legislation.
2. Explicit definition of data types and their safeguards in the bill.
3. Participatory and consultative process adopted during the drafting of the bill to ensure buy-in from various stakeholders.
4. Sub-national-level enforcement and implementation of the law to ensure the constitutional requirements of a federal system are met.
5. Dedicated authorised government authority to implement legislation into policy, standards, and guidelines and to monitor implementation in government agencies.
6. Capacity and willingness of sector agencies to understand, contextualise, and implement policy, standards, and guidelines.
7. Maturity of the government legislative, judicial, and bureaucratic systems.
8. Overall governance rating — a complex hybrid of various indices related to governance (education, social development, corruption index, systems, and rule of law).

Limitations of the Malaysian Personal Data Protection Act

The bill exempts all government agencies from the purview of data regulation procedures, safeguards, and oversight mechanisms. ↑Ping (2021) has identified further limitations including the prohibition of data usage for journalistic purposes. Further, the independence of the Commissioner can be affected through intervention by a government minister. Some of the other notable weaknesses highlighted include no provision for an appeal in case of non-issuance of a notice and the requirement of providing written notice in case of withdrawing consent, which makes it practically difficult to implement (↑Greenleaf, 2010).

Implications

Despite its limitations, Malaysia is ahead of many East Asian countries in the design and implementation of its data protection legal framework. It can serve as a robust example for Pakistan as a starting point for the enforcement and implementation of data protection and the creation of

institutional mechanisms to address future challenges. However, the government sector must not be exempted from data regulation and safeguarding procedures.

5.5.2. Case Study 2: Data Regulation in a federal system — India

Background

A number of countries in the world, such as India, Pakistan, Nigeria, the USA, Malaysia, and Brazil, have a federal system of government, which gives certain powers to regional states.

India is a good example of a country with a federal system whereby regional governments have the power to draft and implement legislation in their 'states'. However, the capacity of regional governments to legislate independently varies across India and depends on the political dynamics in the region and the leadership and the ability of the executive bodies to carry out such functions.

Challenges of establishing a regulatory framework across multiple government levels

Under the Indian Constitution, executive power is divided between the Union (federal) and the (regional) States. The Union Government has jurisdiction over certain categories (Union List), with a few other matters in the sub-federal units' control (State List) while the remainder is to be shared between the two constituencies of power (Concurrent List) (↑Mittal, 2021). Moreover, the states in India are empowered to draft their own legislation and create policies to regulate certain matters. In this way, India is unique, as states are very independent, conserve their rights and resist too much federal government interference.

Furthermore, it is yet to be determined whether privacy is a matter for regional governments / states, or whether it comes under the jurisdiction of the Union Government of India. As such, privacy has been declared a 'Fundamental Right' by the Supreme Court of India (↑Sikri, 2018), and consequently, it becomes obligatory for the government to protect the privacy of data subjects and impose obligations on data processors, but the government level is yet to be determined, hence it is not clear which government level is the competent authority to deliver on data rights. Data protection and associated legislations, policies, and procedures should

address this question categorically to avoid any confusion down the line. The federal government could benefit inadvertently from legislation and regulation introduced at a regional / state level. However, the clarity and consistency of legislation must be focused on to achieve the desired results.

Merits of establishing federal legislation

Although regional states are mandated to draft their own legislation in countries like India and Pakistan, experts argue that consistent national legislation for data protection is much better for four main reasons, namely:

1. uniformity of legislation
2. coverage of protection of all citizens
3. ease in facilitating a coherent regulatory environment
4. to conserve resources.

Box 4. *Case in point: Digital health data in India.*

In a paper titled 'Technological Federalism: A Building Block to Constitutionalise the Digital Sphere', the term 'technological federalism' refers to the digitisation of healthcare and health data by the Union Government in India (↑Mittal, 2021). However, there are several challenges with establishing the exact placement of jurisdiction of health as a subject. As far as data collection for statistical purposes is needed, the federal government may have a mandate, but when it comes to health delivery through digital means, the exact nature of the mandate at the federal level is unclear. In the past, digital health initiatives such as the Health Management Information System were developed in collaboration with sub-national units across India (↑Mittal, 2021).

Possible pathways for clarifying data regulation in federal systems

1. In a federal system, there are always some elements of legislation which are federal and others which are state / provincial, and still others which are interpreted with respect to policy and outcomes of trial cases and are court derived. Therefore, the judiciary can play an important role in interpreting the roles and mandates of different jurisdictions.

2. Initiating a debate on the scope of power of states and federal governments through legislative dialogue and the determination and categorisation of different subjects with digitisation in view.

3. Establishing a cooperative framework and mechanism to work jointly with states / federal government and commercial entities is very important in developing legislation, implementation agencies, and balancing state and federal powers. In Pakistan, these cooperative mechanisms already exist in the form of the Interprovincial Coordination Committee and the Council of Common Interests. However, due to weak norms and political differences they often fail to yield desired results.

4. Developing well-defined, coherent, and clear mechanisms and agreements between states and federal governments can lead to feasible operationalisation of working relationships between different units of government.

Implications

After the passage of the 18th Amendment (2010), when most of the federal ministries such as education and health, among others, were transferred to the provinces (↑The Gazette of Pakistan, 2010), Pakistan's federal structure became more similar to India's. Legally, as well as politically, this leads to inconsistencies, which often impede good governance and also lead to a huge variation in the quality of governance between states. However, Pakistan could devise a well-structured and implementable data protection mechanism through a framework mutually acceptable to all stakeholders and clarify the jurisdiction of data protection in education.

6. A way forward

This brief identifies key recommendations for the Government of Pakistan and development partners on data access and protection. Recommendations on strengthening the legal framework for data protection may sit outside of the education sector; however, recommendations on data access and protection are aimed at the Ministry of Education, the Ministry of Information, and other relevant provincial departments.

6.1. Recommendations to legislators and public bodies

The list below comprises our recommendations for legislators and related public agencies and departments of the Government of Pakistan to strengthen legislation and the legal framework for data protection.

1. Revise the current Personal Data Protection Bill to remove exemptions for government authorities and agencies. This would extend the scope of the current law to cover public organisations, creating greater accountability and transparency. Furthermore, clearly define ambiguous terms like 'state', 'authorities', 'data subjects' and more in the legislation.

2. Focus on implementing the complete range of rights for data subjects to provide data protection in line with the best practices mentioned above to ensure proper protection of privacy rights. Many rights, such as the right to erasure, may be difficult to implement in practice; therefore, exploring effective implementation is critical to achieving strengthened legislation.

3. In any updates to the Personal Data Protection Bill, undertake stakeholder consultations to surface challenges and incorporate viewpoints from government, the public, and third-party stakeholders.

4. Empower the federal supervisory authority by ensuring a higher level of independence to minimise political interference. Empower other important institutions such as the Appeals Tribunals to ensure transparency and accountability. Develop data breach and data

transfer mechanisms to ensure the robustness of the legal framework.

5. Draft subsidiary legislation to facilitate data access, data sharing, the legality of non-personal data, and data use by third parties. However, further legislation should acknowledge the role security plays in protecting the rights of data subjects while introducing measures for data sharing.

6. More importantly, current legislation could be strengthened by putting in place provisions to protect the rights of minors and children and marginalised groups through enforcing stricter safeguarding measures and a regulatory environment.

6.2. Recommendations to the Federal Ministry of Education

6.2.1 Recommendations for data access

1. Strengthen special security mechanisms and their implementation to ensure the rights of minors, children, and minority groups; ensure strict penalties are in place to enforce them in collaboration with the Ministry of Information and other related departments. In light of global efforts to protect children from risks and harm, prioritise enabling a secure environment for children online. Develop national and sub-national policies for the rights of children and disadvantaged minority groups, and develop guidelines for the private sector to ensure children's data security. Design tools like impact assessment for compliance with children's data rights.

2. Prioritise consolidation of all educational databases under EMIS through better data architecture and mechanisms of data sharing. This includes investing in the interoperability of government databases and IT systems at the provincial and federal levels to enable better consolidation of data from different sources and enable data sharing.

3. Build open education data systems and better data architecture, balanced with strong safeguards to protect data and support data accessibility for third parties, including parents, teachers, education administrators, as well as researchers, EdTech startups, and civil society organisations.

4. Ensure that data is accessible to policymakers. Facilitate the linkage of a national EMIS with open data from the education sector to improve transparency and accountability, while simultaneously creating strong safeguards to protect data. Enhanced coordination between different provincial authorities must be ensured for gathering and integrating data and making it available for decision-makers and drawing insights, which can translate into meaningful actions.

5. Efforts to protect privacy and provision of access to data, including sharing data with third parties, must strike a balance between data protection rights and data access. This effort must be complemented by a comprehensive improvement in data infrastructure, transparency mechanisms, institutional change, and detailed policies for education-related institutions.

6.2.2. Recommendations for data protection

1. Across the education system, implement effective data protection practices, such as assigning data protection officers, regularly deleting data that has already served its purpose, encrypting sensitive data, and more. Provide dedicated resources for data security and data infrastructure for compliance with standards in the education sector.

2. Train civil servants working in the education sector and provide them with professional development opportunities on data protection and access. Ensure inclusion of dedicated human and legal resources who can provide expertise to education departments.

3. Invest in technical safeguards to protect the security and privacy of education data, for example, de-identification and encryption techniques.

4. Undertake public consultation on education data access and protection to surface and address concerns and generate buy-in from education sector stakeholders. In addition, the government should ensure that continuous support in developing capacity to adhere to the requirements of data protection are met.

5. Build capacity of the organisations in conducting rigorous privacy and data protection impact assessments, so that their privacy risks can be minimised, managed, or eliminated. Moreover, with the

support of development partners and privacy experts, sophisticated and easy-to-use tools should be developed along with the guidelines on undertaking assessments for the organisations to ensure the sustainability of assessments.

6.3. Recommendations to development partners

Development partners can facilitate and support data protection in four main ways. These include capacity building, strengthening of the enabling environment, advocacy, and public engagement.

6.3.1. Capacity building

Development partners should focus on developing the capacities of different stakeholders in the education sector at two different levels.

1. **Individual-level capacity building**

   To develop leadership on the issues of data protection and data access, development partners should support the government to provide training to key individuals working in important education departments, programmes, and private education organisations. Likewise, the development partners could help the government agencies to conduct capacity-building sessions for education leaders, lawyers, Chief Data Officers and Chief Privacy Officers, data activists and other human rights advocates to build their expertise. Furthermore, development partners could support provincial teacher training departments to design focused data access and protection training sessions for teachers and school principals.

2. **Organisational-level capacity building**

   Development partners can support the development of training manuals or other materials to share effective education data management practices, including case studies on data protection in education settings. Development partners should support government agencies to develop their privacy policies and data strategies. Development partners should prioritise promoting data protection assessment practice in public and private sectors through training. At the same time, development partners can support provincial data-gathering agencies to develop their systems by providing access to experts in EMIS, open data, and monitoring.

6.3.2. Strengthen the enabling environment

Development partners should coordinate efforts across different projects in the country to improve the overall policy framework for data protection, economic, political, environmental, and social factors in a coherent and mutually reinforcing manner. Key recommendations include:

1. **Developing and sharing a road map for adoption**

   Development partners could work with different stakeholders in the education sector to develop a roadmap on ways to achieve some of the recommended steps with specific short-term and medium-term milestones and outcomes. A concrete roadmap could help make lessons learnt more actionable for the Education Ministries and Education departments in the Government of Pakistan.

2. **Facilitating the development of national and sub-national data strategies**

   It is crucial to develop national-level data strategies related to education and build capacities to implement those strategies. Providing key legal and technical expertise and developing toolkits for public organisations that use data frequently can be good starting points.

6.3.3. Advocacy and communication

Political commitment, leadership, and developing an enabling environment are keys to harnessing a culture of data protection and security and at the same time improving access to data under certain obligations. Development partners should facilitate advocacy sessions with policymakers, data activists, and other stakeholders. They could also publish white papers and other material on key data access and protection challenges in the education sector. Furthermore, development partners may have a role to play in facilitating dialogue through consultative sessions with industry partners and other stakeholders to get insights into their perspectives.

6.3.4. Raising awareness

Development partners can support government departments to develop privacy policies and overall data strategies. They can also conduct workshops on stakeholders including academia, think tanks, and civil

society organisations on the value of data access to improve accountability and transparency.

Bibliography

This bibliography is available digitally in our evidence library at https://docs.edtechhub.org/lib/GV4MKFZH

Data Availability and Transparency Bill 2020 [and] Data Availability and Transparency (Consequential Amendments) Bill 2020, 35 (2020) (testimony of David Markham). (details)

Data Availability and Transparency Bill 2022, (2022) (testimony of The Parliament of the Commonwealth of Australia). https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6649_aspassed/toc_pdf/20174b01.pdf;fileType=application%2Fpdf. (details)

Data Protection Act 2018, (2018) (testimony of UK Data Protection Act). https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. (details)

Draft India Data Accessibility and Use Policy (2022) (testimony of Ministry of Electronics and Information Technology). https://www.meity.gov.in/writereaddata/files/Draft%20India%20Data%20Accessibility%20and%20Use%20Policy_0.pdf. (details)

Personal Data Protection Bill 2020, 33 (2021) (testimony of Ministry of Information Technology and Telecommunication). (details)

Prevention of Electronic Crime Bill, (2016) (testimony of Ministry of Information Technology). https://na.gov.pk/uploads/documents/1470910659_707.pdf. (details)

Abdul-Hamid, H. (2014). *What Matters Most for Education Management Information Systems : A Framework Paper*. https://openknowledge.worldbank.org/handle/10986/21586. (details)

Adam, T., El-Serafy, Y., Podea, M., & Haßler, B. (2021). *The Use of "Building Blocks" to Develop Digital Platforms for Education in Sub-Saharan Africa*. EdTech Hub. (details)

Ali, K. (2021). *Pakistan personal data protection bill termed vague – Pakistan — DAWN.COM*. https://www.dawn.com/news/1653675. (details)

Alliance for Digital India Foundation. (2022). *Whose Data is it Anyway?: Decoding the Draft India Data Accessibility & Use Policy, 2022*. https://blog.adif.in/p/whose-data-is-it-anyway-decoding. (details)

Australian Government Productivity Commission. (2017). *Data Availability and Use*. https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf. (details)

Barr, A., Mugisha, F., Serneels, P., & Zeitlin, A. (2012). *Information and collective action in community-based monitoring of schools : Field and lab experimental evidence from Uganda*. https://www.semanticscholar.org/paper/Information-and-collective-action-in-monitoring-of-Barr-Mugisha/99f5806ab361f3308d652b9549b390e4f183b672. (details)

Bhi, B. (2020). Bolo Bhi's Analysis of the Personal Data Protection Bill 2020. *Bolo Bhi*. https://bolobhi.org/bolo-bhis-analysis-of-the-personal-data-protection-bill-2020-3/. (details)

COPPA. (1998). *Children's Online Privacy Protection Rule ("COPPA")*. Federal Trade Commission. http://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa. (details)

Choudhury, D. (2022, February). *India's Draft Data Policy Unlocks Government Data for All Mulls Monetisation*. https://www.business-standard.com/article/economy-policy/india-s-draft-data-policy-unlocks-govt-data-for-all-mulls-monetisation-122022100933_1.html. (details)

Council of the EU. (2022). *Council approves Data Governance Act*. https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/le-conseil-approuve-l-acte-sur-la-gouvernance-des-donnees/. (details)

DFID. (2013). *DFID Research Open and Enhanced Access Policy*. 15. (details)

DLA Piper. (2022). *DLA Piper Global Data Protection Laws of the World – World Map* [Map]. https://www.dlapiperdataprotection.com/. (details)

Department of Education Children Services. (2013). *Data Access Protocol*. https://education.nt.gov.au/__data/assets/pdf_file/0006/257883/DataAccessProtocol.pdf. (details)

European Commission. (2015). *Towards a new digital ethics: Data, Dignity and Technology*. https://edps.europa.eu/data-protection/our-work/publications/opinions/towards-new-digital-ethics-data-dignity-and_en. (details)

Fab Inc. (2021). *Learning from experience: A Post-Covid-19 Data Architecture For a Resilient Education Data Ecosystem in Sierra Leone*. Zenodo. https://doi.org/10.5281/ZENODO.5498054. Available from https://zenodo.org/record/5498054. Available under Creative Commons Attribution 4.0 International, Open Access. (details)

GDPR. (2016). *General Data Protection Regulation (GDPR) – Official Legal Text*. General Data Protection Regulation (GDPR). https://gdpr-info.eu/. (details)

GDPR. (2019). *GDPR Definitions*. GDPR-Text.Com | GDPR Text, Translation and Commentary. https://gdpr-text.com/read/article-4/. (details)

Government of India. (2019). *The Personal Data Protection Bill*. http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf. (details)

Greenleaf, G. (2010). *Limitations of Malaysia's Data Protection Bill*. 4. (details)

Gruen, N., Houghton, J., & Tooth, R. (2014). *Open for Business: How Open Data Can Help Achieve the G20 Growth Target*. Lateral Economics. https://lateraleconomics.com.au/wp-content/uploads/omidyar_open_business.pdf. (details)

Hennessy, S., Jordan, K., Wagner, D. A., & EdTech Hub Team. (2021). *Problem Analysis and Focus of EdTech Hub's Work: Technology in Education in Low- and Middle-Income Countries*. https://docs.edtechhub.org/lib/PBXBB7LF. (details)

Human Rights Watch. (2022, May 25). Governments Harm Children's Rights in Online Learning. *Human Rights Watch*. https://www.hrw.org/news/2022/05/25/governments-harm-childrens-rights-online-learning. (details)

Humanitarian Data Exchange. (n.d.). *Humanitarian Data Exchange*. OCHA Services: Humanitarian Data Exchange. Retrieved June 20, 2022, from https://data.humdata.org/. (details)

Jain, A. (2022). *5 Problems with the Draft India Data Accessibility & Use Policy, 2022*. https://www.moneycontrol.com/news/politics/5-problems-with-the-draft-india-data-accessibility-use-policy-2022-8154271.html. (details)

Jelenic, M. C. (2019). *From Theory to Practice: Open Government Data, Accountability, and Service Delivery*. 49. https://doi.org/10.1596/1813-9450-8873. (details)

Kalyar, B. J. A. (2021). *Comparative Analysis of Personal Data Protection Bill 2020*. https://mediamatters.pk/wp-content/uploads/2021/02/Comparative-Analysis-of-Personal-Data-Protection-Bill-2020.pdf. (details)

Kardefelt-Winther, D., Day, E., Berman, Witting, S. K., & Bose, A. (2020). *Encryption, Privacy and Children's Right to Protection from Harm*. UNICEF Office of Research – Innocenti. https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf. (details)

Khaitan and Co. (2022). *White Paper on Privacy and Data Protection*. https://www.khaitanco.com/sites/default/files/2022-03/KCO%20ASSOCHAM_JPC%20Whitepaper_2%20March%202022.pdf. (details)

Khan, K. (2018). *Punjab, Pakistan: Using Open School Data to Improve Transparency and Accountability*. http://www.iiep.unesco.org/en/punjab-pakistan-using-open-school-data-improve-transparency-and-accountability. (details)

Maldoff, G. (2016, April). *How GDPR changes the rules for research*. https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/. (details)

Massachusetts Department of Elementary and Secondary Education. (n.d.). *School and District Data—Massachusetts Department of Elementary and Secondary Education*. https://www.doe.mass.edu/SchDistrictData.html. (details)

McIntyre, N., Sabates, R., & Eberhardt, M. J. (2021). *A Literature Overview of Accountability and EdTech: Recommendations for Using Technology to Improve Accountability in Educational Systems from Ghana and Other LMICs*. EdTech Hub. (details)

Mittal, A. (2021). *Technological Federalism : A Building Block to Constitutionalise the Digital Sphere*. https://www.epw.in/journal/2021/47/commentary/technological-federalism.html. (details)

OECD. (2019). *The Path to Becoming a Data-Driven Public Sector*. https://www.oecd-ilibrary.org/sites/9cada708-en/index.html?itemId=/content/component/9cada708-en. Available from https://www.oecd-ilibrary.org/sites/9cada708-en/index.html?itemId=/content/component/9cada708-en. (details)

OECD. (2020). *OECD Digital Economy Outlook 2020*. https://www.oecd-ilibrary.org/sites/3b6a594d-en/index.html?itemId=/content/component/3b6a594d-en. Available from https://www.oecd-ilibrary.org/sites/3b6a594d-en/index.html?itemId=/content/component/3b6a594d-en. (details)

OECD. (n.d.). *Data Governance, Privacy and Digital Security*. Retrieved June 15, 2022, from https://www.oecd.org/digital/ieconomy/information-security-and-privacy.htm. (details)

OECD. (n.d.). *Data-driven innovation for growth and well-being*. https://www.oecd.org/sti/ieconomy/data-driven-innovation.htm. (details)

OneTrust DataGuidance. (2022, February 28). *Pakistan: Federal Cabinet approves Draft Personal Data Protection Bill*. DataGuidance. https://www.dataguidance.com/news/pakistan-federal-cabinet-approves-draft-personal-data. (details)

Open Data Handbook. (2022). *Open Data Handbook*. https://opendatahandbook.org/. (details)

Open Data Punjab. (2022). *Open Data Punjab*. https://open.punjab.gov.pk/schools/. (details)

Open Knowledge Foundation. (n.d.). *Open Data Commons: legal tools for open data*. Retrieved June 20, 2022, from https://opendatacommons.org/. (details)

OpenEMIS. (2019). *OpenEMIS_Data_Security_Practices_en.pdf*. https://www.openemis.org/wp-content/uploads/2019/10/OpenEMIS_Data_Security_Practices_en.pdf. (details)

Pandey, P., Goyal, S., & Sundararaman, V. (2008). *Public Participation, Teacher Accountability, and School Outcomes: Findings from Baseline Surveys in Three Indian States*. https://openknowledge.worldbank.org/handle/10986/6346. (details)

Parliament of Malaysia. (2010). *Personal Data Protection Act 2010*. https://www.pdp.gov.my/jpdpv2/assets/2019/09/Personal-Data-Protection-Act-2010.pdf. (details)

Ping, J. C. Y. (2021, June 24). *Malaysia Data Protection Overview*. DataGuidance. https://www.dataguidance.com/notes/malaysia-data-protection-overview. (details)

Principles for Digital Development. (n.d.). *Principles for Digital Development*. Principles for Digital Development. Retrieved June 20, 2022, from https://digitalprinciples.org/. (details)

Punjab Curriculum & Textbook Board. (2021). *Teaching of Naazrah Quran Grade I–V as a separate compulsory subject*. https://pctb.punjab.gov.pk/system/files/Teaching%20of%20Naazrah%20Quran%20Grade%20I-V%20as%20a%20separate%20compulsary%20subject_Compressed.pdf. (details)

Punjab School Monitoring. (n.d.). *Punjab School Monitoring*. Retrieved June 20, 2022, from https://open.punjab.gov.pk/schools/. (details)

RD4C. (n.d.). *Responsible Data for Children: Principles*. Responsible Data for Children. Retrieved June 20, 2022, from https://rd4c.org//. (details)

Romadhoni, F. (2020). *What is Data Lifecycle Management? And What phases would it pass through? https://medium.com/jagoanhosting/what-is-data-lifecycle-management-and-what-phases-would-it-pass-through-94dbd207ff54*. (details)

SEDCR. (1991). *Standards for Education Data Collection and Reporting* (p. 145). (details)

SEDCR. (2021). *Forum Guide to Strategies for Education Data Collection and Reporting*. 50. (details)

Shahani, S. H. (2020, May 28). *Comparative Analysis of Personal Data Protection Bill 2020 with Laws and Bills in the EU, UK, India, and Malaysia*.

https://bolobhi.org/comparative-analysis-of-personal-data-protection-bill-2020-with-laws-and-bills-in-the-eu-uk-india-malaysia/. (details)

Sharma, P. (2004). Civil society and right to information: a perspective on India's experience. *Eldis*. https://www.eldis.org/document/A41898. (details)

Sikri, A. (2018). *Justice K.S. Puttaswamy (Retd) vs Union Of India on 26 September, 2018*. https://indiankanoon.org/doc/127517806/. (details)

The Gazette of Pakistan. (2010). *18th Amendment*. https://na.gov.pk/uploads/documents/1302138356_934.pdf. (details)

The Personal Data Protection Bill. (2019). *The Personal Data Protection Bill 2019*. http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf. (details)

The Punjab Transparency and Right to Information Act. (2013). *The Punjab Transparency and Right to Information Act 2013*. http://punjablaws.gov.pk/laws/2547.html. (details)

U.S. Department of Education. (2015). *Data Governance and Stewardship*. 7. (details)

UK Information Commissioner's Office. (2021). *Data sharing agreements*. https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/data-sharing-agreements/. (details)

UK Parliament. (2022). *Online Safety Bill publications – Parliamentary Bills – UK Parliament*. https://bills.parliament.uk/bills/3137/publications. (details)

UNCTAD. (2022). *Data Protection and Privacy Legislation Worldwide | UNCTAD*. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. (details)

UNESCO. (2019). *Access to information: A New Promise for Sustainable Development*. https://unesdoc.unesco.org/ark:/48223/pf0000371485. (details)

UNICEF. (2011). *Child Safety Online: Global challenges and strategies*. Innocenti Publications.

https://www.unicef-irc.org/publications/650-child-safety-online-global-challenges-and-strategies.html. (details)

UNICEF. (2020). *Review of Education Management Information Systems (EMIS) that Track Individual Student Data – Malaysia*. https://www.unicef.org/eap/media/6021/file/EMIS%20malaysia.pdf. (details)

UNICEF. (2021). *The Case for Better Governance of Children's Data: A Manifesto*. https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf. (details)

Unlocking Data Initiative. (n.d.). *Unlocking Data*. Retrieved June 20, 2022, from https://unlockingdata.africa/. (details)

Verizon Data Breach Investigations Report. (2022). *2022 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/. (details)

World Bank. (2021). *World Development Report 2021: Data for Better Lives*. The World Bank. https://doi.org/10.1596/978-1-4648-1600-0. Available from http://elibrary.worldbank.org/doi/book/10.1596/978-1-4648-1600-0. (details)

World Bank. (2022). *Microdata Library*. https://microdata.worldbank.org/index.php/home. (details)

World Bank. (n.d.). *ID4D Practitioner's Guide*. Retrieved June 14, 2022, from https://id4d.worldbank.org/guide/non-exclusion-and-non-discrimination. (details)

World Economic Forum. (2021). *6 Data Policy Issues Experts Are Tracking Right Now*. https://www.weforum.org/agenda/2021/03/6-key-issues-that-are-trending-in-data-policy-right-now/. (details)

Yao, K., & Park, M. K. (2020). *UN/DESA Policy Brief #89: Strengthening Data Governance for Effective Use of Open Data and Big Data Analytics for Combating COVID-19*. https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-89-strengthening-data-governance-for-effective-use-of-open-data-and-big-data-analytics-for-combating-covid-19/. (details)