Toward a trusted digital nation

A multicountry analysis on data protection in Africa and Asia

Authors: Vineet Anand, Surbhi Sood, and Shrabasti Dhar

MSC
MicroSave Consulting

The GDPR spurred a global shift and prompted nations to adopt strong data laws that protect privacy, ensure accountability, and secure digital spaces

The European Union enacted the General Data Protection Regulation (GDPR) in 2018, which marked a pivotal shift in the global approach to data privacy and security. As the first comprehensive regulatory framework of its kind, the GDPR set stringent standards for the collection, storage, and processing of personal data and empowered individuals with greater control over their information.

The GDPR's influence has since catalyzed the development of similar legislations worldwide. These include the California Consumer Privacy Act (CCPA) in the United States, the Personal Information Protection Law (PIPL) in China, and the Digital Personal Data Protection Act (DPDPA) in India. These laws collectively signal a global movement toward securing digital environments, safeguarding user rights, and ensuring organizational accountability. As of 2025, 39 out of 55 countries in Africa have enacted data protection laws.

1. **SIM swap fraud via data leak:** A major data breach exposed *Aadhaar* numbers and linked phone numbers, which fraudsters used to perform SIM swap scams. They hijacked mobile numbers to bypass OTP-based bank security and withdrew money from victims' accounts. This incident highlighted critical gaps in data security, including inadequate protection of sensitive personal data, a lack of user consent controls, and the absence of real-time fraud detection. It resulted in financial loss for individuals and damaged public trust in the country's digital infrastructure.
2. **The Philippines 2016 election data breach: Cybersecurity failure:** In 2016, the Philippines' election commission suffered a massive data breach, which exposed sensitive information of more than 55 million voters, including passport details, fingerprints, and mailing addresses. The breach resulted from a lack of encryption and inadequate cybersecurity infrastructure. As a result, citizens were left vulnerable to identity theft, fraud, and phishing attacks, which sparked public outcry and legal scrutiny.

Robust data protection in digital transactions builds trust, ensures regulatory coherence, and drives inclusive growth, particularly in emerging digital economies

In 2023, digital transactions were valued at an estimated USD 1.4 trillion globally. Enhanced consumer protection in digital transactions could unlock an additional USD 300–400 billion in transaction volume. This underscores the importance of robust data protection frameworks, particularly in developing economies, to build secure and inclusive digital infrastructures.

A study by the Asian Development Bank (ADB) further reinforces this imperative and highlights data protection as an essential element that builds trust, ensures equitable access, and promotes regulatory coherence. Worldwide, 71% of countries and 57% in Asia and the Pacific have enacted data protection laws, many with extraterritorial and cross-border provisions. These regulations help establish a level playing field that balances consumer rights with business compliance across jurisdictions.

Digital protection now serves as a critical policy lever to advance inclusive and secure digital ecosystems. MicroSave Consulting (MSC) has emphasized that trust remains a foundational element in digital inclusion. Our research shows that nearly 50% of registered users disengage from digital financial services due to concerns over trust and data security.

Uniform consent rules hamper the digital economy's growth as it makes compliance costly and unviable—20.5% of apps breach the GDPR, and 30% of consent management platforms ignore opt-outs. If smaller players treat all data the same, it burdens them and stifles innovation. A tiered consent management system that aligns with data sensitivity is essential for practical, scalable data sharing. It enables low-risk exchanges with simpler consent and simultaneously enforces stricter controls for sensitive data, which ensures both user protection and the feasibility of digital economy use cases.

3. Biggest cyber targets - Nigeria and South Africa:

A 2020 report by Sophos on cloud security revealed growing vulnerabilities in Africa, with Nigeria and South Africa facing significant threats.

- In Nigeria, 86% of organizations reported cloud security incidents, with misconfigurations (64%) and stolen credentials (36%) being the main causes.
- Only 54% of Nigerian firms had full visibility into their cloud assets, which indicates gaps in infrastructure management.
- In contrast, South Africa had better asset awareness (79%) but reported one of the highest global rates of stolen cloud credentials, which contributed to 59% of breaches.

These findings underscore the need for improved cloud governance, stronger authentication methods, better configuration controls, and enhanced user education to protect both systems and consumers.

For more case studies and data protection judgments click here

Data protection landscape

Methodology for the multi country analysis on data protection policy and guidelines

Objectives

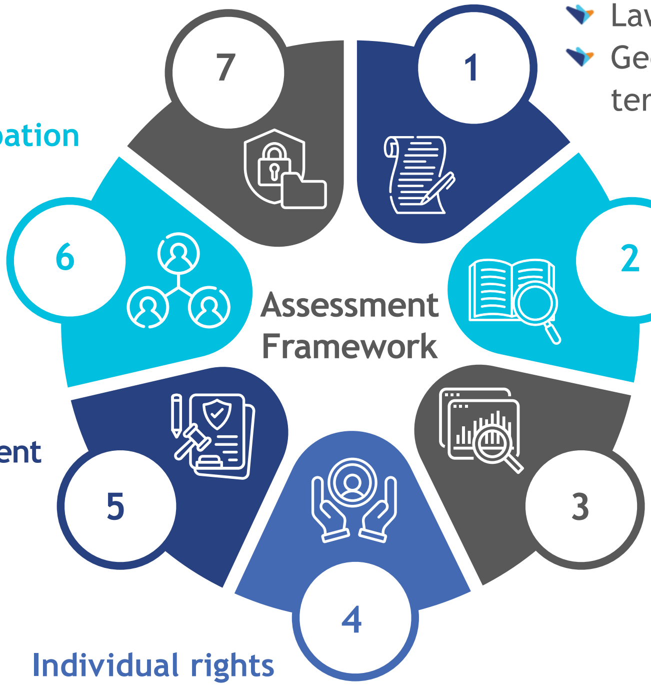
- This study intends to analyze data protection policies, regulations, and enforcement in jurisdictions across 12 countries, to highlight regional differences and distinctive regulatory features for comparative insights.
- Based on the findings, we will identify strategic recommendations for each country to strengthen its data protection framework.

Countries

The regions covered in the study include:

- South Asia: India, Bangladesh, Pakistan
- Southeast Asia: Indonesia, Cambodia, the Philippines, Lao PDR, Myanmar
- Africa: Kenya, Nigeria, Uganda, Senegal

Framework for the data protection policy analysis



Legislation and scope

- Law
- Geographical territory
- Material
- Authority
- Consent

Definitions

- Data controller
- Data processor
- Personal data
- Sensitive data
- Health data
- Biometric data
- Pseudonymization

Controller and processor obligations

- Data transfer
- Data processing
- Breach notification
- Data retention
- Children's data

Individual rights

- Nominate
- Access
- Rectification
- Erasure
- Object
- Portability

Penalties and enforcement

- Penalty
- Enforcement

Stakeholders participation

- Private players
- Government programs
- Donors' aid

Data privacy interventions for consumers

- Event/ Campaign
- Solution Development

Our assessment framework outlines key variables essential for a thorough assessment of data protection policies, regulations, and enforcement across jurisdictions (1/2)

Legislation and scope: The variable assesses the presence of data privacy legislations, their geographical applicability, the types of data identified for processing, the establishment of a regulatory authority, and the inclusion of consent in the law or bill. Details here.

Definitions: The variable assesses the presence and clarity of definitions in data privacy laws, including data controller, data processor, personal data, sensitive data, health data, biometric data, and pseudonymization. This assessment is based on an evaluation of whether these terms are explicitly defined, referenced through other terms, or lack a clear interpretation. Details here.

Controller and processor obligations: The variable assesses data handling obligations, including data localization requirements, offshore data transfer measures, record-keeping duties, breach notification obligations, data retention timeframes, and rules for handling children's data. Details here.

Individual rights: The variable assesses the individual rights of data subjects in data privacy laws, which include the right to nominate, access, rectify, erase, object, and ensure portability. The assessment is based on an evaluation of whether these rights are explicitly defined, linked to other rights in draft stages, or lack clarity in explanation. Details here.

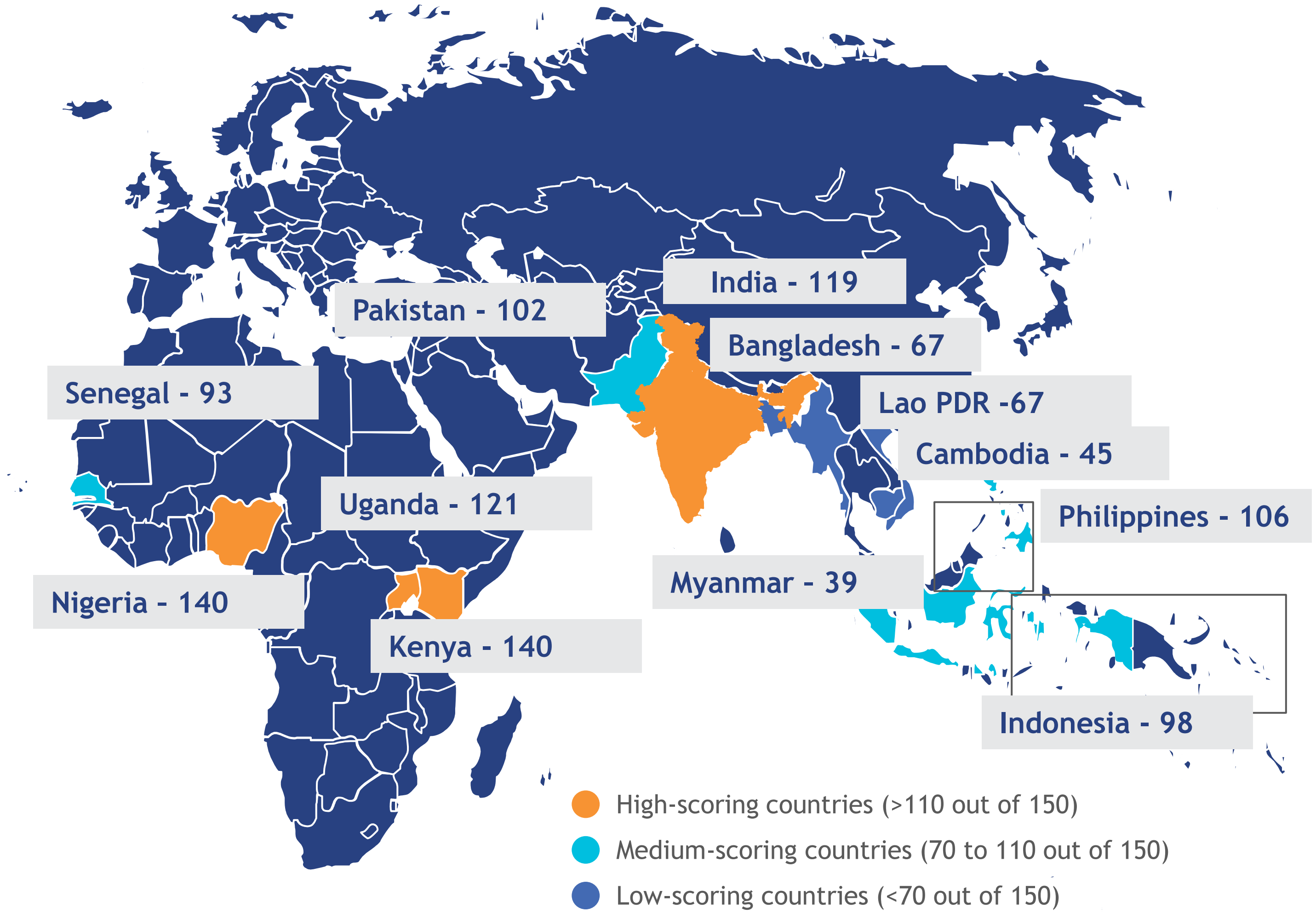
Our assessment framework outlines key variables essential for a thorough assessment of data protection policies, regulations, and enforcement across jurisdictions (2/2)

Penalties and enforcement: The variable assesses penalties and enforcement in data privacy laws, including the strictness of penalties for violations and the status of law enforcement within the jurisdiction. Details here.

Stakeholder participation: The variable assesses stakeholder participation in data privacy, including contributions from private players, government programs for awareness, and donor aid for initiatives in the data privacy space. Details here.

Data privacy intervention for consumers: The variable assesses consumer-focused data privacy efforts, including awareness campaigns and the development of solutions to address data privacy issues.

While data protection guidelines are evolving in many countries*, significant gaps persist in their implementation and enforcement.



The scores presented here are derived from our assessment of the respective data protection laws using the framework as a reference.

*The selected countries from the Global South reflect a range of data protection challenges and are particularly vulnerable to privacy risks, driven by rapid digitization in the context of evolving regulatory environments and emerging institutional capacities.

- **Strengthening regulatory alignment:** Countries, such as India, Indonesia, the Philippines, Kenya, and Uganda, are progressively aligning their data protection regimes with global benchmarks, such as the GDPR. These efforts include the introduction of stricter compliance obligations, mandatory breach notifications, and enhanced enforcement mechanisms to bolster data governance and user trust.
- **Persistent gaps and implementation barriers:** Several countries struggle when they seek to enforce data protection frameworks. These nations include Bangladesh, Pakistan, Senegal, and Uganda. Bangladesh's draft legislation lacks provisions for individual data rights; Pakistan's regulatory progress has stalled; while Senegal's mandates for breach notifications remain weak, which reflects broader challenges in legal comprehensiveness and stakeholder engagement.
- **Evolving compliance landscapes and business implications:** Regulatory shifts have been reshaping operational norms for businesses. Bangladesh has eased data localization requirements but also introduced steeper penalties for violations. India's draft Digital Personal Data Protection (DPDP) Rules 2025 allow data transfers to designated jurisdictions. Yet, they also impose more stringent data processing standards and sector-specific obligations, which have intensified the compliance burden for enterprises.

Best practices around data protection across developed countries

US data protection laws

- The US lacks a single national privacy law and relies on a mix of federal sector-specific laws and state-level regulations. A set of laws shapes this decentralized model. These laws include HIPAA, GLBA, and COPPA at the federal level, alongside comprehensive state laws, such as California's CCPA/CPRA and similar laws in more than a dozen other states.
- Key best practices in U.S. data protection include granting consumers rights to access, delete, and correct their data; conducting mandatory privacy risk assessments and cybersecurity audits; and enforcing rules through dedicated agencies, such as the FTC and California Privacy Protection Agency. States, such as California, have introduced centralized deletion tools (e.g., the Delete Act) and strict rules for data brokers. The nation has also emphasized the protection of children's data, biometric data (e.g., Illinois BIPA), and consumer health data (e.g., Washington's MHMD Act).

UK data protection laws

- The UK's GDPR and Data Protection Act 2018 together form the country's primary data protection framework. The UK's GDPR largely aligns with the EU's GDPR. However, best practices in the UK include provisions to ensure data is processed lawfully and transparently, uphold strong individual rights, such as access and erasure, conduct Data Protection Impact Assessments (DPIAs) for high-risk processing, maintain clear records of processing activities, and report data breaches promptly. The Information Commissioner's Office (ICO) oversees enforcement and provides detailed guidance to support compliance.

Japan

- The Act on the Protection of Personal Information (APPI) is Japan's main data protection law, enforced by the Personal Information Protection Commission. Best practices include clear purpose specification, consent for data use and sharing, strict rules for cross-border transfers, strong security controls, and mandatory breach notifications. The law also promotes transparency and regulates the processing of anonymized and pseudonymized data for safer handling.

Singapore

- **Singapore:** The Personal Data Protection Act (PDPA) of Singapore applies to identifiable data about individuals and excludes business contact details used solely for work. While it does not define sensitive data, the regulator advises stronger safeguards for information, such as health, financial, and children's data. Best practices include limited use, encryption, and strict controls on national ID data to reduce risk and ensure higher protection where harm from disclosure is significant.

Landmark global judgements on data protection

Nigeria: Fidelity Bank fined for data privacy violations

- In August 2024, Nigeria’s Data Protection Commission (NDPC) fined Fidelity Bank NGN 555.8 million (USD 358,580) for violating data privacy laws. The fine, which represents 0.1% of the bank’s 2023 annual revenue, is the largest issued by the NDPC so far. This action highlights the growing enforcement of data protection regulations in Nigeria.
- The NDPC found that Fidelity Bank had collected personal data from customers during the account opening process without obtaining proper consent. Additionally, the bank was accused of using non-compliant tools, such as cookies and banking applications, which processed personal data without informing users. These violations led to an initial fine of NGN 250 million, which was later increased to NGN 555.8 million.
- Fidelity Bank denied any wrongdoing and stated that the account opening process was never completed and no data breach occurred. Despite this, the NDPC upheld the fine, emphasizing the need for businesses to comply with Nigeria’s data protection laws. This case sets a precedent for stricter enforcement of data privacy regulations in the country.

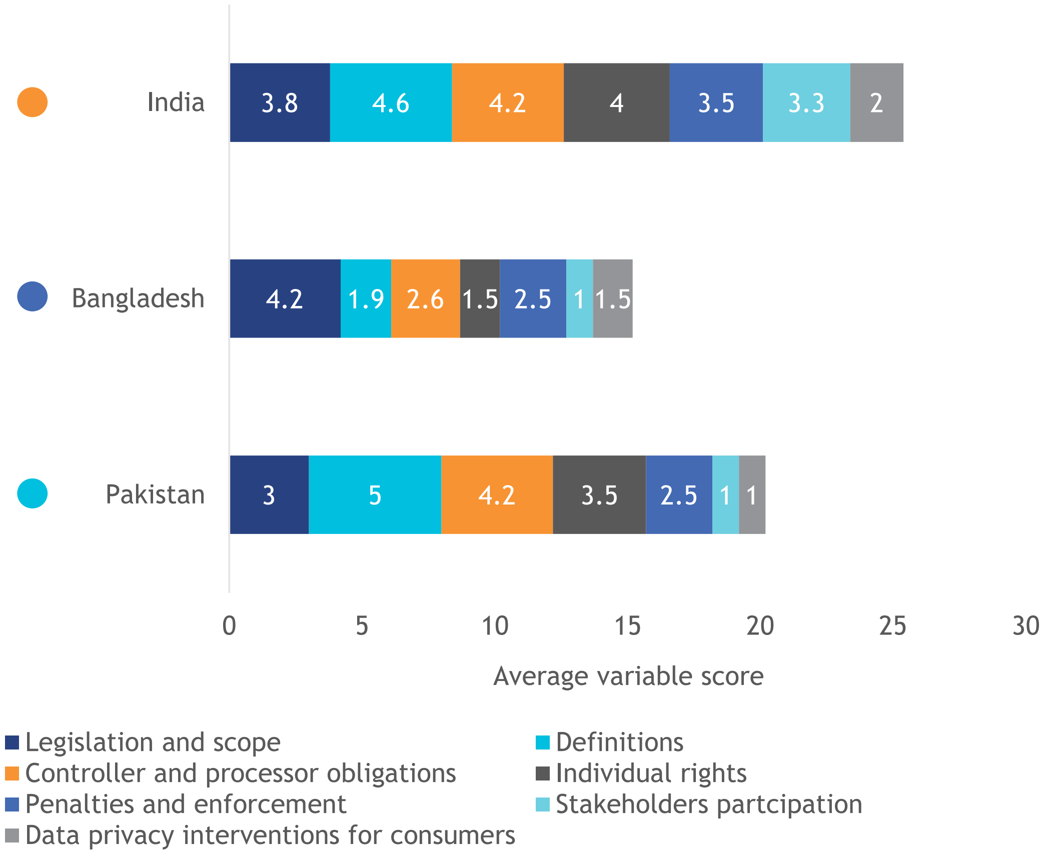
Kenya: WPP Scangroup Case

- In October 2024, WPP Scangroup, a subsidiary of the global marketing firm WPP, was fined KES 1.95 million (approximately GBP 11,600). This penalty was imposed by Kenya’s Office of the Data Protection Commissioner (ODPC) for failing to comply with the Data Protection Act. The case highlights the increasing enforcement of data privacy laws in Kenya and the consequences of non-compliance.
- The case centered around allegations by Bharat Thakrar, the former CEO of WPP Scangroup, who claimed that his personal data was accessed without his consent. This occurred during an internal investigation and raised concerns about the improper handling of sensitive employee data. Unauthorized access to personal data directly violates data protection regulations, emphasizing the need for strict compliance.
- The ODPC found that WPP Scangroup had failed to obtain proper consent before accessing Thakrar’s personal data. Additionally, the company did not provide him with the requested investigation reports, further breaching legal requirements. As a result, the ODPC imposed a fine, which reinforced the importance of transparency and accountability in handling personal data.

Region-specific analysis

South Asia: India leads regarding data protection policies with proactive legislation, extensive stakeholder consultations, and detailed draft rules compared to Bangladesh and Pakistan’s slow regulatory advancements.

Average score* across seven parameters in South Asia



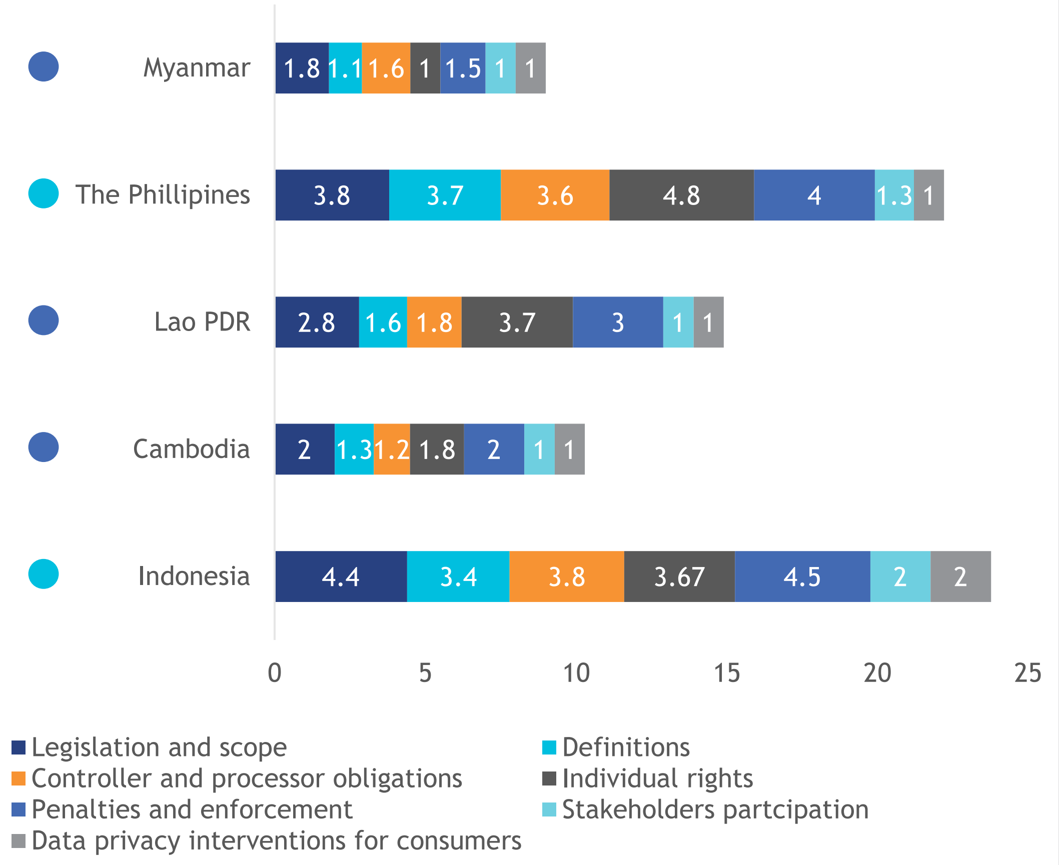
* The scores are the average of the variable after summing up the individual sub-variables from the value of 1 to 5. For the complete scoring matrix, refer to the annex.

Key insights

- India’s Digital Personal Data Protection (DPDP) Draft Rules 2025 propose regulations on cross-border data transfers and place compliance obligations on multinational companies. While it permits transfers to approved jurisdictions, stringent processing norms and sector-specific restrictions could add to operational complexities and increase the cost to manage data consent within India.
- The recent draft of the Cybersecurity Act of Bangladesh (draft), along with the **2023 Baseline Study on National Data Governance**, has significantly relaxed data protection laws. However, while specific regulations on data transfers remain in place, penalties for non-compliance have increased. At the same time, reduced data localization requirements have heightened the risk of data leakages.
- Both **Bangladesh** and **Pakistan** face significant challenges in the development of robust data protection frameworks. Bangladesh’s current draft lacks provisions for individual rights, which poses a serious risk to personal data security. Meanwhile, Pakistan has made little progress, with no substantial updates since its initial draft, which highlights ongoing delays. Additionally, both countries lag in stakeholder participation, which further hinders the development of comprehensive and effective data protection regulations.

South-East Asia: Indonesia and the Philippines have comprehensive data protection laws, while Cambodia, Lao PDR, and Myanmar rely on fragmented, sector-specific regulations for privacy safeguards.

Average score* across seven parameters in South-East Asia



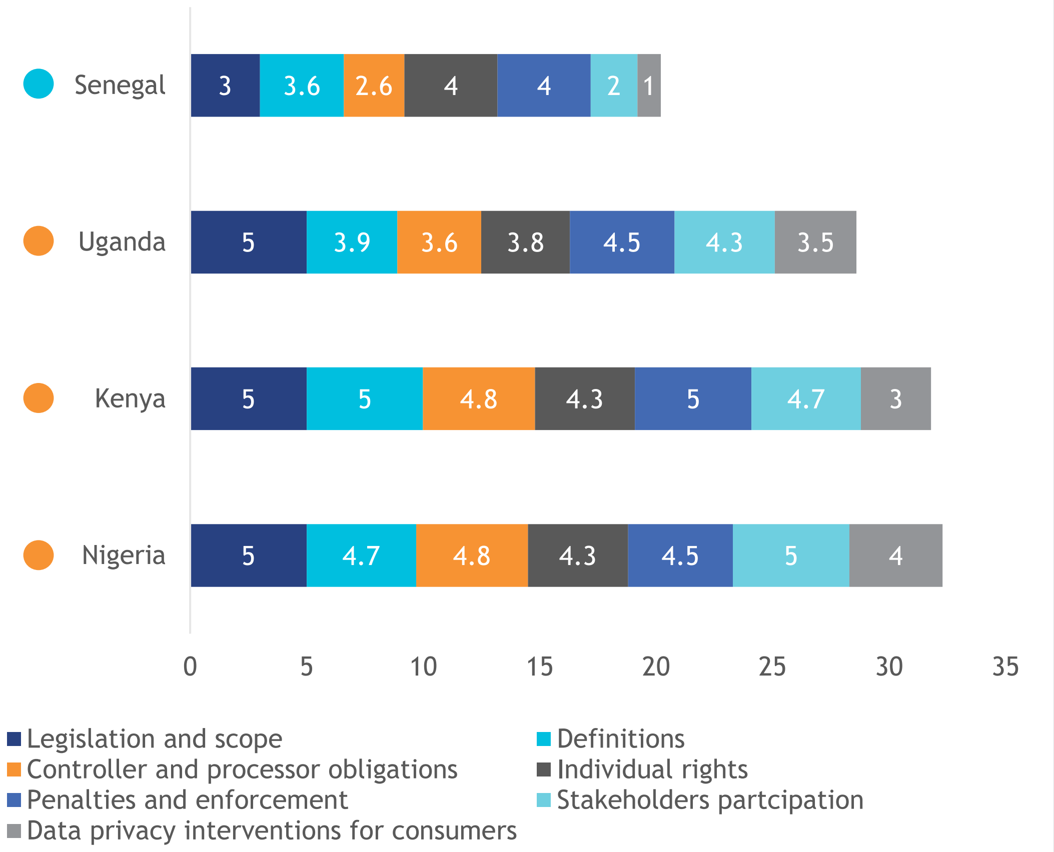
* The scores are the average of the variable after summing up the individual sub-variables from the value of 1 to 5. For the complete scoring matrix, refer to the annex.

Key insights

- Indonesia and the Philippines have aligned their data protection regulations with global standards, influenced by **GDPR principles**—Indonesia through its **Personal Data Protection Law (PDPL) 2022** and the Philippines via its **Data Privacy Act 2012**. In contrast, several countries in the region lack such internationally recognized frameworks.
- Indonesia's **PDPL** is now fully enforced and now requires organizations to notify data subjects of any **data breaches within three days**. Additionally, the law mandates that if individuals request data erasure for a legitimate reason, controllers must **permanently delete or destroy** the data across all storage locations.
- Similarly, **the Philippines** has recently introduced amendments to its **Data Privacy Act**, which aligns its data breach regulations with those of **Indonesia**. One of these amendments has refined the definition of **sensitive data** and strengthened enforcement through **higher fines and longer imprisonment** for violations of data protection laws.
- In contrast, **Cambodia, Lao PDR, and Myanmar** regulate privacy through **sector-specific laws**, such as those governing banking and healthcare. In contrast, **Indonesia and the Philippines** have implemented **comprehensive data protection frameworks** that extend across multiple sectors.

Sub-Saharan Africa: Nigeria with NDPR and Kenya with DPA have strong data protection laws whereas Senegal, and Uganda are still in the process of strengthening their data protection frameworks.

Average score* across seven parameters in Africa



Key insights

- Kenya and Uganda have data protection regulations that align closely with **GDPR**. Meanwhile, Nigeria has adopted a partial alignment, and Senegal is still adapting to global data protection standards.
- **Nigeria, Kenya, and Uganda** have active regulatory bodies that enforce compliance, though Uganda is still strengthening its oversight mechanisms. **Conversely, Senegal** has a dedicated regulatory authority, the **Commission for Protection of Personal Data (CDP)**. It comprises **11 members** but remains a **temporary** regulatory body.
- All four countries impose penalties for non-compliance with data protection regulations, with **Nigeria enforcing the highest fines**. However, Uganda's enforcement mechanisms are still evolving under its **2019 Data Protection and Privacy Act**.
- Senegal lacks a **mandatory data breach notification** requirement for data subjects, and stakeholder participation remains limited due to the **scarcity of private sector involvement** in data protection discussions.

* The scores are the average of the variable after summing up the individual sub-variables from the value of 1 to 5. For the complete scoring matrix, refer to the annex.

What this landscape indicates

Stakeholders have an opportunity to strengthen data protection and regulatory ecosystem across different country categories.

● High scoring countries (>110): Nigeria, Kenya, Uganda, India

- **Refine sensitive data protection:** Clearly define sensitive personal data, including traditional and emerging types (e.g., biometrics, wearables, telemedicine), and ensure protection across public and private entities, aligned with global best practices
- **Strengthen enforcement and representation:** Establish standardized penalty criteria for transparency and compliance; amend laws to grant individuals the right to appoint representatives to exercise data rights, which would ensure accountability and accessibility
- **Enhance compliance and public awareness:** Encourage private sector participation in data protection, implement large-scale awareness campaigns, and mandate training programs to improve adherence, empower individuals, and reinforce privacy safeguards

● Medium scoring countries (70-110): The Philippines, Pakistan, Indonesia, Senegal

- **Strengthen oversight and governance:** Establish an independent Data Protection Authority (DPA) with enforcement powers to oversee government data practices, regulate security laws, and set guidelines for cross-border data transfers while ensuring financial and operational autonomy
- **Enhance compliance and accountability:** Implement a structured penalty system with fines scaled to breach severity, introduce standardized transfer mechanisms, such as binding corporate rules, and standard contractual clauses; define national security exemptions with strict criteria and periodic reviews for transparency
- **Ensure secure and interoperable data ecosystems:** Develop robust cloud policies, data interoperability frameworks, and security laws tailored to different data categories, to ensure privacy and facilitate seamless and secure data exchange

● Low-scoring countries (<70): Lao PDR, Myanmar, Cambodia, Bangladesh

- **Enact a dedicated data protection law:** Establish a comprehensive data protection regulation aligned with global standards to ensure clear definitions, enforcement mechanisms, and safeguards for personal data
- **Strengthen oversight and governance:** Create an independent Data Protection Authority (DPA) with enforcement powers, mandate DPIAs for high-risk processing, and engage stakeholders to address regional concerns
- **Enhance compliance and security:** Implement breach notification rules, cross-border data transfer regulations, privacy-by-design principles, and strict penalties, and assess economic and societal impacts before finalization
- **Improve digital infrastructure and security measures:** Develop cybersecurity frameworks, promote secure data storage solutions, and invest in technological infrastructure to ensure data resilience and prevent breaches

Annex 1: Assessment framework details

Legislation and scope

Law

Indicates the presence of a basic law framework related to data privacy and identity privacy

Geographical territory

Measures the territorial scope and clarity of the applicability of data privacy laws across different geographical regions

Material

Measures the types of data identified in the law for processing and the specified methods, whether manual or automated

Authority

Measures the establishment and presence of a regulatory authority within the data privacy law

Consent

Measures the inclusion of consent, defined as a freely given, specific, and informed agreement to data collection or processing

Definition

Data controller

Refers to a natural or legal person, public authority, agency, or body that determines the purposes and means of processing personal data

Data processor

A natural or legal person, public authority, agency, or body that processes personal data on behalf of the controller

Personal data

Assesses the specific mention and explanation of laws related to personal data

Sensitive data

Evaluates whether the law explicitly defines sensitive data as confidential information accessible only to authorized users

Health data

Covers data on an individual’s physical or mental health, including medical records and information linked to health services

Biometric data

Includes personal data derived from the technical processing of physical, physiological, or behavioral traits, such as fingerprints, DNA, and retinal scans

Pseudonymization

Refers to processing personal data in a way that prevents identification without additional, separately stored information secured by technical and organizational measures

Controller and processor obligations

Data transfer

Measures the extent of data localization requirements, including regulations on data transfer and access by offshore entities, favoring complete localization

Data processing

Measures the requirement for entities to maintain data processing records and provide them to authorities upon request

Breach notification

Measures the obligation to inform data subjects about breaches and the authority's responsibility to notify affected individuals

Data retention

Measures the presence of a data retention timeframe and whether processors are required to delete data after a specified period

Children's data

Measures the presence of regulations or guidelines issued by authorities for handling minors' and children's data

Individual rights

Nominate

Checks whether the law allows data ownership transfer in the event of the data subject's death or unavailability

Access

Checks if data subjects have the right to access their personal data in a structured format and transfer it to another controller without restrictions

Rectification

Checks whether data subjects have the right to be notified by the controller when their data is rectified

Erasure

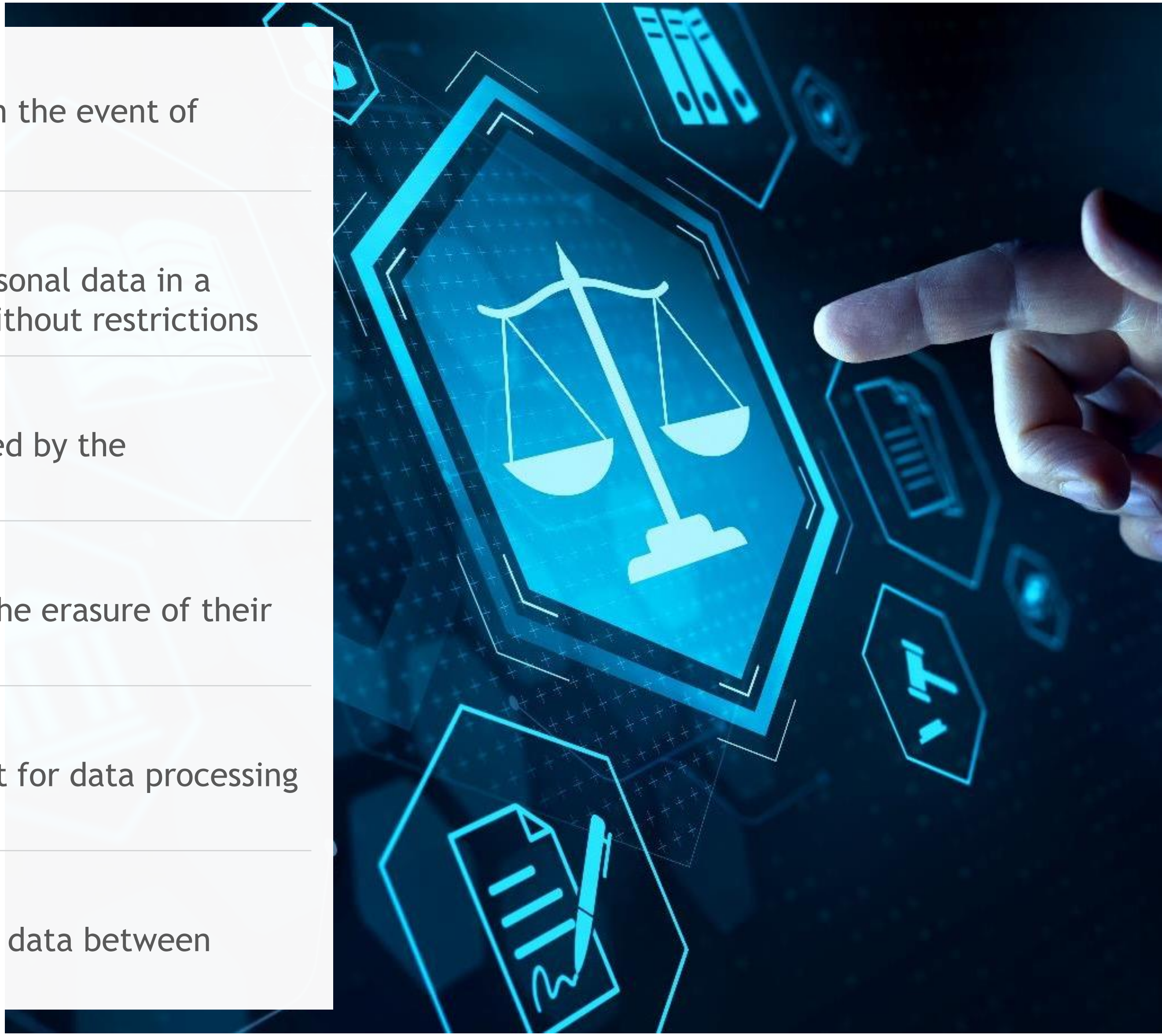
Checks whether data subjects have the right to request the erasure of their personal data

Object

Checks whether data subjects can withdraw their consent for data processing at any time

Portability

Checks whether data subjects can transfer their personal data between controllers without restrictions



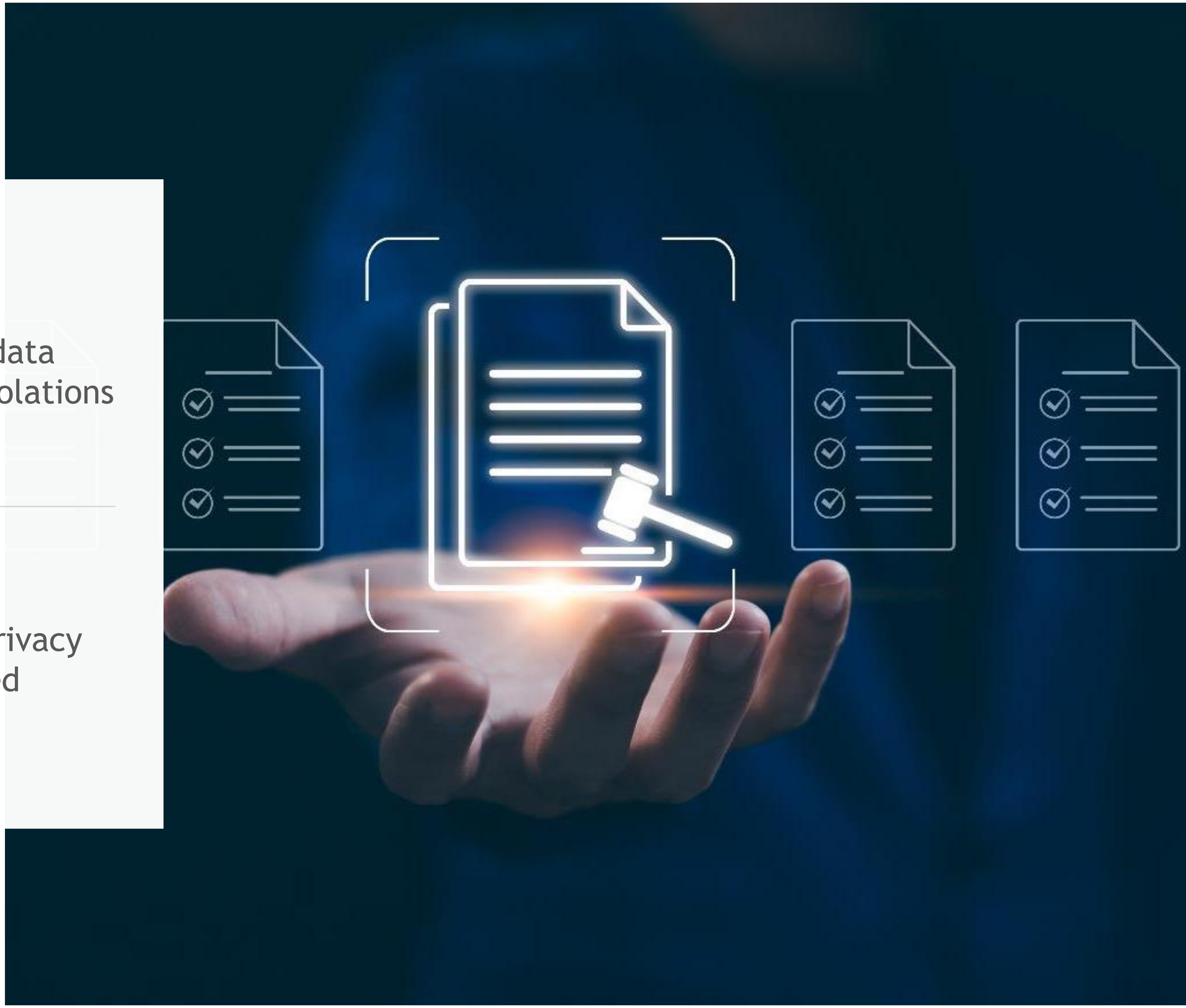
Penalties and enforcement

Penalty

Measures the strictness and enforcement of penalties in data privacy law, assessing the severity of consequences for violations and non-compliance

Enforcement

Evaluates the implementation status of dedicated data privacy laws, assessing whether they have been officially enforced within the jurisdiction



Stakeholders’ participation

Private players

Assesses the role private entities play to raise awareness and promote the importance of data privacy

Government programs

Evaluates government initiatives and programs that seek to raise awareness of the importance of data privacy

Donors’ aid

Assesses the support and funding provided by donors for initiatives and projects in the data privacy sector

Data privacy interventions for consumers

Event or campaign

Evaluates the existence of events or campaigns that seek to raise awareness of data privacy

Solution development

Assesses the development of solutions that seek to address data privacy challenges

Annex 2: Scoring matrix and judgement examples

Annex

Parameter	Score	Explanation
1. Legislation and scope		
Presence of data privacy law - Indicates the presence of basic law framework related to data Privacy and privacy.	1	There is an absolute absence of data privacy law in all forms and all spaces.
	2	There is no law dedicated to data privacy but some sectors have their own specific laws and provisions.
	3	The dedicated data privacy laws are still in the draft stage and has not been enacted in the country.
	4	There is a dedicated data privacy law, but the notification has not been issued, and the provisions are still on paper.
	5	There is a fully enforced data privacy law.
Clarity on the applicability of data privacy law across geographical territory - Indicates the presence of basic law framework related to data Privacy and privacy.	1	There is no mention about the applicability of the law in the geographical area of the country and beyond.
	2	The law is applicable only within the own country geographical territory
	3	There is a mention of territorial/geographical scope but since the laws are in a draft stage so no clear evidence of application
	4	The application of the law is on the data of own citizens whether it is in their own geographical territory or outside, but lacks some clarity.
	5	The law clearly mentions the forms of data eligible for processing i.e. manual and digital
Forms of data identified in the law for processing - Measures the provisions related to territorial application	1	There is no mention of the forms of data that can be processed.
	2	The law does not identify the digitalization of manual data for processing
	3	The identification of manual as well as digital data for processing is in draft stage
	4	Lacks clarity on the use of manual data in processing
	5	The law clearly mentions the forms of data eligible for processing i.e. manual and digital

Annex

Parameter	Score	Explanation
1. Legislation and scope		
Establishment of a regulatory authority - Measures the method of processing the data, i.e., in manual or automated means.	1	There exists no designated authority for the regulation of data protection
	2	The regulatory body functions are not defined or clear and no significant impact can be seen
	3	The authority is proposed but not functional yet
	4	Any existing authority has been assigned the task of acting temporarily as data protection authority
	5	There exists an independent authority that is responsible for regulation and is functional
Presence of the concept of consent in law - Captures the concept of consent - Any freely given, specific, informed, and unambiguous indication of the data subject's wish which they, by a statement or by a clear affirmative action, signifies agreement to the collection or processing of personal data relating to them.	1	There is no mention of consent in law
	2	Consent has not been mentioned clearly but some sense of consent can be observed
	3	Consent has been mentioned but not functional yet
	4	Consent needs to be defined more clearly
	5	Consent is clearly defined and the concept is functional
2. Definition		
Data Controller - “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data	1	There is no mention of the term in the official text for data privacy
	2	The context is available, but it is not clearly mentioned
	3	The term draws its definition from other terms that are defined.
	4	The definition is not clear and easy to interpret
	5	The term is clearly defined and explicitly mentioned in the official text.

Annex

Parameter	Score	Explanation
2. Definition		
Data processor- “Processor” means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller	1	There is no mention of the term in the official text for data privacy
	2	The context is available, but it is not clearly mentioned
	3	The term draws its definition from other terms that are defined.
	4	The definition is not clear and easy to interpret
	5	The term is clearly defined and mentioned specifically in the official text
Personal data - Measures the specific mention and explanation of laws related to Personal Data	1	There is no mention of the term in the official text for data privacy
	2	The context is available, but it is not clearly mentioned
	3	The term draws its definition from other terms that are defined.
	4	The definition is not clear and easy to interpret
	5	The term is clearly defined and mentioned specifically in the official text
Sensitive data - Checks if the law defines "Sensitive Data " specifically- Sensitive data is information stored, processed, or managed by an individual or organization that is confidential and only accessible to authorized users with proper permission, privileges, or clearance to view it.	1	There is no mention of the term in the official text for data privacy
	2	The context is available, but it is not clearly mentioned
	3	The term draws its definition from other terms that are defined.
	4	The definition is not clear and easy to interpret
	5	The term is clearly defined and mentioned specifically in the official text
Health data - Implies data related to the state of physical or mental health of the data subject, and includes records regarding the past, present, or future state of the health, data collected during registration for, or provision of, health services, or data which associates the data subject to the provision of specific health services.	1	There is no mention of the term in the official text for data privacy
	2	The context is available, but it is not clearly mentioned
	3	The term draws its definition from other terms that are defined.
	4	The definition is not clear and easy to interpret
	5	The term is clearly defined and mentioned specifically in the official text

Annex

Parameter	Score	Explanation
2. Definition		
Biometric data - Implies any personal data resulting from specific technical processing based on physical, physiological, or behavioral characterization, including blood typing, fingerprinting, DNA analysis, earlobe geometry, retinal scanning, and voice recognition.	1	There is no mention of the term in the official text for data privacy
	2	The context is available, but it is not clearly mentioned
	3	The term draws its definition from other terms that are defined.
	4	The definition is not clear and easy to interpret
	5	The term is clearly defined and mentioned specifically in the official text
Pseudonymization - The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person	1	There is no mention of the term in the official text for data privacy
	2	The context is available, but it is not clearly mentioned
	3	The term draws its definition from other terms that are defined.
	4	The definition is not clear and easy to interpret
	5	The term is clearly defined and mentioned specifically in the official text
3. Controller and Processor Obligations		
Extent of data localization as per the law - Measures the transfer of data and access to offshore entities. It is best suited if there is complete data localization	1	There exists no rules regarding localization of the data
	2	There are some sector specific rules for localization of data
	3	The rules for data localization are in the draft stage
	4	Transfer of data can take place with the permission of the apex authority
	5	There exists complete data localization and no data can be transferred to another country for processing

Annex

Parameter	Score	Explanation
3. Controller and Processor Obligations		
Provision of maintaining data processing records - Means that if the entity maintains the processed data record, it could provide this to the authority when asked	1	There is no obligation on controller for maintaining data processing records
	2	There are some sector specific obligations for data audits and keeping data processing records
	3	The rules related to data processing records are in draft stage
	4	It is the duty of data controller to inform the data subject in case of their data breach
	5	It is the duty of data controller to inform the data subject in case of their data breach within a stipulated time period
Obligation to inform data subject about data breach - Measures if the authority is liable to inform the data principal about the data breach	1	There is no provision for informing the data subject in case of data breach
	2	There exists an obligation on the data controller to inform the authority and coordinate with them, but not to the data subject.
	3	The rules regarding informing the data subject in case of data breach is in draft stage
	4	It is the duty of data controller to inform the data subject in case of their data breach
	5	It is the duty of data controller to inform the data subject in case of their data breach within a stipulated time period
Presence of data retention timeframe - Measures if the data processor is asked to remove data after a fixed interval of time	1	There is no obligation on controller/ processor for abiding the rule of deleting data after a fixed interval of time.
	2	There are some sector specific obligations for deleting data after a fixed interval of time.
	3	The rules related to deletion of data after a fixed time interval are in draft stage
	4	There are rules defined for storing / deleting data for a time interval but there is a lack of clarity
	5	There exists fully enforced rule for storing and deleting data in a timeframe

Annex

Parameter	Score	Explanation
3. Controller and Processor Obligations		
Rules for handling children's data - Measures if the authority has ordered or if there are any guidelines specifically related to the data of minors and children	1	There is no rule for handling data related to children
	2	There are some sectors only that follow a guideline for dealing with children's data
	3	The rules for handling children's data are in draft stage
	4	Lacks some clarity on the use of children's data in processing
	5	The rules are clearly defined for the processing of children's data
4. Individuals' rights provided to data subjects		
Right to nominate - If the law permits the transfer of ownership of the data in case of death or unavailability of the data subject.	1	The law does not mention any individual rights for data subjects
	2	Explanation to the rights provided lacks clarity
	3	Individual rights of the data subject are in draft stage
	4	The rights are not explicitly explained but can be found in linkage with other rights
	5	The rights of the data subjects are explicitly mentioned with clear explanation
Right to access - A data subject has the right to receive the personal data concerning them, which they have provided to a data controller, in a structured, commonly used and machine-readable format, and have the right to transmit that data to another data controller without hindrance from the data controller to which the personal data has been provided	1	The law does not mention any individual rights for data subjects
	2	Explanation to the rights provided lacks clarity
	3	Individual rights of the data subject are in draft stage
	4	The rights are not explicitly explained but can be found in linkage with other rights
	5	The rights of the data subjects are explicitly mentioned with clear explanation

Annex

Parameter	Score	Explanation
4. Individuals' Rights provided to Data Subjects		
Right to rectification - A data subject has the right to be notified by the data controller of the rectification of data	1	The law does not mention any individual rights for data subjects
	2	Explanation to the rights provided lacks clarity
	3	Individual rights of the data subject are in draft stage
	4	The rights are not explicitly explained but can be found in linkage with other rights
	5	The rights of the data subjects are explicitly mentioned with clear explanation
Right to erasure - A data subject has the right to the erasure of their personal data	1	The law does not mention any individual rights for data subjects
	2	Explanation to the rights provided lacks clarity
	3	Individual rights of the data subject are in draft stage
	4	The rights are not explicitly explained but can be found in linkage with other rights
	5	The rights of the data subjects are explicitly mentioned with clear explanation
Right to object - A data subject has the right to withdraw their consent to the processing of their personal data at any time	1	The law does not mention any individual rights for data subjects
	2	Explanation to the rights provided lacks clarity
	3	Individual rights of the data subject are in draft stage
	4	The rights are not explicitly explained but can be found in linkage with other rights
	5	The rights of the data subjects are explicitly mentioned with clear explanation
Right to portability - A data subject has the right to transmit personal data from one data controller to another without hindrance from the data controller	1	The law does not mention any individual rights for data subjects
	2	Explanation to the rights provided lacks clarity
	3	Individual rights of the data subject are in draft stage
	4	The rights are not explicitly explained but can be found in linkage with other rights
	5	The rights of the data subjects are explicitly mentioned with clear explanation

Annex

Parameter	Score	Explanation
5. Penalties and enforcement		
Intensity of provision for penalty in the data privacy law - Measures the strictness in the penalty system for offenders of the data privacy law	1	There is no provision for penalty in data privacy law
	2	There are warnings issued to the offender and no provision for monetary penalty
	3	Provision for monetary penalties are subject to change as the law is in draft stage
	4	There is fixed penalty for all the types of data privacy related crimes
	5	There is clearly defined penalty system for the data privacy offender
Status of enforcement of the dedicated data privacy law	1	There is complete absence of data privacy law
	2	There are some sectoral laws that capture some aspects of data privacy
	3	The data privacy dedicated law is in draft stage and are subject to changes
	4	The law has been made but still the notification for enforcement are await
	5	The law is fully enforced and functional
6. Stakeholder participation		
Private players' contribution to sensitizing the need for data privacy	1	There is complete absence of private players in sensitizing the need for data privacy
	2	There have been little effort by the private players for addressing this concern
	3	Some autonomous institutions are working to creating awareness about data privacy
	4	Some private players are identified but the impact of their programs are unknown
	5	There are major private players for sensitizing the issue of data privacy to the masses
Government programs for sensitizing the need for data privacy	1	There is complete absence of government in sensitizing the need for data privacy
	2	There have been little effort by the government for addressing this concern
	3	Some government-funded institutions are working to create awareness on data privacy
	4	Government programs are identified, but the impact of their programs are unknown
	5	Government is actively working for sensitizing the issue of data privacy to the masses

Annex

Parameter	Score	Explanation
6. Stakeholder Participation		
Donor aid for working in the data privacy space	1	There is complete absence of donors in data privacy related space
	2	There have been little effort by donors for addressing this concern
	3	Some donor institutions are working to creating awareness about data privacy
	4	Donors' participation are identified but the impact of their programs are unknown
	5	There is a major presence of donors, actively working to sensitize the issue of data privacy to the masses and in solution development
7. Data Privacy Interventions for Consumers		
Presence of Event/Campaign for Creating Awareness about Data Privacy	1	No events or campaigns have been identified to create awareness on data privacy
	2	Some events or campaigns are identified but details are missing to assess what it aimed at
	3	Events or campaigns for data privacy are identified on a small scale
	4	There are some events or campaigns organized, but their impact is unknown
	5	There are active running and impactful campaign for addressing the awareness about data privacy with suitable impact
Solution Development to Deal with Data Privacy Issues	1	There has been no identifiable work for solution development to deal with data privacy issues
	2	There exists some solution development tools but have not been used yet for addressing data privacy issues
	3	Some software or AI systems have been identified, but their impact is unknown
	4	Some solution development tools have been assigned projects to address data privacy concerns
	5	A robust solution development system has been developed and is actively working to deal with data privacy problems

```
#include <stdint.h>
int main(int argc, char **argv) {
        int64_t src = argc;
        int64_t dst;
        __asm__ volatile(
                "lzcnt %1, %0\n"
                :"=r"(dst)
                :"r"(src)
                :"cc"
   ;
   turn (int)dst;
```

Annex 3: Limitations of the study

MSC

A score-based study to assess the data protection landscape in developing countries across Asia and Africa has probable limitations

Subjectivity in scoring and weightage challenges

- Despite using a global benchmark, assigning scores (1 to 5) to variables inherently involves some level of subjective judgment, which can lead to biases.
- Additionally, determining the appropriate weightage for draft regulations versus enacted laws is challenging, as some drafts may be close to implementation while others remain stagnant for years.

Contextual & geopolitical factors, including external influences

- Geopolitical, cultural, and governance-related factors influence data protection enforcement but are challenging to quantify. The study may not fully capture the political will or government intentions behind regulations.
- Additionally, external forces such as global organizations, multinational corporations, and foreign policies shape data protection regimes, which may not be accurately reflected in a simple score-based assessment.

Implementation vs. Existence of Law

- A country may have strong data protection laws, but enforcement mechanisms and institutional capacity can be weak. The study may not adequately reflect ground-level realities, where regulatory oversight, institutional strength, and political commitment determine actual compliance and enforcement.

Comparability Issues

- Countries differ in legal traditions, economic development, and regulatory maturity. Applying a uniform scoring system may not account for variations in enforcement structures and institutional capacities. Some countries may have sectoral or decentralized approaches to data protection that do not fit neatly into a singular scoring framework.

Evolving Nature of Data Protection Laws & lack of granular enforcement data

- Data protection laws continuously evolve, with frequent amendments that may quickly render scoring assessments outdated.
- Additionally, reliable enforcement data—such as fines, regulatory audits, and citizen complaints—remains scarce, making it challenging to assess real-world compliance levels accurately.

Acknowledgement

Lead authors*	Vineet Anand | Surbhi Sood | Shrabasti Dhar
Contributing authors*	Brenda Awuor Oyugi | Nabilla Prita Fiandini | Suardi Ihsan | Jyoti Shishodia | Ihsan Mahboob Hoq | Md. Tanvir Quader | Gregory Emeka Ilukwe | Debarshi Chakraborty
Reviewer	Akhand Tiwari
Copy-edit and design	Rahul Ganguly | Kamiya Satija | Nikhil Sati

*Authors belong to multiple country offices of MSC including Kenya, Bangladesh, Indonesia, and India

Sectors we work in

Providing impact-oriented business consulting services

- Banking, financial services, and insurance (BFSI)
- Water, sanitation, and hygiene (WASH)
- Government and regulators
- Micro, small, and medium enterprise (MSME)
- Social payments and refugees
- Youth
- Gender equality and social inclusion (GESI)
- Education and skills
- Digital and FinTech
- Agriculture and food systems
- Climate change and sustainability
- Health and nutrition

Multi-faceted expertise

Advisory that helps you succeed in a rapidly evolving market

- Policy and strategy
- Products and channels
- Research, evaluation, and analytics
- Organizational transformation
- Digital technology and channels
- Catalytic finance
- Design thinking and innovation
- Marketing and communication
- Training
- Government regulations and policy
- Data Insight
- Customer protection and engagement for responsible finance

MSC is recognized as the world's local expert in economic, social and financial inclusion

International financial, social and economic inclusion consulting firm with 25+ years of experience

>300 staff in 10 offices around the world

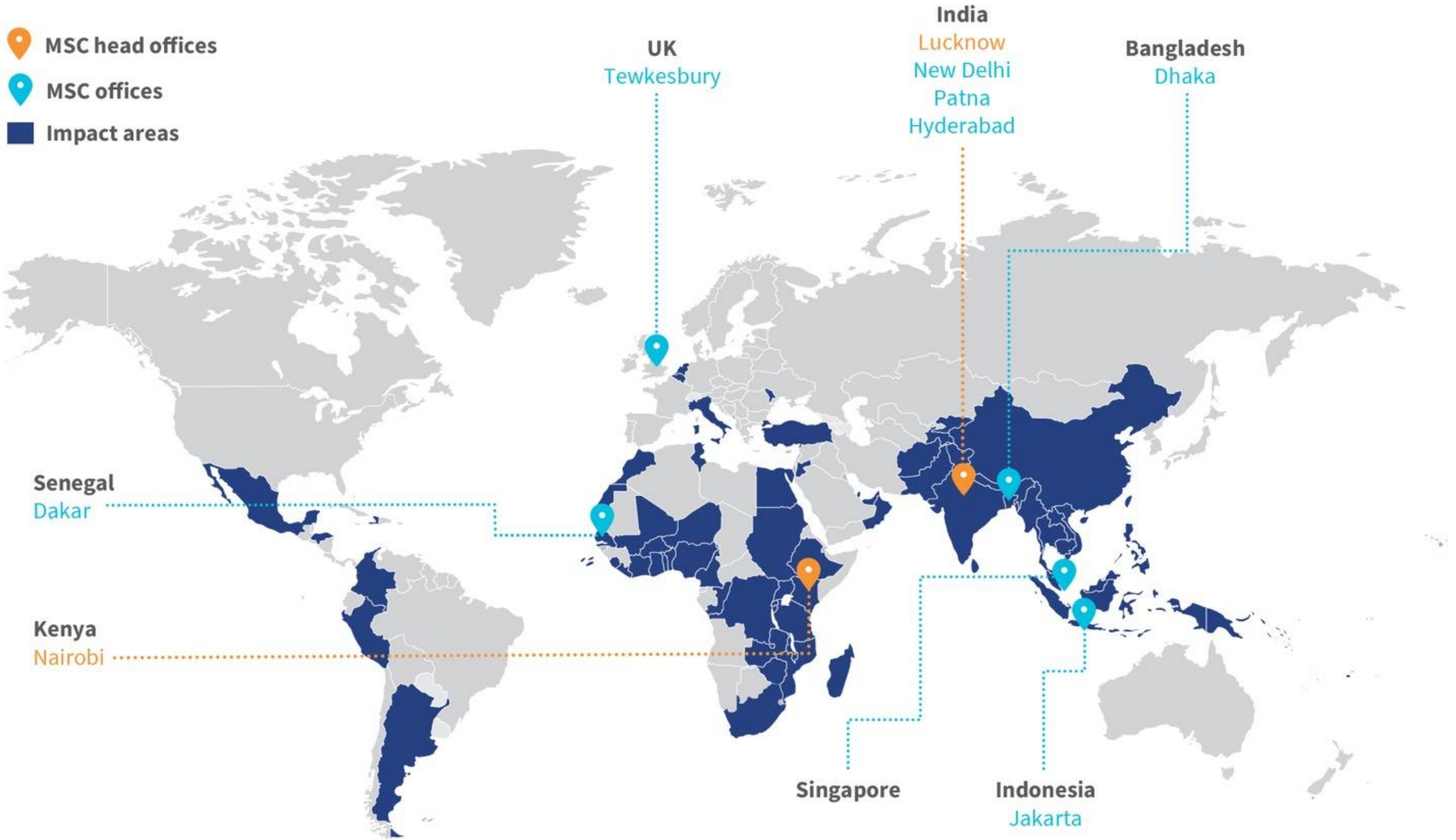
Projects in ~68 developing countries

Our impact so far

>550 clients	>1,400 publications
Assisted development of digital G2P services used by >875 million people	Implemented >950 DFS projects
Developed >300 FI products and channels now used by >1.7 billion people	Trained >11,100 leading FI specialists globally

Some of our partners and clients

- Bill & Melinda Gates foundation
- MetLife Foundation
- mastercard foundation
- IFC International Finance Corporation World Bank Group
- UNCDF
- USAID From the American People
- World Bank Group
- CGAP
- Omidyar Network
- ADB Asian Development Bank
- NPCI National Payments Corporation of India
- NITI Aayog
- dfcu Bank …with pleasure
- Equity
- Family Bank With you, for life
- FirstBank Since 1894
- Safaricom
- Centenary Bank
- m-pesa
- MTN Mobile Money
- Center for Global Development
- airtel
- vodafone
- moov no limit
- UKaid from the British people
- Michael & Susan Dell Foundation
- OJK Otoritas Jasa Keuangan
- Ecobank The Pan African Bank
- CESAG
- BURO Bangladesh
- SCBF
- avpn
- CIFAR Alliance
- Bank Asia For a better tomorrow
- BRAC Bank



MSC corporate brochure | Email: info@microsave.net | Website: www.microsave.net

Asia head office

28/35, Ground Floor, Princeton Business Park,
16 Ashok Marg, Lucknow, Uttar Pradesh, India 226001
Tel: +91-522-228-8783 | Fax: +91-522-406-3773

Africa head office

Landmark Plaza, 5th Floor, Argwings Kodhek Road
P.O. Box 76436, Yaya 00508, Nairobi, Kenya
Tel: +254-20-272-4801/272-4806

MSC

MicroSave Consulting