DATA HARMONISATION BILL

ARRANGEMENT OF SECTIONS

A BILL ENTITLED

THE DATA HARMONISATION ACT, 20XX (ACT XXXX)

AN ACT to promote data harmonisation, standardisation and exchange to enhance data governance, enable efficient public service delivery, and safeguard data rights and to provide for related matters.

DATE OF ASSENT:
PASSED by Parliament and assented to by the President:

Preliminary Matters

Application of this Act

1. (1) This Act applies to all public interest data and all holders of public interest data.

(2) Without limiting subsection (1), this Act applies to:
- (a) all public sector institutions, including ministries, departments, agencies, and statutory bodies, that collect, generate, process, store or hold public interest data;
- (b) all private sector entities that generate, collect, store, or otherwise control or process public interest data in connection with a public function, a regulatory obligation, or the provision of goods or services;
- (c) any person or institution granted access to the National Data Exchange Platform under this Act; and
- (d) any category of persons whom the Minister shall designate.

(3) This Act shall not compel the mandatory sharing of any information classified as restricted data, or any other information whose disclosure would endanger national security, defence, or public safety.

Objectives of the Act

2. The purpose of this Act is to establish a legal and institutional framework for the harmonisation, sharing and use of public interest data, through a secure data exchange infrastructure, to support efficient public administration and national development. The objectives of this Act are to:

- (a) promote coordinated and harmonised data governance across public and private institutions;
- (b) improve the quality, accessibility, interconnectedness and interoperability of public interest data;
- (c) provide the legal mandate for the sharing of public interest data;
- (d) enable the lawful and secure sharing of public interest data across institutional and sectoral boundaries;
- (e) support innovation, competition, research, and evidence-based policy making by enabling lawful access to public interest data;
- (f) protect the public from fraud, misinformation, and other risks arising from poor data management and fragmented information systems; and
- (g) ensure that public interest data is governed in accordance with national values, applicable standards, and international best practices.

Guiding Principles

3. The implementation of this Act shall be guided by the following principles:

(a) data integrity, public interest data must be consistent, accurate and reliable;
(b) data standardisation, there must be common formats, definitions and classifications used across databases to enable exchange of information and comparability;
(c) data democratisation, public interest data must be accessible and readily available for use across sectors;
(d) interoperability, systems and institutions must be able to interpret, use, and exchange data seamlessly through the appropriate standards and protocols;
(e) reusability, redundant data collection must be avoided; where applicable, the same data should be collected once only and re-used appropriately across institutions;
(f) security, access to public interest data should be as open as possible, but as closed as necessary; the right to access data must be balanced with the privacy and safety of citizens and the security of the Republic;
(g) optimisation, data sharing and system integration should support the delivery of timely, efficient and citizen-centred public services; and
(h) transparency, the collection, access and use of public interest data should be forthright and promote accountability and public trust.

Data Sharing and the National Data Exchange Platform

Establishment of the National Data Exchange Platform

4. (1) There is established by this Act the National Data Exchange Platform, a public digital infrastructure for the secure, standardised and interoperable exchange of public interest data.

(2) The National Data Exchange Platform shall operate as the central national infrastructure for the provision and exchange of public interest data held by public institutions and eligible private entities, specifically comprising open data and shareable data.

(3) The National Data Exchange Platform shall:
(a) facilitate the lawful sharing, exchange and re-use of public interest data in accordance with this Act;
(b) support machine-readable access to public interest data through standardised APIs and related technologies;
(c) support accessibility to public interest data and the interoperability of databases;
(d) facilitate the onboarding of data providers and data consumers; and
(e) promote transparency in the access and management of public interest data.

(4) The National Data Exchange Platform shall be held by the Republic through the Ministry.

(5) The technical operation, configuration, administration and maintenance of the National Data Exchange Platform shall be managed and supervised by the Authority in accordance with the policy direction and objectives prescribed by the Minister.

(6) The installation and day-to-day operations of the National Data Exchange Platform shall at all times be managed by an entity registered under the laws of Ghana and

subject to the local content and local participation requirements prescribed by the Authority.

(7) The Minister may prescribe requirements and procedures for the administration of the National Data Exchange Platform.

Data Sharing Obligations

5. (1) All holders of public interest data shall identify and classify the public interest data they hold as either open data, shareable data or restricted data in accordance with Schedule 1 of this Act.

(2) The Minister may from time to time prescribe additional classifications of public interest data.

(3) All open data holders shall provide access to such open data via the National Data Exchange Platform in accordance with this Act and any directives issued under it.

(4) Shareable data holders shall provide access to shareable data via the National Data Exchange Platform upon the fulfilment of the relevant conditions required to access that shareable data.

(5) Shareable data holders shall clearly define and make transparent any conditions, procedures or terms which need to be met to access the shareable data.

(6) Nothing in this section shall be construed to require the sharing of data classified as restricted, except as may be authorised under this Act or any other applicable law.

(7) A holder of public interest data who fails to provide access in contravention of this section commits an offence and shall be liable upon summary conviction to a fine of not less than two hundred penalty units and not more than ten thousand penalty units.

Data Providers

6. (1) A holder of public interest data may be designated as a data provider under this Act and shall be onboarded onto the National Data Exchange Platform.

(2) A person shall qualify as a data provider if that person:
- (a) is a public body or private entity or institution that holds public interest data; or
- (b) performs a statutory, regulatory, or public service function involving the generation or management of public interest data; and
- (c) meets the eligibility criteria prescribed by the Authority.

(3) Without limiting the provisions of subsection (2) above, the Minister may designate entities, bodies, systems, organisations and institutions as data providers.

(4) The Authority shall, in consultation with the Advisory Committee, prescribe the criteria and procedures for determining eligibility as a data provider and the responsibilities of approved data providers in their operations on the National Data Exchange Platform.

(5) The Authority shall issue guidelines on the process and technical requirements for onboarding and integration with the National Data Exchange Platform.

(6) A data provider shall:
(a) ensure the accuracy and completeness of their database provided;
(b) apply the appropriate classification, specifications and format requirements as prescribed under this Act;
(c) implement appropriate security and technical measures, access controls and data protection measures as required under this Act or any other applicable law; and
(d) maintain internal processes to support timely and efficient data exchange in accordance with this Act and any Regulations, directives or guidelines issued under this Act.

(7) The Authority shall, in consultation with relevant sector regulators, maintain a register of approved data providers.

Data Exchange Framework

7. (1) Data providers shall grant access to their databases in a file format which is structured, machine-readable and compatible with the National Data Exchange Platform to allow software applications to easily identify, recognise and extract specific data.

(2) The Authority shall, in consultation with the Advisory Committee, prescribe technical and operational standards, including but not limited to:
(a) the use of standardised data formats across all databases;
(b) the adoption of sector-appropriate data exchange formats, including but not limited to XML and JSON;
(c) connectivity protocols that ensure secure, real-time, or scheduled data transmission;
(d) the application of sector-specific classification systems, taxonomies, and data dictionaries;
(e) the use of unique identifiers across sectors to ensure traceability and data deduplication; and
(f) metadata standards, classification levels, and tagging practices for all public interest data.

(3) The Authority shall prescribe the technical specifications referenced under subsection (2) and update them periodically to reflect international best practices and emerging technologies.

(4) Where conversion of public interest data into the prescribed digital format is impossible or would involve a disproportionate effort, the data provider shall consult with the Authority to determine an appropriate alternative prior to their onboarding.

System Integration and API Governance

8. (1) A data provider shall ensure that all data sharing occurs through secure, standardised, and auditable APIs, as prescribed by the Authority in consultation with the Ghana Standards Authority.

(2) The Authority shall prescribe technical specifications on:
(a) API architecture, protocols, and endpoints to ensure system-wide interoperability;
(b) authentication and authorisation mechanisms, including the use of digital credentials, access tokens, and role-based permissions;

(c) encryption requirements for data in transit and at rest to preserve confidentiality and integrity;
(d) tracking, logging, and audit mechanisms for each data request and response exchanged via the National Data Exchange Platform;
(e) implementation of tiered access or safeguard measures for sensitive data requiring limited or controlled disclosure; and
(f) any other specifications that the Authority may deem relevant.

(3) A data provider shall comply with all specifications provided by the Authority in accordance with subsection (2) and shall implement robust internal policies and procedures to protect and safeguard access to their API keys to prevent unauthorised use.

(4) A data provider who intentionally, recklessly or by gross negligence fails to prevent API exposure and unauthorised access is subject to an administrative penalty of up to ten thousand penalty units.

(5) A data provider shall not expose or allow access to any database through the National Data Exchange Platform unless the relevant API integration has been tested and approved by the Authority or a body designated by the Authority.

(6) A data provider who fails to comply with subsection (5) commits an offence and shall be liable upon summary conviction to a fine of not less than five hundred penalty units and not more than fifty thousand penalty units.

(7) The Authority may, in addition to the penalty under subsection (6), impose an administrative penalty of up to one thousand penalty units.

(8) The Authority shall monitor API performance, integrity, and security on a continuous basis, and may issue technical updates or revoke access where necessary to ensure compliance with this Act.

Data Security

9. (1) A data provider shall implement appropriate technical and organisational measures to ensure the confidentiality, integrity, security and continuous availability of the public interest data they share through the National Data Exchange Platform.

(2) Without limiting subsection (1) or any other obligations of data providers under this agreement, a data provider shall:
(a) establish role-based access controls and user authentication protocols to prevent unauthorised access to the database;
(b) ensure encryption of data in transit and at rest, using standards prescribed by the Authority;
(c) maintain routine backup systems for the database;
(d) implement business continuity and disaster recovery measures to minimise disruption in the event of system failure or compromise; and
(e) maintain internal controls and procedures for identifying, reporting, and responding to security incidents.

(3) The Authority may, in consultation with the Cyber Security Authority, Data Protection Commission and any other relevant government agencies, issue guidelines or directives specifying minimum security standards for data providers and data consumers.

(4) The Authority may prescribe different data security benchmarks for specific sectors or databases, taking into account the nature, use, and sensitivity of the data.

(5) A data provider shall, upon request, furnish the Authority with evidence of the internal procedures and systems in place to ensure data security in accordance with this section.

(6) A data provider shall notify the Authority promptly of any actual or suspected breach, compromise, or unauthorised access affecting its database, and in any case, no later than within seventy-two (72) hours of discovery:

(a) where the breach is of a nature affecting personal data, then the data provider shall additionally notify the Data Protection Commission in accordance with the provisions of the [Data Protection Act 20XX, (Act XXX)].

(b) where the breach is of a nature involving cybersecurity-related matters then the data provider shall additionally notify the Cybersecurity Authority within twenty-four (24) hours of detection in accordance with the [Cybersecurity Act 20XX, (Act XXX)];

(7) The form and manner of notification in subsection (6) and the immediate steps to be implemented after notification shall be prescribed by the Authority.

(8) A data provider who fails to comply with this section 9 commits an offence and shall be liable upon summary conviction to a fine of not less than five hundred penalty units and not more than fifty thousand penalty units.

(9) The Authority may, in addition to the penalty under subsection (8), impose an administrative penalty of up to ten thousand penalty units.

Data Quality Requirements

10. (1) A data provider shall ensure that all databases made available through the National Data Exchange Platform meet the quality standards prescribed by the Authority.

(2) For the purposes of subsection (1), a data provider shall:

(a) maintain the accuracy and completeness of public interest data contained in its databases;

(b) eliminate duplicate records and ensure data consistency across systems;

(c) establish procedures for regular updates, corrections, and verification of data entries; and

(d) where appropriate, implement version control mechanisms to track changes and ensure the integrity of historical records.

(3) The Authority may prescribe different data quality benchmarks for specific sectors or categories of data, taking into account the nature, use, and sensitivity of the data.

(4) A data provider shall, upon request, furnish the Authority with evidence of the internal procedures and systems in place to ensure data quality in accordance with this section.

Audit Trails and Logging

11. (1) A data provider shall implement and maintain audit trails and logging mechanisms for every access, transmission, or modification of public interest data through the National Data Exchange Platform.

(2) The audit trails and logs shall, at a minimum:
  (a) record the identity of the data consumer or system initiating the access or request;
  (b) specify the nature, date, time, and outcome of the transaction;
  (c) indicate the database and category or classification of data accessed or exchanged; and
  (d) capture any anomalies, access failures, or unauthorised attempts.

(3) Audit logs shall be:
  (a) securely stored in tamper-evident form;
  (b) encrypted and protected from unauthorised access or deletion; and
  (c) retained for a minimum of five (5) years, or such other period as may be prescribed by the Authority.

(4) The Authority may:
  (a) conduct periodic reviews of audit trails for compliance monitoring or technical assessment;
  (b) require the submission of logs by data providers to support investigations, verify system integrity, or assess suspected misuse; and
  (c) issue directives regarding the format, storage, or transmission of audit logs.

(5) A data provider shall establish internal protocols for monitoring and analysing audit trails to detect unusual activity, prevent abuse, and support incident response.

Oversight and Accountability

12. (1) The Authority shall monitor and enforce compliance with this Act, and may take appropriate enforcement actions against any data provider or data consumer who fails to meet their obligations under this Act.

(2) In carrying out its oversight function, the Authority shall issue guidelines, directives, and notices to ensure the proper functioning of the National Data Exchange Platform.

(3) The Authority shall consult the Advisory Committee and other relevant stakeholders in matters of joint oversight or technical coordination.

(4) A data provider shall submit periodic reports on their performance on the National Data Exchange Platform and their compliance with this Act. The form and frequency of the reports shall be determined by the Authority.

(5) The Authority shall publish an annual report detailing performance indicators and other key metrics of the National Data Exchange Platform and other relevant information to promote transparency.

(6) Each data provider shall:
  (a) appoint a designated officer responsible for ensuring compliance with the obligations under this Act;
  (b) respond to queries or directives issued by the Authority within the prescribed timelines; and
  (c) take corrective actions directed by the Authority promptly where deficiencies are identified.

Oversight Authority

13. The Authority shall be responsible for overseeing the implementation and enforcement of this Act.

Functions of the Authority

14. The functions of the Authority include but are not limited to:

(a) overseeing the establishment and maintenance of the National Data Exchange Platform;
(b) ensuring the operational integrity, accessibility and efficiency of the National Data Exchange Platform;
(c) overseeing compliance with the provisions of this Act and any subsidiary legislation, regulations, directives, guidelines or notices issued under this Act;
(d) developing, issuing and updating technical, operational and security guidelines in consultation with the Advisory Committee;
(e) overseeing the onboarding, registration, and monitoring of data providers and data consumers;
(f) maintaining a register of data providers and data consumers connected to the National Data Exchange Platform;
(g) collaborating with relevant stakeholders to ensure alignment with national policies and frameworks;
(h) coordinating with other regulatory bodies to ensure alignment with applicable laws, including but not limited to laws on data protection, cybersecurity, standardisation and open banking;
(i) issuing and enforcing administrative directives, notices or sanctions as provided under this Act;
(j) investigating and resolving disputes;
(k) coordinating capacity building, stakeholder engagement, and public education on data harmonisation and the National Data Exchange Platform; and
(l) advising the Minister on policy implementation matters under this Act.

Data Harmonisation Advisory Committee

15. (1) There is established by this Act a Data Harmonisation Advisory Committee to provide operational insight, discuss cross-sectoral matters on data harmonisation and provide strategic advice to support the Authority in the effective performance of its functions.

(2) The Committee shall be composed of:

(a) the Minister;
(b) a representative of the National Information Technology Agency not below the rank of a director;
(c) a representative of the Bank of Ghana not below the rank of director;
(d) a representative of the Cyber Security Authority not below the rank of a director;
(e) a representative of the Data Protection Commission not below the rank of a director;
(f) a representative of the Ghana Standards Authority not below the rank of a director or its functional equivalent;
(g) a representative of the Ghana Statistical Service not below the rank of a director or its functional equivalent;
(h) a representative of the National Communications Authority not below the rank of a director;
(i) a representative of the National Identification Authority not below the rank of a director or its functional equivalent;

(j) a senior officer of the [National Intelligence Bureau/National Security Council];
(k) a representative of the Office of the Registrar of Companies not below the rank of a director or its functional equivalent;
(l) two persons from the private sector with expertise in data management, data architecture, data analysis, standards engineering, ICT or digital services; and
(m) one representative of civil society with experience in data protection, intellectual property or digital rights.

(3) The members of the Committee shall be appointed by the Minister on the recommendation of the respective institutions and at least three (3) of the representatives shall be women.

(4) The Minister shall be Chairperson of the Advisory Committee.

(5) The Committee shall meet at least once every six months and may hold extraordinary meetings:
(a) at the request of the Chairperson; or
(b) upon the written request of not less than one-third of the members of the Advisory Committee.

(6) The Advisory Committee shall provide practical guidance on the implementation of this Act only and shall not exercise any executive, regulatory or operational authority under this Act.

(7) The Committee shall advise the Authority on:
(a) strategic direction and long-term planning for data exchange and harmonisation;
(b) stakeholder coordination and multi-agency alignment;
(c) phased implementation of the Act and any practical challenges;
(d) cross-sector engagements and feedback;
(e) drafting of guidelines under the Act;
(f) standards for interoperability and integration; and
(g) any other matters as may be referred to it by the Authority or the Minister.

(8) The term of office of a member of the Committee is four years, and a member is eligible for reappointment for another term only.

Access and Use of the National Data Exchange Platform

Data Access

16. (1) A person approved by the Authority as a data consumer may access public interest data through the National Data Exchange Platform in accordance with this Act.

(2) Access to data on the National Data Exchange Platform shall be granted for the following permitted purposes:
(a) delivery of public services or performance of statutory functions;
(b) research, innovation, and academic development;
(c) statistical analysis and evidence-based policymaking;
(d) detection and prevention of fraud, financial crime or other unlawful conduct;
(e) regulatory compliance, oversight and supervision functions; or
(f) any other lawful purposes approved by the Authority in consultation with the Minister.

(3) A person seeking approval as a data consumer shall apply to the Authority for authorisation. The application shall be made in a manner prescribed by the Authority and at a minimum, must:
   (a) identify the applicant and describe the purpose for which access is required;
   (b) specify the public interest data for which access is being requested, including any intended re-use or onward sharing;
   (c) disclose the applicant's legal basis or authorisation for accessing the data, where applicable;
   (d) include high-level information on its technical systems for the purpose of assessment for integration;
   (e) comply with any other conditions prescribed by the Authority, including the payment of prescribed fees.

(4) A person seeking approval as a data consumer shall be a legal entity or body corporate and shall not be a natural person.

(5) Upon approval, a data consumer shall be granted access credentials to the National Data Exchange Platform for a period of one (1) year and assigned a data access tier in accordance with their authorisation level.

(6) A data consumer may, upon expiration of their credentials, apply to the Authority for a renewal of their subscription in the prescribed form. The Authority may request additional up-to-date information from the applicant prior to granting a renewal.

(7) A person who unlawfully or without the proper authorisation accesses databases on the National Data Exchange Platform commits an offence and shall be liable upon summary conviction to a fine of not less than one thousand penalty units and not more than one hundred thousand penalty units or a term of imprisonment of not more than five years or both.

(8) The Authority may, in addition to the penalty under subsection (7), impose an administrative penalty of up to ten thousand penalty units.

(9) Data consumers may be required to enter data use agreements as a precondition to accessing shareable data or restricted data.

(10) Data consumers shall not re-use data obtained through the National Data Exchange Platform in a manner that duplicates or directly competes with the service offered by the data provider whose database they accessed.

(11) Data consumers shall not re-use personal data except in a manner that has been consented to by the data subject or is otherwise permitted by law.

(12) A data consumer that contravenes subsections (10) and (11) commits an offence and is liable on summary conviction to a fine of not less than five thousand penalty units and not more than fifty thousand penalty units.

(13) The Authority shall, in consultation with the Advisory Committee, issue guidelines on the permitted re-use of data.

(14) A person who purchases or sells, attempts to purchase or sell, or does any act with the intent to purchase or sell data obtained through the National Data Exchange Platform, except as otherwise approved by the Authority, commits an

offence and is liable upon summary conviction to a fine of not less than five thousand penalty units and not more than one hundred thousand penalty units or a term of imprisonment of not more than seven years or both.

(15) A data provider shall maintain and submit to the Authority, in the form and manner prescribed by the Authority, a data register cataloguing the public interest data available through its database to promote ease of access. The data register shall indicate:
(a) the public interest data available on the data provider's database;
(b) the classification of such data as open, shareable or restricted;
(c) for restricted or shareable data, any conditions or protocols required for the disclosure of that data;
(d) the fees required to access their database, where applicable; and
(e) any other information prescribed by the Authority.

(16) The Authority may refuse to grant an application where:
(a) the applicant fails to satisfy the applicable eligibility, legal, or technical requirements;
(b) the data requested is classified as restricted and the applicant does not possess the necessary clearance;
(c) granting access may compromise national security, public safety, or data integrity; or
(d) the request is otherwise inconsistent with the objectives of this Act.

(17) In the event of refusal, the Authority shall notify the applicant of the reasons for the refusal.

(18) An international organisation or a foreign entity operating in Ghana may apply for access to the National Data Exchange Platform through the Authority. Applications for foreign data consumers shall be subject to additional conditions prescribed by the Authority, and must be approved by the Minister.

(19) The Authority shall submit a list of all foreign data consumer applications that have satisfied the prescribed additional criteria to the Minister for final approval on a quarterly basis.

Onboarding and Access Control Protocols

17. (1) The Authority shall establish a process for onboarding data consumers which may include the payment of any applicable onboarding or service fees.

(2) The Authority shall implement access control protocols to govern the scope and level of access granted to each data consumer.

(3) A data consumer shall not access any database or transmit data beyond the level or purpose for which access has been granted. The Authority may suspend or revoke access for any data consumers who fail to comply with this section.

(4) Data consumers who contravene subsection (3) commit an offence and shall be liable upon summary conviction to a fine of not less than five hundred penalty units and not more than fifty thousand penalty units.

(5) The Authority may, in addition to the penalties under subsections (3) and (4), impose an administrative penalty of up to five hundred penalty units.

Cross-Border Transfers

18. (1) The transfer of public interest data through the National Data Exchange Platform to data consumers outside the jurisdiction of Ghana is permitted only in accordance with the provisions of this Act.

(2) Cross-border transfers pursuant to subsection (1) shall:

(a) be in compliance with the [Data Protection Act, 20XX(Act XXX)] and other applicable laws;

(b) comply with any safeguards, protocols or limitations prescribed under this Act or issued by the Authority; and

(c) be approved by the Minister.

(3) Safeguards under subsection (2) may include:

(a) restrictions on the type or category of data which may be transferred outside the jurisdiction;

(b) mandatory access through a registered Ghanaian subsidiary or an approved local representative regulated by the Authority;

(c) limitations on the duration of access;

(d) additional requirements for technical safeguards, access logs and audits; and

(e) any safeguards prescribed by the Minister or the Authority.

(4) A data provider or data consumer that facilitates or permits cross-border transfers of data through the National Data Exchange Platform in a manner that circumvents or violates this section, commits an offence and shall be liable upon summary conviction to a fine of not less than five hundred penalty units and not more than one hundred thousand penalty units.

(5) The Authority may, in addition to the penalty under subsection (4), impose other administrative sanctions, including an administrative penalty of up to five thousand penalty units.

Data Protection

Data Subject Rights

19. Nothing in this Act shall be construed to limit or derogate from the rights of data subjects under the [Data Protection Act, 20XX (Act XXX)]. Where public interest data includes personal data, the processing, access, or sharing of such data through the National Data Exchange Platform shall be undertaken in a manner that upholds Act XXX. The Authority shall work in collaboration with the Data Protection Commission to ensure the enforcement of data subject rights in relation to the use, re-use and exchange of personal data through the National Data Exchange Platform.

Obligations of Data Controllers and Data Processors

20. Nothing in this Act shall be construed to limit or derogate from the obligations of data controllers and data processors under the [Data Protection Act, 20XX(Act XXX)].

Compliance and Enforcement

Compliance Monitoring

21. (1) The Authority shall establish and maintain a monitoring system to monitor compliance with the rules, obligations and requirements of the National Data Exchange Platform and this Act.

(2) The Authority may appoint inspectors to carry out monitoring functions outlined under this Act or prescribed by the Authority or the Minister.

(3) The inspector may at reasonable times:
(a) enter and inspect a premises, which the inspector knows or reasonably suspects to be used for a purpose to which this Act applies, to ensure that the provisions of this Act are complied with; or
(b) enter a premises to perform any other function imposed on the inspector under this Act, or by the Authority.

(4) The inspectors shall submit quarterly compliance reports in the manner prescribed by the Authority.

(5) The Authority may conduct audits on all participating institutions, within periods to be determined by the Authority, to assess a participating institution's compliance with applicable laws and the rules of the National Data Exchange Platform.

Reporting Requirements

22. (1) Where requested by the Authority, a participating institution shall provide reports on activities undertaken through the National Data Exchange Platform. The report shall include any information as may be prescribed by the Authority.

(2) A participating institution shall notify the Authority within seven days of any change in the information that was submitted to the Authority for approval as a participating institution.

Offences and Penalties

23. (1) A person who contravenes or fails to comply with any provision of this Act commits an offence and, where no penalty is expressly provided, shall be liable upon summary conviction to a fine of not less than two hundred penalty units and not more than ten thousand penalty units or to a term of imprisonment of not more than two years or both.

(2) A person who fails to comply with an administrative sanction prescribed by the Authority under section 24 of this Act commits an offence and, where no penalty is expressly provided, shall be liable upon summary conviction to a fine of not less than two hundred penalty units and not more than ten thousand penalty units or to a term of imprisonment of not more than two years or both.

(3) Where an offence under this Act is committed by a body corporate or by a member of a partnership or other firm, every director or officer of that body corporate or a member of the partnership or any other person concerned with the management of the firm shall be deemed to have committed that offence and is liable on summary conviction to a fine or term of imprisonment as prescribed.

(4) A person shall not be convicted of an offence under subsection (3) if it is proved that:
(a) due diligence was exercised to prevent the commission of the offence; and
(b) the offence was committed without the knowledge, consent or connivance of that person.

Administrative Sanctions

24. (1) A person who contravenes or fails to comply with any provision of this Act which is not designated as an offence may be liable to administrative sanctions as prescribed by the Authority.

(2) The Authority may prescribe the following sanctions:
   (a) issue a warning or non-compliance notice to a participating institution;
   (b) suspend a participating institution from use of the National Data Exchange Platform;
   (c) revoke access and remove a participating institution from the National Data Exchange Platform;
   (d) impose administrative penalties on a participating institution;
   (e) impose bans on a participating institution; and
   (f) any other sanction as may be appropriate to redress the stated non-compliance.

(3) A participating institution that has its access or approval revoked may submit a fresh application to the Authority to be reinstated after rectifying the breach or non-compliance.

(4) Participating institutions that have been banned shall not be permitted to reapply for access.

(5) The imposition of administrative sanctions or fines under this Act shall be without prejudice to any penalties, fines or sanctions that may be imposed by any other regulatory authority under any other enactment.

(6) Where the conduct of a person constitutes an offence under this Act and any other enactment, nothing in this Act shall prevent the institution of proceedings under that other enactment.

Dispute Resolution

25. (1)The Authority shall establish a dispute resolution process to resolve disputes:
   (a) between data providers and data consumers;
   (b) between or among different data providers;
   (c) between data subjects and data providers or data consumers; and
   (d) between the Authority and data providers, data consumers or data subjects.

(2) Where a dispute, pursuant to subsections (c) and (d) above, concerns a matter involving data subjects, their personal data and data subject rights, then the Authority shall involve the Data Protection [Commission/Authority] in the resolution of the dispute.

(3) Where a dispute under subsection (1) involves matters pertaining to issues of cybersecurity, then the Authority shall involve the Cybersecurity Authority in the resolution of the dispute.

(4) Any one or more parties to a dispute may refer the dispute to the Authority for settlement by any alternative dispute resolution mechanism.

(5) Where parties to a dispute agree that the dispute is to be settled by
   (a) the dispute resolution committee established under section 26; or
   (b) any alternative dispute resolution mechanism
   the parties shall not institute an action in court until the dispute resolution procedure has been exhausted.

Dispute Resolution Committee

26. (1) The Authority shall establish a Dispute Resolution Committee for the purpose of the resolution of disputes and shall prescribe the rules of procedure of the Dispute Resolution Committee.

(2) The composition of the Dispute Resolution Committee shall be determined by the board of the Authority in consultation with the Advisory Committee.

(3) The Dispute Resolution Committee shall expeditiously investigate and hear any matter which is brought before it.

(4) The Authority shall determine the period within which disputes may be settled.

(5) The Dispute Resolution Committee may require evidence or arguments to be presented in writing and may decide the matters upon which it will hear oral evidence or written arguments.

(6) A party to a dispute may appear at the hearing and may be represented by a lawyer or another person of that person's choice.

Powers of the Dispute Resolution Committee

27. (1) The Dispute Resolution Committee shall have the power to:

(a) issue summons to compel the attendance of witnesses;
(b) examine witnesses on oath, affirmation or otherwise;
(c) compel the production of documents; and
(d) refer a person for trial at the High Court for contempt.

(2) A summons issued by the Dispute Resolution Committee shall be under the hand of the Secretary of the Authority.

Resolution of Referred Disputes

28. (1)The Dispute Resolution Committee may, in settling a dispute.

(a) make a declaration setting out the rights and obligations of the parties to the dispute;
(b) make provisional or interim orders or awards related to the matter or part of the matter, or give directions in furtherance of the hearing;
(c) dismiss or refrain from hearing or determining a matter in whole or in part if it appears that the matter or part of the matter, is trivial or vexatious or that further proceedings are not necessary or desirable in the public interest;
(d) in appropriate circumstances, order any party to pay the reasonable costs and expenses of another party, including the expenses of witnesses and fees of lawyers, in bringing the matter before the Authority; and
(e) generally give directions and do anything that is necessary or expedient for the hearing and determination of the matter.

Data Harmonisation Tribunal

Establishment of the Data Harmonisation Tribunal

29. (1) There is by this Act established an appeal tribunal to be called the Data Harmonisation Tribunal which shall be convened on an ad-hoc basis to consider appeals against:

(a) decisions or orders made by the Authority or to review a particular matter under this Act or its regulations, directives or guidelines; and
(b) decisions of the Dispute Resolution Committee of the Authority.

Composition of the Tribunal

30. (1) The members of the Tribunal shall be appointed by the Minister and shall consist of:

(a) a chairperson who is either a retired Justice of the Superior Court or a lawyer of at least fifteen years standing who has experience in technology law (particularly data privacy, intellectual property, and cybersecurity matters), policy, regulations or arbitration; and

(b) two other members with experience or academic or professional qualifications in the data governance, public digital infrastructure, electronic engineering, data protection, cybersecurity, law, economics or business or public administration.

(3) The Minister shall appoint a registrar and other staff necessary for the smooth operations of the Tribunal.

(4) The expenses of the Tribunal shall be paid out of income derived by the Authority under this Act and shall be part of the annual budget of the Authority.

Rules of Procedure of the Tribunal

31. (1) The Authority shall, within thirty days of the commencement of this Act, prepare proposals for rules of procedure for the Tribunal.

(2) The proposals shall be approved by a panel of the Tribunal specifically convened for the purpose.

(3) The Authority shall by legislative instrument make Regulations under this Act which shall prescribe the approved rules.

Right of Appeal

32. (1) A person affected by a decision of the Authority or the Dispute Resolution Committee may appeal against it by sending a notice of appeal to the Tribunal in accordance with the rules of procedure of the Tribunal.

(2) The notice of appeal must be sent within twenty-eight days after the date on which the decision being appealed against is announced or received.

(3) The appellant shall set out in the notice of appeal:

(a) the decision appealed against;

(b) the provision under which the decision appealed against was taken; and

(c) the grounds of appeal.

(4) Within one month after receipt of a notice of appeal the Tribunal shall be convened to consider the appeal.

Decisions of the Tribunal

33. (1) The Tribunal, after hearing the appeal may:

(a) quash the decision;

(b) allow the appeal in whole or in part; or

(c) dismiss the appeal and confirm the decision of the Authority.

(2) If the Tribunal allows the appeal in part, it may vary the decision of the Authority in any manner and subject to any conditions or limitations that it considers appropriate to impose.

(3) The Tribunal may take into account any submissions filed by a person acting as a friend of the Tribunal in reaching a decision on an appeal brought before it.

(4) A decision of the Tribunal has the same effect as a judgement of the High Court and shall be final unless submitted to the High Court for review.

Financial Provisions

Fees

34. The Minister shall determine the fees to be charged under this Act in accordance with the Fees and Charges (Miscellaneous Provisions) Act, 2022 (Act 1080).

Sources of Funds

35. The funds of the National Data Exchange Platform shall include:

(a) seed money;
(b) fees accruing to the National Data Exchange Platform under this Act;
(c) moneys provided by Parliament;
(d) donations, gifts, grants and other voluntary contribution; and
(e) any other moneys that are approved by the Minister responsible for Finance.

Expenses

36. The expenses of the National Data Exchange Platform shall be paid from moneys provided from the funds of the National Data Exchange Platform.

Accounts and audits

37. (1) The Authority shall keep books of account and proper records in relation to the National Data Exchange Platform in the form approved by the Auditor-General.

(2) The Authority shall submit the accounts of the National Data Exchange Platform to the Auditor-General for audit within three months after the end of the financial year.

(3) The Auditor-General shall, not later than three months after the receipt of the accounts, audit the accounts and forward a copy of the audit report to the Minister.

(4) The Internal Audit Agency Act, 2003 (Act 658) shall apply to this Act.

(5) The financial year of the Authority and the entity that manages the National Data Exchange Platform shall be the same as the financial year of the Government.

Transitional and Miscellaneous Provisions

Implementation and Pilot Scheme

38. The implementation of this Act shall be in phases as prescribed by the Minister.

Relationship and Integration with Existing Laws

39. (1)This Act shall be read in conjunction with applicable laws governing data protection, intellectual property, public access to information, cybersecurity, electronic transactions, and any other law which confers rights or imposes obligations relating to the generation, use, protection, and sharing of data in Ghana, including but not limited to the:

(a) Copyright Act, 2005 (Act 690);
(b) [Cybersecurity Act 20XX (Act XXXX)];
(c) [Data Protection Act, 20XX (Act XXXX)];
(d) [Electronic Communications Act, 20XX (Act XXXX)];
(e) [Electronic Transactions Act, 20XX (Act XXXX)];

(f) Ghana Standards Authority Act, 2022 (Act 1078);
(g) National Identification Authority Act, 2006 (Act 707)
(h) National Signals Bureau Act, 2020 (Act 1040);
(i) Patents Act, 2003 (Act 657);
(j) Protection Against Unfair Competition Act, 2000 (Act 589);
(k) Right to Information Act, 2019 (Act 989);
(l) Security and Intelligence Agencies Act, 2020 (Act 1030);
(m) State Secrets Act, 1962 (Act 101);

and shall not, except as otherwise provided in this Act, derogate from the provisions of these Acts.

(2) Where there is any conflict between this Act and any relevant enactment in respect of the standardisation and sharing of data, the provisions of this Act shall prevail.

40. Repeals and Savings
[TBD]

Regulations
41. The Minister may, on the recommendation of the Authority, make Regulations for the implementation of this Act.

Interpretation
42. In this Act unless the context otherwise requires:
“Advisory Committee” means the strategic Advisory Committee established to advise the Authority on the implementation of this Act;

“API” means an Application Programming Interface that enables the secure and structured exchange of data between different systems or databases, including authentication, authorisation, and data formatting protocols.

“Authority” means the National Information Technology Agency;

“database” means an organised collection of relevant public interest data, whether structured or unstructured, which is maintained and made available by a data provider for access, exchange and use on the National Data Exchange Platform;

"data consumer" means an artificial person or entity that accesses, uses, re-uses or exchanges data through the National Data Exchange Platform for any lawful purpose, including research, service delivery, innovation, or regulatory compliance;

“data controller” shall be construed in accordance with the [Data Protection Act, 20XX (Act XXX)] and means a person who either alone, jointly with other persons determines the purposes for and the manner in which personal data is processed or is to be processed;

"data provider" means a public or private entity that generates, collects, processes, stores or holds public interest data and makes that data available through the National Data Exchange Platform in accordance with this Act;

“data register” means a catalogue created by data providers to assist with navigating their database.

“data subject” shall be construed in accordance with the Data Protection Act, 20XX (Act XXX) and means an individual who is the subject of personal data;

“data subject rights” shall be construed in accordance with the [Data Protection Act, 20XX (Act XXX)] and means […]

“exchange” means the structured, secure, and authorised transmission of data between systems, institutions, or entities for a specific permitted purpose

“foreign” means, in relation to a person or entity, any person or entity that is not Ghanaian or an entity that is not incorporated, registered, or established under the laws of Ghana.

"National Data Exchange Platform" means the public digital infrastructure designated under this Act for the secure and standardised exchange of public interest data between the public and private sectors;

“Minister” means the Minister assigned responsibility for the Ministry of Communications;

“Ministry” means the Ministry of Communications;

"open data" means public interest data that is not subject to any law, regulation, or policy that restricts its access or use, and may be accessed, used, reused, and distributed by any person without legal or technical restriction;

“personal data” shall be construed in accordance with the Data Protection Act, 20XX (Act XXX) and means any information relating to an identified or identifiable natural person, and includes one or a combination of the following, whether identified by manual or automated processing:

(a) direct identifiers such as name; email address; phone number, identification number; registration number; bank account, bank or smart card number; photographic or video image of face;
(b) indirect identifiers such as an location data; age or age-range, occupation; job; profession; vocation; business; workplace; title; education; voice-recordings, postal code; place of birth; date of birth; marital status; photographs or videos without facial detail but identifications such as side views, clothing, marks and mannerism; language preference; profiles without facial detail but which could be attributed to a natural person by the use of additional information;
(c) online identifiers such as IP address; cookies; device ID; login credentials; user IDs; push notification tokens, browser history or fingerprints;
(d) data which have undergone pseudonymisation, but which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person; and
(e) one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that natural person;

“participating institution” means a data provider or data consumer as defined under this Act;

“processing” shall be construed in accordance with the [Data Protection Act, 20XX (Act XXXX)] and means an operation or activity or set of operations by electronic or other means that concerns data or personal data and the

(a) collection, organization, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or other means available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data;

"public interest data" means data, whether personal or non-personal, recorded and documented in any manner and on any medium, which is collected, created, generated, held or otherwise processed by public authorities, private entities, or other institutions, and is either necessary for or beneficial to public purposes, including but not limited to, the provision of public services, performance of public functions, regulatory compliance, or national development. Public interest data shall include any data prescribed as public interest data by the Minister;

"restricted data" means public interest data of a sensitive or classified nature, for which access is limited by law, or may only be granted upon fulfilment of specified conditions, including the demonstration of a legitimate interest or the application of special procedures. Restricted Data includes state secrets, information relating to national security, confidential business information, or other categories that the law exempts from public disclosure. Restricted data shall include any data prescribed as restricted data by the Minister;

“Republic” means the Republic of Ghana;

“re-use” means the use, whether commercial or non-commercial, of public interest data obtained through the National Data Exchange Platform for a purpose other than the initial purpose for which the data was collected;

"shareable data" means public interest data that is not classified as restricted data but may only be accessed or used subject to prescribed terms, procedures, or conditions; and

FIRST SCHEDULE
Part X
(Section X)

Public Interest Data Classification Framework

Public interest data shall be classified for the purposes of this Act into—
a. **open data**,
b. **shareable data**, and
c. **restricted data**.

Open data refers to public interest data that:
a. is not subject to any legal, commercial, or confidentiality restrictions; and
b. may be freely accessed, used, reused, or redistributed without requiring specific authorisation.

Shareable data refers to public interest data that:
a. is not openly available to the public; but
b. may be accessed or reused by authorised persons under specific terms, conditions or procedures prescribed by law or determined by the data provider.

Restricted data refers to public interest data:
a. which is subject to legal, contractual, or institutional restrictions on access, use, or disclosure; or
b. which, if disclosed, may reasonably be expected to pose a risk to national security, public order, individual privacy, or the rights and interests of a third party.

The Data Protection [Commission/Authority] is in consultation with the Authority shall prescribe guidelines for the classification of data

The Minister may, on the advice of the Authority, by legislative instrument, issue guidelines for:
a. the further classification of public interest data by sector, type, sensitivity, or purpose; and
b. the criteria for reclassification of data from one category to another, including from restricted to shareable or from shareable to open, where applicable.

SECOND SCHEDULE
Part X
(Section X)

Local Participation and Local Content Requirements for the National Data Exchange Platform operator