ARRANGEMENT OF SECTIONS

A

BILL

ENTITLED

DATA PROTECTION ACT, 2025

An Act to establish the Data Protection Authority; to regulate the processing of personal data; to provide the legal framework for the protection of personal data, and for related matters.

DATE OF ASSENT:

Preliminary Provisions

Application of the Act

1. (1) Except as otherwise provided, this Act applies to a data controller in respect of data where:

(a) the data controller is established in this country and the data is processed in this country;

(b) the data controller is established in this country and the data is processed outside the country by either the data controller or data processor;

(c) the data controller is not established in this country but offers goods and services to persons who are within the country;

(d) the data controller is not established in this country but their activities involve monitoring or profiling of individuals in the country;

(e) the data controller is not established in this country but uses equipment or a data processor carrying on business in this country to process the data; or

(f) processing is in respect of information which originates partly or wholly from this country.

(2) Subject to the requirements under subsection (3), a data controller that is not established in this country shall not be required to register as an external company unless otherwise required by any other enactment or law.

(3) A data controller that is not established in this country shall designate in writing a representative within the country where:

(a) the data controller processes large-scale data on a frequent or continuous basis;

(b) the data controller processes special personal data of individuals in the country; or

(c) the data controller processes personal data relating to criminal offences in the country.

(4) The requirement to designate a representative in the country shall not apply to a data controller whose processing of personal data is not likely to result in risks to rights and freedoms of data subjects.

(5) For the purposes of this Act, provided that liability under the Act shall remain with the data controller, the representative shall only:

(a) serve as the primary contact for the Authority and data subjects of the data controller;

(b) document and maintain records of the data controller's processing activities in the country;

(c) be authorised to receive and process all documentation relating to data processing on behalf of the data controller; and

(d) be subject to enforcement actions under the Act on behalf of the data controller.

(6) For the purposes of this Act the following are to be treated as established in this country:

(a) an individual who is ordinarily resident in this country;

(b) a body incorporated or registered under the laws of this country;

(c) a body whose central administration or management of business or operational activities takes place in this country;

(d) a partnership, persons registered under the Registration of Business Names Act, 1962 (Act 151) and the Trustees (Incorporation) Act, 1962 (Act 106);

(e) an unincorporated joint venture or association operating in part or in whole in this country; and

(f) any person who does not fall within paragraphs *(a),(b), (c)* or *(d)* but maintains an office, branch or agency through which business activities are carried out in this country.

(7) For the purposes of this Act, a person is ordinarily resident in the country where that person holds a residence permit issued by the appropriate authority, or in any other situation where:

(a) that person has been present in this country for an aggregate period of not less than 183 days in any 12-month period, regardless of temporary absences; and

(b) has adopted living in the country for settled purposes as part of regular activities.

(8) Subject to the Republic's national security and intelligence needs, this Act does not apply to data which originates externally and merely transits through this country unless it is subsequently processed in the country.

Application to the State

2. (1) This Act binds the Republic.

(2) For the purposes of this Act, each government department shall be treated as a data controller.

(3) Each government department shall appoint an officer to act as a data protection officer.

(4) Subject to subsection (5), government departments shall not engage in any dealings or transaction with other government departments or any other

person that involve the processing of personal data, without a valid certificate of registration issued by the Authority, or by a national foreign data protection regulator where that person is not established in the country.

(5) For the purposes of this Act, the following constitutes dealings or transactions with a person provided that it involves the processing of personal data:

(a) public-private partnerships under the Public Private Partnership Act, 2020 (Act 1039);

(b) procurement contracts or agreements under the Public Procurement Act, 2003 (Act 663) as amended;

(c) any contract or agreement where the data controller processes large-scale data or special personal data;

(d) any contract for the provision of services including legal, medical, health, broadcast and telecommunication, engineering, transportation and logistics, education, technology and software provision, water and sanitation, marketing and advertisement, real estate, research and development, human resource and recruitment, tourism and hospitality, event management, food production and agriculture, accounting, finance, insurance, banking, consulting, power and energy, mining, oil and gas, security, emergency and relief, non-profit and other professional services;

(e) any contract or agreement for the provision of a services which is necessary or incidental to the business or operations of the government department;

(f) any contract or agreement that requires cross-border transfer of data; and

(g) international business and economic transactions.

(6) For the avoidance of doubt, the routine procurement of goods and services such as food supplies, office equipment, stationery or administrative materials do not constitute dealings and transactions under this section.

(7) The failure of the government department to comply with subsection (4) shall not invalidate a contract or render a contract illegal and unenforceable.

(8) A government department who breaches subsection (4) shall be liable to an administrative penalty.

(9) The Authority may by guidelines or directives, determine which categories of dealings or transactions under subsection (5) may be not be subject to the requirements under subsection (4) for the time being.

(10) The Minister may by legislative instrument expand the categories or transactions under subsection (5).

(11) Where the purposes and the way the processing of personal data are determined by a person acting on behalf of the Executive, Parliament and the Judiciary, the data controller in respect of that data for the purposes of this Act is

(a) in relation to the Executive, the Chief of Staff, *(b)* in relation to Parliament, the Clerk to Parliament, and *(c)* in relation to the Judiciary, the Judicial Secretary.

(12) Despite subsection (11), a person in a different capacity may be appointed as data controller and such person must be designated in writing to the Authority.

Data Protection Authority

Establishment of the Data Protection Authority

3. (1) There is established by this Act, the Data Protection Authority.

(2) The Authority –

(a) shall be a body corporate, with perpetual succession and a common seal;

(b) may sue or be sued in its corporate name; and *(c)* may acquire, hold and dispose of its property.

(3) Where there is hindrance to the acquisition of property, the property may be acquired for the Authority under the Land Act, 2020 (Act 1036) and the costs shall be borne by the Authority.

Object of the Authority

4. The object of the Authority is to:

(a) protect the privacy of the individual and personal data by regulating the processing of personal information,

(b) ensure efficient management of personal data to prevent data exploitation and abuse;

(c) establish standards for the processing of data locally and by crossborder transfer mechanisms,

(d) regulate the personal data digital economy to build trust and confidence in the delivery of digital services, and

(e) provide the process to obtain, hold, use or disclose personal information.

Independence of the Authority

5. (1) The Authority shall be independent, and shall not be subject to the direction, control, influence and pressure of any person or authority, including the government in the exercise of its object, powers and functions.

(2) The primary decision-making power and enforcement as it relates to rights and obligations under this Act shall reside with the Authority.

(3) The Authority shall exercise its functions and powers impartially, without bias, and in the best interests of safeguarding individuals' rights under this Act.

(4) The Authority shall establish and implement mechanisms for ensuring accountability of the actions or inactions and obligations of data controllers and data processors under the Act.

(5) The Authority shall have power to determine its organisational structure and regulate its own internal procedures.

Powers of the Authority

6. The Authority is granted the power to:

(a) issue market conduct regulations, rules, directives and guidelines under this Act;

(b) conduct investigations into alleged breaches of data protection regulations;

(c) provide accreditation to data protection service providers;

(d) facilitate conciliation, mediation and negotiation on disputes arising from this Act;

(e) issue summons to a witness for the purposes of investigation;

(f) issue corrective measures, administrative fines, penalties, direct peer regulators to cancel or suspend licenses or operations or issue sanctions in response to identified non-compliance with the provisions of this Act and

(g) make any determination as the Authority finds just and equitable.

Functions of the Authority

7. To achieve the object, the Authority shall

(a) implement and monitor compliance with the provisions of this Act;

(b) make the administrative arrangements it considers appropriate for the discharge of its duties;

(c) investigate any complaint under this Act and determine it in the manner the Authority considers fair;

(d) keep and maintain the Data Protection Register;

(e) carry out audits to assess compliance with the provisions of this Act;

(f) facilitate training of data protection officers;

(g) provide guidance, disseminate information, and collaborate with relevant entities to enhance understanding and awareness of data protection principles and

(h) prescribe and enforce appropriate remedies to address violations and mitigate the impact on individuals' privacy and data management and data security rights.

Governing body of the Authority

8. (1) The governing body of the Authority is a Board consisting of

(a) a chairperson;

(b) one representative from the following:

(i) Commission on Human Rights and Administrative Justice not below the rank of a Deputy Commissioner;

(ii) Ministry of Communications not below the rank of a Director;

(iii) National Communications Authority not below the rank of a Director;

(iv) Bank of Ghana not below the level of Deputy Governor;

(c) one representative elected by the Industry Forum;

(d) two other persons nominated by the President at least one of whom is a woman; and the Director General of the Authority.

(e) *(f)* provided that the composition of the Board shall have not less than three women

(2) The members of the Board shall be appointed by the President in accordance with article 70 of the Constitution.

(3) The Board shall ensure the proper and effective performance of the functions of the Authority.

Duties and liabilities of a member of the Board of Directors

9. (1) A member of the Board of Directors has the same fiduciary relationship with the Authority and the same duty to act with loyalty and in good faith as a director of a company incorporated under the Companies Act, 2019 (Act 992).

(2). Without limiting subsection (1), a member of the Board of Directors has a duty

(a) to act honestly and in the best interest of the Authority in the performance of the functions of the Authority;

(b) to exercise the degree of care and diligence in the performance of functions that a person in that position would reasonably be expected to exercise in the circumstances;

(c) not to disclose information acquired in the capacity of the member as a member of the Board of Directors to any person or make use of that information, except in the performance of functions;

(d) not to abuse the position of the office; and

(e) not to pursue personal interests at the expense of the Authority.

(3) A member of the Board of Directors, other than the Director General, shall not participate in the day-to-day running of the Authority.

(4) A member of the Board is not personally liable for damage or injury to a third party that arises in the execution of an official duty of that member, if the member at all material times acted in good faith.

(5) The Authority shall indemnify and hold harmless such a member against any legal costs, including attorney's fees, expenses, and liabilities reasonably incurred in connection with any legal proceedings instituted against the member in respect of acts done or purported to have been done in the performance of official duties, provided that the member acted in good faith and in the interest of the Authority.

(6) A member of the Board of Directors who contravenes subsection (1) or (2) commits an offence and is liable on summary conviction to a fine of not

less than two thousand penalty units and not more than twenty thousand penalty units.

(7) Where a court determines that the Authority has suffered a loss or damage as a result of the act or omission of a member of the Board of Directors, the court may, in addition to imposing a fine, order the member to pay appropriate compensation to the Authority.

Tenure of office of members

10. (1) A member of the Board shall hold office for a period not exceeding four years and is eligible for re-appointment, but a member shall not be appointed for more than two terms.

(2) Subsection (1) does not apply to the Director General of the Authority.

(3) A member of the Board may at any time resign from office in writing addressed to the President through the Minister.

(4) A member of the Board, other than the Director General who is absent from three consecutive meetings of the Board without sufficient cause ceases to be a member of the Board.

(5) The President may by letter addressed to a member revoke the appointment of that member.

(6) Where a member of the Board is, for a sufficient reason, unable to act as a member, the Minister shall determine whether the inability would result in the declaration of a vacancy.

(7) Where there is a vacancy

(a) under subsection (3) or (4);

(b) as a result of a declaration under subsection (6); or

(c) by reason of the death of a member the Minister shall notify the President of the vacancy and the President shall appoint a person to fill the vacancy.

Meetings of the Board

11. (1) The Board shall meet at least once every three months for the dispatch of business at the times and in the places determined by the chairperson.

(2) The chairperson shall at the request in writing of not less than onethird of the membership of the Board convene an extraordinary meeting of the Board at the place and time determined by the chairperson.

(3) The quorum at a meeting of the Board is seven members of the Board or a greater number determined by the Board in respect of an important matter.

(4) The chairperson shall preside at meetings of the Board and in the absence of the chairperson, a member of the Board elected by the members present from among their number shall preside.

(5) Matters before the Board shall be decided by a majority of the members present and voting and in the event of an equality of votes, the person presiding shall have a casting vote.

(6) The Board may co-opt a person to attend a Board meeting but that person shall not vote on a matter for decision at the meeting.

Disclosure of interest

12. (1) A member of the Board who has an interest in a matter for consideration

(a) shall disclose the nature of the interest and the disclosure shall form part of the record of the consideration of the matter; and

(b) shall not participate in the deliberations of the Board in respect of that matter.

(2) A member ceases to be a member of the Board if that member has an interest on a matter before the Board and

(a) fails to disclose that interest; or

(b) participates in the deliberations of the Board in respect of the matter.

Establishment of committees

13. (1) The Board may establish committees consisting of members of the Board or non-members or both to perform a function.

(2) A committee of the Board may be chaired by a member of the Board.

(3) Section 12 applies to members of committees of the Board.

Allowances

14. Members of the Board and members of a committee of the Board shall be paid the allowances approved by the Minister in consultation with the Minister responsible for Finance.

Policy directives

15. (1) Notwithstanding subsection 5, the Minister may give written directives to the Board of Directors on matters of policy in line with the object and functions of the Authority, and the Board of Directors shall comply in a manner consistent with the effective performance of the functions of the Authority.

(2) Subsection (1) shall not be construed to confer on the Minister the power to instruct the Authority on specific technical or operational matters in relation to the object and functions of the Authority.

Administration

Appointment of Director-General

16. (1) The President shall, in accordance with article 195 of the Constitution, appoint a Director-General for the Authority.

(2) The Director-General shall hold office on the terms and conditions specified in the letter of appointment.

(3) The Director-General shall be a person of high moral character and integrity with the relevant professional qualifications and experience related to the functions of the Authority.

Functions of the Director-General

17. (1) The Director-General is responsible for

(a) the day-to-day administration of the affairs of the Authority and is answerable to the Board in the performance of functions under this Act, and

(b) the implementation of the decisions of the Board.

(2) The Director-General shall perform any other functions determined by the Board.

(3) The Director-General may delegate a function to an officer of the Authority but shall not be relieved of the ultimate responsibility for the performance of the delegated function.

Appointment of Deputy Director General

18. (1) The President shall, in accordance with article 195 of the Constitution appoint a Deputy Director General for the Authority.

(2) The Deputy Director-General shall hold office on such terms and conditions as shall be specified in his letter of appointment

(3) The Deputy Director-General shall be responsible to the DirectorGeneral in the performance of his functions under this Act.

(4) The Deputy Director-General shall, subject to the provisions of this Act

(a) assist the Director-General in the discharge of his functions and perform such other functions as the Director General may delegate to him; and

(b) be responsible for the direction of the Authority when the Director-General is absent from Ghana or is otherwise unable to perform his functions.

Appointment of other staff

19. (1) The President shall in accordance with article 195 of the Constitution appoint for the Authority other staff that are necessary for the proper and effective performance of its functions.

(2) Other public officers may be transferred or seconded to the Authority or may otherwise give assistance to it.

(3) The Authority may engage the services of advisers and consultants on the recommendation of the Board.

Finances of the Authority

Funds of the Authority

20. The funds of the Authority include

(a) moneys approved by Parliament;

(b) grants and donations;

(c) internally generated funds;

(d) any other moneys that are approved by the Minister responsible for Finance.

Bank accounts of the Authority

21. Moneys for the Authority shall be paid into bank accounts opened for the purpose with the approval of the Controller and Accountant-General.

Expenses of the Authority

22. The expenses of the Authority shall be charged on the funds of the Authority.

Exemption from tax

23. Subject to article 174 of the Constitution and the Exemptions Act, 2022 (Act 1083), the Authority is exempt from the payment of taxes that the Minister responsible for Finance may, in writing, determine with the prior approval of Parliament.

Borrowing powers

24. (1) Subject to article 181 of the Constitution and section 76 of the Public Financial Management Act, 2016 (Act 921), and with the prior consent in writing of the Minister, the Authority may borrow money from a body corporate or any other person.

(2) For the purposes of securing the money borrowed, the Authority may, with the prior consent in writing of the Minister, mortgage, charge or pledge a right, title or an interest in any of the properties of the Authority.

Accounts and audit

25. (1) The Board shall keep books of accounts and proper records in relation to them in the form approved by the Auditor-General.

(2) The Board shall submit the accounts of the Authority 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.

Annual report and other reports

26. (1) The Board shall within one month after the receipt of the audit report, submit an annual report to the Minister covering the activities and the operations of the Authority for the year to which the report relates.

(2) The annual report shall include:

(a) the report of the Auditor- General;

(b) an assessment of the targets of the Authority; and

(c) a summary of challenges and feedback from stakeholders and recommendations to improve the efficiency and effectiveness of the Authority.

(3) The Minister shall, within one month after the receipt of the annual report, submit the report to Parliament with a statement that the Minister considers necessary.

(4) The Board shall also submit to the Minister any other reports, which the Minister may require in writing.

Information provided to the Authority

Disclosure of information

27. Except for special personal data and information relating to intelligence, and counterintelligence, the provisions of an enactment or law which prohibit or restrict the disclosure of information do not apply to a case where a person furnishes the Authority with information reasonably necessary for the performance of the functions of the Authority under this Act.

Confidentiality of information

28. (1) The Authority, an employee or an agent of the Authority shall not disclose information

(a) obtained by the Authority under or for the purposes of this Act,

(b) furnished to the Authority under or for the purposes of this Act,

(c) which relates to an identifiable individual, and

(d) which is not at the time of the disclosure and has not previously been available to the public from other sources

unless the disclosure is made with lawful authority.

(2) A disclosure is made with lawful authority where the disclosure

(a) is made with the free, informed and explicit consent of the individual or the person for the time being carrying on the business,

(b) was made for the purpose of it being made available to the public under the provisions of this Act,

(c) is made for the purposes of, and is necessary for, the performance of a function under this Act,

(d) is made for the purposes of any civil or criminal proceedings, which arise under or by virtue of this Act or otherwise, or

(e) having regard to the rights, freedoms or legitimate interests of a person, the disclosure is necessary in the public interest.

(3) A person who knowingly or recklessly discloses information in contravention of subsection (1) commits an offence and is liable on summary conviction to a fine of not more than two thousand five hundred penalty units.

Enforcement

Enforcement notice

29. (1) Where the Authority is satisfied that a data controller has contravened or is contravening any of the data protection principles, the Authority shall serve the data controller with an enforcement notice to require that data controller to do any of the following:

(a) to take or refrain from taking the steps specified within the time stated in the notice,

(b) to refrain from processing any personal data or personal data of a description specified in the notice; or

(c) to refrain from processing personal data or personal data of a description specified in the notice for the purposes specified or in the manner specified after the time specified.

(2) In deciding whether to serve an enforcement notice, the Commission shall consider whether the contravention has caused or is likely to cause damage or distress to any person.

(3) An enforcement notice issued in respect of a contravention of a provision of this Act may also require the data controller to rectify, block, erase or destroy other data held by the data controller and which contains an expression of opinion which appears to the Authority to be based on the inaccurate data.

(4) Where

(a) an enforcement notice requires the data controller to rectify, block, erase or destroy personal data, or

(b) the Authority is satisfied that personal data which has been rectified, blocked, erased or destroyed was processed in contravention of any of the data protection principles

the Authority may require the data controller to notify a third party to whom the data has been disclosed of the rectification, blocking, erasure or destruction.

(5) An enforcement notice shall contain a statement of the data protection principle which the Authority is satisfied has been contravened and the reasons for that conclusion.

(6) Subject to this section, an enforcement notice shall not require any of the provisions of the notice to be complied with before the end of the period within which an appeal may be brought against the notice and, if the appeal is brought, the notice may not be complied with pending the determination or withdrawal of the appeal.

(7) Despite subsection (6), the Authority may in exceptional circumstances order that the notice apply immediately.

Cancellation of enforcement notice

30. The Authority may, on its own motion or on an application made by a person on whom a notice is served, cancel or vary the notice to that person.

Request for assessment

31. (1) A person who is affected by the processing of any personal data may on that person's own behalf or on behalf of another person request the Authority to make an assessment as to whether the processing is in compliance with the provisions of this Act.

(2) On receiving a request, the Authority may make an assessment in the manner that the Authority considers appropriate.

(3) The Authority may consider the following in determining whether an assessment is appropriate:

(a) the extent to which the request appears to the Authority to raise a matter of substance;

(b) any undue delay in making the request; and

(c) whether or not the person making the request is entitled to make an application in respect of the personal data in question.

(4) The Authority shall not publish the report of any finding unless

(a) the request is accompanied with the prescribed fee, or

(b) the Authority waives payment based on proven pecuniary challenges of the applicant.

(5) Where the Authority finds that the processing by a data controller is contrary to the provisions of this Act, the Authority shall issue a

determination notice to the data controller specifying the contravention and give the data controller notice to cease business operations and the data controller shall comply immediately.

Complaints redress procedure

32. (1) Any individual who believes that their rights under this Act have been infringed upon by a data controller or data processor shall have the right to lodge a complaint with the Authority.

(2) Complaints shall be submitted to the Authority in writing, electronically, or through any other means designated for this purpose.

(3) Complaints shall contain sufficient information to identify the complainant and the alleged infringement, including details of the data controller or data processor involved, the nature of the alleged violation, and any supporting evidence.

(4) Upon receipt of a complaint, the Authority shall conduct an initial assessment to determine its validity and whether it falls within the jurisdiction of the Authority.

(5) The investigation shall be conducted in accordance with the procedures established by the Authority, ensuring fairness, transparency, and adherence to the principles of natural justice.

(6) The data controller or data processor against whom the complaint is lodged shall be provided with an opportunity to respond to the allegations and present evidence in their defense.

(7) Following the investigation, the Authority shall issue a determination on the complaint, including remedial actions or sanctions deemed necessary and or prescribe compensation commensurate with the harm or distress suffered.

(8) The Authority may by guidelines or directives, prescribe timelines for the complaints redress procedure.

Determination by the Authority

33. (1) Where at any time it appears to the Authority that personal data

(a) is being processed in a manner inconsistent with the provisions of this Act, or

(b) is not being processed with a view to the publication by a person of a journalistic, literary or artistic material which has not previously been published by the data controller the Authority may make a determination in writing to that effect.

(2) The Authority shall give a notice of the determination to the data controller.

Restriction on enforcement in case of processing for special purposes **34.** (1) The Authority shall not serve an enforcement notice on a data controller in relation to the processing of personal data unless a determination has been made by the Authority.

(2) The Authority shall not serve an information notice on a data controller in relation to the processing of personal data unless a determination has been made by the Authority.

Failure to comply with notice

35. (1) A person who fails to comply with an enforcement notice commits an offence and is liable on summary conviction to a fine of not more than ten thousand penalty units or to a term of imprisonment of not more than one year or to both.

(2) A person who, in compliance with an information notice,

(a) makes a statement which that person knows to be false in a material respect, or

(b) recklessly makes a statement which is false in a material respect commits an offence and is liable on summary conviction to a fine of not more than one hundred and fifty thousand penalty units.

(3) It is a defence for a person charged with an offence under sub- section (1) to prove that, that person exercised due diligence to comply with the notice in question.

Compliance audit

36. (1) The Authority shall in writing, authorise an officer of the Authority or any other officer to perform the functions determined by the Authority for the purpose of enforcing the provisions of this Act and the Regulations.

(2) Without limiting subsection (1), a person authorised by the Authority shall:

(a) with a warrant of the court issued by *ex-parte* proceedings, or

(b) with the free, written, informed and explicit consent of the data controller or data processor

enter the premises of a data controller or data processor to audit the data protection processes of a data controller or data processor to ensure compliance with this Act.

(3) Where there has been a data breach or a likely threat of a breach, and it would be impracticable to obtain a warrant due the exigencies of the situation, the Authority may without warrant and with supervision of law enforcement, enter the premises of a data controller or data controller to audit the data protection systems of a data controller or data processor at a reasonable time to ensure compliance with this Act.

(4) The cost of the audit shall be agreed upon between the data controller and the Authority where the data controller or data processor has prior notice of the inspection.

(5) The Authority shall review the findings of the audit, make appropriate determinations and issue sanctions or compliance audit certifications accordingly.

Data Protection Principles

Accountability

37. (1) A data controller who processes personal data shall ensure that the personal data is processed:

(a) without infringing the privacy rights of the data subject;

(b) in a lawful and reasonable manner;

(c) for a specified purpose compatible with further processing;

(d) in a manner that adheres with standards of quality of information and openness;

(e) in manner that prioritises data subject participation.

(2) A data controller or data processor shall in respect of foreign data subjects ensure that personal data is processed in compliance with data protection legislation of the foreign jurisdiction of that subject where personal data originating from that jurisdiction is sent to this country for processing.

(3) A data controller or data processor that is not established in this country shall ensure that personal data is processed in compliance with this Act where personal data originating from this country is processed outside the country.

Lawfulness of Processing

38. (1) A data controller or processor may only process personal data if the purpose for which the personal data is to be processed, is necessary, relevant and not excessive.

(2) A data controller or processor shall not process personal data without the prior written, informed and explicit consent of the data subject unless the purpose for which the personal data is processed is

(a) necessary for the purpose of a contract to which the data subject is a party;

(b) authorised by law;

(c) necessary for the proper performance of a statutory duty; or

(3) Unless otherwise provided by law, a data subject may object to the processing of personal data.

(4) Where a data subject objects to the processing of personal data, the person who processes the personal data shall stop the processing of the personal data.

(5) A person shall collect personal data directly from the data subject.

(6) Despite subsection (5), personal data may be collected indirectly where:

(a) the data is contained in a public record;

(b) the data subject has deliberately made the data public;

(c) the data subject has consented to the collection of the information from another source;

(d) the collection of the data from another source is not likely to prejudice a legitimate interest of the data subject;

(e) the collection of the data from another source is necessary:

(i) for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law;

(ii) for the enforcement of a law which imposes a pecuniary penalty; (iii) for the enforcement of a law which concerns revenue collection;

(iv) for the conduct of proceedings before any court or tribunal that have commenced or are reasonably contemplated;

(v) for the protection of national security; or

(vi) for the protection of the interests of a responsible or third party to whom the information is supplied;

(f) compliance would prejudice a lawful purpose for the collection; or

(g) compliance is not reasonably practicable.

(7) Subject to subsections (2) and (3), a data controller who records personal data shall not retain the personal data for a period longer than is necessary to achieve the purpose for which the data was collected and processed unless *(a)* the retention of the record is required or authorised by law,

(b) the retention of the record is reasonably necessary for a lawful purpose related to a function or activity,

(c) retention of the record is required by virtue of a contract between the parties to the contract, or

(d) the data subject consents to the retention of the record.

(8) Subsection (7) does not apply to records of personal data retained for

(a) historical,

(b) statistical, or

(c) research purposes.

(9) A person who retains records for historical, statistical or research purposes shall ensure that the records that contain the personal data are adequately protected against access or use for unauthorised purposes.

(10) A person who uses a record of the personal data of a data subject to make a decision about the data subject shall

(a) retain the record for a period required or prescribed by law or a code of conduct, or

(b) where there is no law or code of conduct that provides for the retention period, retain the record for a period which will afford the data subject an opportunity to request access to the record.

(11) A data controller shall destroy or delete a record of personal data or deidentify the record at the expiry of the retention period.

(12) The destruction or deletion of a record of personal data shall be done in a manner that prevents its reconstruction in an intelligible form.

(13) A data processor or a person who processes personal data on behalf of a data controller shall

(a)process the data only with the prior knowledge or authorisation of the data controller, and

(b)treat the personal data which comes to the knowledge of the data processor or the other person as confidential.

(14) A data processor or a person who processes personal data on behalf of a data controller shall not disclose the data unless

(a) required by law, or

(b) in the course of the discharge of a duty.

Specification of purpose for collection of personal data

39. (1) A data controller or processor shall collect personal data for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

(2) A data controller who collects personal data shall collect the data for a purpose which is specific, explicitly defined and lawful and is related to the functions or activity of the person.

(3) A data controller who collects data shall take the necessary steps to ensure that the data subject is aware of the purpose for the collection of the data.

Compatibility of Further Processing with Purpose of Collection

40. (1) Where a data controller holds personal data collected in connection with a specific purpose, further processing of the personal data shall be for that specific purpose.

(2) A person who processes data shall take into account

(a) the relationship between the purpose of the intended further processing and the purpose for which the data was collected,

(b) the nature of the data concerned,

(c) the manner in which the data has been collected,

(d) the consequences that the further processing is likely to have for the data subject, and

(e) the contractual rights and obligations between the data subject and the person who processes the data.

(3) The further processing of data is considered to be compatible with the purpose of collection where

(a) the data subject consents to the further processing of the information,

(b) the data is publicly available or has been made public by the person concerned,

(c) further processing is necessary

(i) for the prevention, detection, investigation, prosecution or punishment for an offence or breach of law,

(ii) for the enforcement of a law which imposes a pecuniary penalty,

(iii) for the enforcement of legislation that concerns protection of revenue collection,

(iv) for the conduct of proceedings before any court or tribunal that have commenced or are reasonably contemplated, or

(v) for the protection of national security;

(d) the further processing of the data is necessary to prevent or mitigate a serious and imminent threat to

(i) public health or safety, or

(ii) the life or health of the data subject or another individual;

(f) the data is used for historical, statistical or research purposes and the person responsible for the processing ensures that:

(i) the further processing is carried out solely for the purpose for which the data was collected, and

(ii) the data is not published in a form likely to reveal the identity of the data subject; or

(g) the further processing of the data is in accordance with this Act.

Quality of Information

41. Subject to data participation rights of the data subject, a data controller who processes personal data shall ensure that the data is complete, accurate, up to date and not misleading having regard to the purpose for the collection or processing of the personal data.

Openness

42. (1) A data controller who intends to collect personal data shall ensure that the data subject is aware of

(a) the nature of the data being collected;

(b) the name and address of the person responsible for the collection;

(c) the purpose for which the data is required for collection;

(d) whether or not the supply of the data by the data subject is discretionary or mandatory;

(e) the consequences of failure to provide the data;

(f) the authorised requirement for the collection of the information or the requirement by law for its collection;

(g) the recipients of the data;

(h) the nature or category of the data; and

(i) the existence of the right of access to and the right to request rectification of the data collected before the collection.

(3) Where the data is collected from a third party, the data subject shall be given the information specified in subsection (1) before the collection of the data or as soon as practicable after the collection of the data.

(4) Subsection (1), shall not apply in the following situations where it is necessary:

(a) to avoid the compromise of the law enforcement power of a public body responsible for the prevention, detection, investigation, prosecution or punishment of an offence;

(b) for the enforcement of a law which imposes a pecuniary penalty;

(c) for the enforcement of legislation which concerns revenue collection;

(d) for the preparation or conduct of proceedings before a court or tribunal that have been commenced or are reasonably contemplated;

(e) for the protection of national security;

(f) to avoid the prejudice of a lawful purpose;

(g) to ensure that the data cannot be used in a form in which the data subject is identified; or

(h) because the data is to be used for historical, statistical or research purposes.

Data security safeguards

43. (1) A data controller or processor shall take the necessary steps to secure the integrity of personal data in the possession or control of the data controller or processor through the adoption of appropriate, reasonable, technical and organisational measures to prevent

(a) loss of, damage to, or unauthorised destruction; and

(b) unlawful access to or unauthorised processing of personal data.

(2) For the purpose of subsection (1), the data controller shall take reasonable measures to

(a) identify reasonably foreseeable internal and external risks to personal data under the possession or control of the data controller or processor;

(b) establish and maintain appropriate safeguards against the identified risks;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies.

(3) A data controller or processor shall observe

(a) generally accepted information security practices and procedures, and

(b) specific industry or professional rules and regulations.

(4) Data controllers who collect, process, or store data shall implement policies and procedures for the secure disposal of data when it is no longer needed for its intended purpose.

(5) Data disposal procedures shall be designed to ensure the permanent and irretrievable removal of data from all storage devices and systems.

(6) The Authority shall –

(a) regulate the deployment of technological and organisational measures to enhance personal data protection; and

(b) foster the development of personal data protection technologies, in accordance with recognised international best practices and applicable international law.

Data subject participation

44. (1) A data subject shall have the right to:

(a) access their personal data;

(b) request rectification, correction or erasure of their personal data;

(c) request to be forgotten;

(c) request restriction of processing of their personal data.

(2) A data controller shall facilitate the exercise of these rights and respond to requests within twenty-one working days.

Application of Principles of Data Protection

Retention of records

45. (1) A data controller who records personal data shall not retain the personal data for a period longer than is necessary to achieve the purpose for which the data was collected and processed unless

(a) the retention of the record is required or authorised by law,

(b) the retention of the record is reasonably necessary for a lawful purpose related to a function or activity,

(c) retention of the record is required by virtue of a contract between the parties to the contract, or

(d) the data subject consents to the retention of the record.

(2) Subsection (1) does not apply to records of personal data retained for

(a) historical,

(b) statistical, or *(c)* research purposes.

(3) A person who retains records for historical, statistical or research purposes shall ensure that the records that contain the personal data are adequately protected against access or use for unauthorised purposes.

(4) A person who uses a record of the personal data of a data subject to decide about the data subject shall

(a) retain the record for a period required or prescribed by law or a code of conduct, or

(b) where there is no law or code of conduct that provides for the retention period, retain the record for a period which will afford the data subject an opportunity to request access to the record.

(5) A data controller shall destroy or delete a record of personal data or de-identify the record at the expiry of the retention period.

(6) The destruction or deletion of a record of personal data shall be done in a manner that prevents its reconstruction in an intelligible form.

Ownership of records

46. (1) As far as personal data is concerned, personal data shall remain the property of the data subject and shall not be deemed to be owned by any other person or entity solely by virtue of its processing.

(2) A data controller or data processor shall be deemed to be a custodian or steward of personal data and shall only process such data in accordance with this Act and for the purposes explicitly consented to by the data subject or permitted under law.

(3) Any provision of another enactment that purports to confer proprietary rights over personal data to a person other than the data subject shall, to the extent of such inconsistency, be void and of no effect.

(4) For the avoidance of doubt, ownership of computer equipment, databases, or software systems used to store or process personal data shall not confer ownership of the personal data contained therein.

Data Protection Impact Assessment

47. (1) Where a data processing activity is likely to pose real risk to the rights and freedoms of a data subject, the data controller or data processor shall conduct a data protection impact assessment prior to processing the personal data.

(2) In consideration of the rights and legitimate interests of data subjects, the data protection impact assessment must encompass the following elements:

(a) details of the intended processing activities, the purposes of the intended processing activities, and any legitimate interests pursued by the data controller or data processor.

(b) an evaluation of the legal basis, and appropriateness of the processing activities with respect to their intended purposes.

(c) an appraisal of the potential risks posed to the rights and freedoms of data subjects.

(d) the proposed measures to mitigate identified risks, along with security safeguards aimed at ensuring the protection of personal data and demonstrating compliance with the relevant provisions outlined in this Act.

(3) Should a data protection impact assessment conducted under this section reveal that the processing of data would likely result in a real high risk to the rights and freedoms of a data subject, the data controller or data processor is obligated to submit a report to the Authority for review and approval before proceeding with the processing.

(4) The Authority shall provide comprehensive guidelines for the execution of impact assessments as outlined in this section, ensuring clarity and consistency in their implementation.

Legitimate interest assessment in data processing

48. (1) A data controller shall ensure that any processing of personal data based on legitimate interests is preceded by a Legitimate Interest Assessment.

(2) The Legitimate Interest Assessment shall include:

(a) a determination that the processing serves a legitimate interest of the data controller or a third party;

(b) an evaluation of whether the processing is necessary to achieve the identified interest; and

(c) an assessment of whether the legitimate interest outweighs the rights and freedoms of the data subject.

(3) The data controller shall document the Legitimate Interest Assessment and maintain records demonstrating compliance with this section.

(4) Where the data subject objects to processing on grounds relating to their rights and freedoms, the data controller shall reassess the Legitimate Interest Assessment and cease processing where the interests of the data subject override the legitimate interest.

(5) The Authority may request access to the Legitimate Interest Assessment documentation to verify compliance with this section.

Data protection by design and by default

49. (1) A data controller or data processor shall implement appropriate technical and organisational measures which are designed—

(a) to implement the data protection principles in an effective manner; and

(b) to integrate necessary safeguards for that purpose into the processing.

(2) The duty under subsection (1) applies both at the time of the determination of the means of processing the data and at the time of the processing.

(3) A data controller or data processor shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose is processed, taking into consideration—

(a) the amount of personal data collected;

(b) the extent of its processing;

(c) the period of its storage;

(d) its accessibility; and

(e) the cost of processing data and the technologies and tools used.

(4) To give effect to this section, the data controller or data processor shall consider measures such as

(a) to identify reasonably foreseeable internal and external risks to personal data under the person's possession or control;

(b) to establish and maintain appropriate safeguards against the identified risks;

(c) to the pseudonymization and encryption of personal data;

(d) to the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(e) to verify that the safeguards are effectively implemented; and

(f) to ensure that the safeguards are continually updated in response to new risks or deficiencies.

(5) The Minister shall by legislative instrument specify categories of data controllers and industry-specific data controllers that must implement this requirement.

Data processor to comply with security measures

50. (1) A data controller shall ensure that a data processor who processes personal data for the data controller, establishes and complies with the security measures specified under this Act.

(2) The processing of personal data for a data controller by a data processor shall be governed by a written contract.

(3) A contract between a data controller and a data processor shall require the data processor to establish and maintain the confidentiality and security measures necessary to ensure the integrity of the personal data.

(4) Where a data processor is not domiciled in this country, the data controller shall ensure that the data processor complies with the relevant laws of this country.

Notification of security compromises

51. (1) A data controller shall notify the Authority and the data subject, without any undue delay, of any security breach affecting personal data being processed by or on behalf of the data controller.

(2) The notification shall be made immediately or within 72 hours after the discovery of the unauthorised access or acquisition of the data.

(3) A data controller shall take steps to ensure the restoration of the integrity of the information system.

(4) A data controller shall delay notification to the data subject where the security agencies or the Authority inform the data controller that notification will impede a criminal investigation.

(5) The notification to a data subject shall be communicated by

(a) registered mail to the last known residential or postal address of the data subject or

(b) electronic mail to the last known electronic mail address of the data subject.

(c) placement in a prominent position on the website of the responsible party;

(d) publication in the media; and

(e) any other manner that the Authority may direct.

(6) A notification shall provide sufficient information to allow the data subject to take protective measures against the consequences of unauthorised access or acquisition of the data.

(7) The information shall include, if known to the data controller, the identity of the unauthorised person who may have accessed or acquired the personal data.

(8) Where the Authority has grounds to believe that publicity would protect a data subject who is affected by the unauthorised access or acquisition of data, the Authority may direct the data controller to publicise in the specified manner, the fact of the compromise to the integrity or confidentiality of the personal data.

(9) A data controller who fails to notify the Authority within the stipulated 72 hours timeframe shall be subject to an administrative penalty of not less than two thousand penalty units and not more than hundred thousand penalty units.

(10) The Authority may, in addition to compensation granted to a data subject, impose an administrative penalty where it is of the opinion that security compromise resulted from the data controller's inadequate compliance with the provisions of this Act relating to safeguarding personal data.

Correction of personal data

52. (1) A data subject may request a data controller to

(a) correct or delete personal data about the data subject held by or under the control of the data controller that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, or

(b) destroy or delete a record of personal data about the data subject held by the data controller that the data controller no longer has the authorisation to retain or

(c) destroy or delete a record of personal data about the data subject generally without reason if it is not unlawful.

(2) On receipt of the request, the data controller shall comply with the request or provide the data subject with credible evidence in support of the data.

(3) Where the data controller and the data subject are unable to reach an agreement and if the data subject makes a request, the data controller shall attach to the record an indication that a request for the data has been made but has not been complied with.

(4) Where the data controller complies with the request, the data controller shall inform each person to whom the personal data has been disclosed of the correction made.

(5) The data controller shall notify the data subject of the action taken as a result of the request.

(6) The data subject shall bear the consequences of deletion or destruction of personal data that is essential for a service, purpose, or objective, or if it results in a breach of law, breach of legal obligations between parties, invalidation of service or application, eligibility of service, denial of service, unreliability of record, incorrect and incomplete outcomes.

Application of Emerging Technologies

53. (1) Data controllers utilising advanced methods in data processing shall ensure compliance with data protection principles.

(2) Technology-driven decisions impacting data subjects shall be explainable, contestable, and subject to human oversight to prevent bias and harm.

(3) Privacy enhancing technologies shall be employed to ensure transparency and accountability in automated decision-making processes.

(4) The Authority shall regulate data processing involving these technologies, conduct risk assessments, and impose penalties for noncompliance.

(5) Systems used in critical sectors including but not limited to health, energy, finance, banking, government services, transportation and logistics, food and agriculture shall undergo periodic audits bi-annually to evaluate ethical implications and ensure adherence to national and international standards.

(6) Data controllers developing or deploying such technologies shall implement safeguards to protect personal data from unauthorised access, discrimination, and unethical use.

(7) In addition to any other requirements under an enactment for timebeing, any service that utilises personal data to provide tailored experience, including but not limited to social media services; video-on-demand or streaming services; messaging application services; and e-commerce services and relies on emerging technologies, shall undergo a mandatory data protection impact assessment prior to launch and shall implement personal data governance frameworks consistent with data protection principles.

Rights of Data Subjects and Others

Right to access to personal data

54. (1) A data controller shall

(a) inform an individual who is the data subject of the processing of the individual's personal data held by the data controller or another person on behalf of the data controller;

(b) upon the request of a data subject, give to the data subject, a description of

(i) the personal data of which that individual is the data subject;

(ii) the purpose for which the data is being or is to be processed; and

(iii) the recipient or class of recipients to whom the data may be disclosed;

(c) communicate in an intelligible form to the data subject

(i) information which constitutes personal data of which that individual is the subject;

(ii) information which is available to the data controller as to the source of the data; and

(d) inform the individual who is the data subject of the logic or rationale behind the decision that was made based on the processing where the processing constitutes the sole basis for the taking of a decision which significantly affects that individual.

(2) Where the data constitutes a trade secret, the provision of data related to the logic or rationale involved in any decision taken does not apply.

(3) A data controller shall not comply with a request under subsection (1) unless the data controller is supplied with the data that the data controller may reasonably require to identify the person making the request and to locate the data which that person seeks.

(4) Where a data controller is unable to comply with the request without disclosing data related to another individual who may be identified from the information, the data controller shall not comply with the request unless

(a) the other individual consents to the disclosure of the data to the person who makes the request, or

(b) it is reasonable in all circumstances to comply with the request without the consent of the other data subject

(5) A reference to data related to another individual in subsection (4) includes a reference to data which identifies that individual as the source of the data requested.

(6) For the purposes of subsection (4)*(b),* to determine whether it is reasonable to comply with the request without the consent of the other individual concerned, regard shall be had in particular, to

(a) any duty of confidentiality owed to the other individual,

(b) any steps taken by the data controller to seek the consent of that other individual,

(c) whether the other individual is capable of giving consent, and *(d)* any express refusal of consent by the other individual.

(7) An individual who makes a request under this section may specify that the request is limited to personal data of any description.

(8) Subject to subsection (5), a data controller shall comply with a request under this section promptly and in any event within twenty-one working days from the date of receipt of the request.

(9) Where the Authority is satisfied on the application or a complainant in relation to matters under subsections (1) to (8) that the data controller has failed to comply with the request, the Authority may order the data controller to comply with the request.

(10) The data which is supplied pursuant to a request may take into account an amendment or deletion made between the time of the request and the time when the data is supplied.

(11) A data controller shall create an enabling environment for a timely fulfillment of a request to access their personal data.

(12) For the purposes of this section another individual may be identified from the data disclosed if that individual can be identified

(a) from that data, or

(b) from that data and any other data which in the reasonable belief of the data controller are likely to be in, or come into the possession of the data subject who made the request.

Right to be informed

55. (1) A data subject who provides proof of identity may request a data controller to

(a) confirm to the data subject whether the data controller holds personal data about that data subject,

(b) give a description of the personal data which is held by the data controller including data about the identity of a third party or a category of a third party who has or has had access to the information, and

(c) correct data held on the data subject by the data controller.

(2) The data subject shall make the request

(a) in a manner determined by the data controller;

(b) within a reasonable time;

(c) in a form that is acceptable.

Right to give and withdraw consent

56. (1) A data subject shall have the right to grant and withdraw consent for the processing of their personal data, that is to opt-in and opt-out, provided such consent is:

(a) freely given, specific, informed, and unambiguous;

(b) expressed through a clear affirmative act, including written, electronic, or other recorded means;

(c) revocable in accordance with the provisions of this Act.

(2) A data controller or processor shall ensure that the request for consent is presented in a manner distinguishable from other terms and conditions, using clear and plain language.

(3) Consent obtained through coercion, deception, or undue influence shall be deemed invalid and unenforceable.

(4) A data subject shall have the right to withdraw consent at any time, without prejudice to the lawfulness of processing based on consent prior to its withdrawal.

(5) Upon withdrawal of consent, the data controller or processor shall:

(a) immediately cease processing the affected personal data, except where otherwise authorized by law.

(b) ensure the prompt deletion or anonymization of such data, unless retention is necessary for legal compliance, contractual execution, or the establishment, exercise, or defense of legal claims.

(6) The mechanism for withdrawal of consent shall be as simple as the mechanism for granting consent and shall not impose an undue burden on the individual.

Right to data portability

57. (1) A data subject shall, at a cost borne by the data subject, have the right to receive the personal data concerning him or her, which has been provided to a data controller, in a structured, commonly used and machinereadable format and have the right to transmit those data to another data controller without hindrance from the data controller to which the personal data have been provided.

(2) In exercising the right to data portability, the data subject shall have the right to have the personal data transmitted directly from one data controller to another, either manually or by electronic means.

(3) Under subsection (2), the responsibility for ensuring the secure and safe transfer of personal data rests with the data controller initiating the transmission.

(4) The right to data portability shall not apply in the following circumstances:

(a) when the processing of personal data is necessary for tasks carried out in the public interest or under the authority of a public institution.

(b) where the exercise of data portability infringes upon the rights and freedoms of third parties.

(c) if the direct transfer of personal data between data controllers is impractical or not technically viable.

Right to complain

58. (1) A data subject shall have the right to lodge a complaint with the data controller regarding any alleged violation of their rights under this Act.

(2) The data controller shall provide an accessible mechanism for submitting complaints and shall respond within 72 hours of receiving the complaint.

(3) Where a data subject is dissatisfied with the response from the data controller or does not receive a response within the prescribed period, the data subject may lodge a complaint with the Authority.

(4) The Authority shall investigate complaints and impose penalties where necessary.

Right to compensation

59. (1) Where a data subject suffers damage or distress through the contravention by a data controller of the requirements of this Act, that data subject is entitled to compensation from the data controller for the damage or distress.

(2) In proceedings under this section, a data controller who provides documentary evidence of efforts towards accountability, can use that as a defence to prove that the data controller took reasonable care in all the circumstances to comply with the requirements of this Act.

Right to object processing of personal data

60. (1) A data subject shall at any time by notice in writing to a data controller require the data controller to cease or not begin processing for a specified purpose or in a specified manner.

(2) A data controller shall within three working days after receipt of a notice inform the individual in writing

(a) that the data controller has complied, or *(b)*
of the reasons for non-compliance.

(3) (3) Where the Authority is satisfied that the complaint is justified, the Authority may order the data controller to comply.

Right to erasure and the right to be forgotten

61. (1) A data subject shall have the right to request from the data controller the erasure of personal data concerning them without undue delay, and the data controller shall be obliged to erase such personal data without undue delay where one of the following grounds applies:

(a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;

(c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;

(d) the personal data has been unlawfully processed;

(e) the personal data must be erased for compliance with a legal obligation in applicable law.

(2) A data subject shall have the right to request from the data controller to be forgotten concerning them without undue delay, and the data controller shall be obliged to forget such personal data without undue delay without providing justification for requesting to be forgotten.

(3) For the purposes of this Act, the right to be forgotten means in addition to erasure of personal data kept by the data controller or data processor, the right to complete removal to the greatest extent possible, of personal data available to the public through links, copies, websites, replications of that personal data or other means, as a result of disclosures made by the data controller.

(4) For the purposes of this section, "greatest extent possible" shall not be construed in subsection (3) as an excuse for non-performance of the right to be forgotten but shall be interpreted in light of technical limitations, jurisdictional boundaries and conflicting public and private interest to mean, subject to subsection (7):

(a) all actions within the control of the data controller to forget all personal data from all systems;

(b) all actions in respect of notification of third parties who were given access to the data or replicated the data to forget all personal data from all systems;

(c) all actions in respect of request of removal of links to personal data from major search engines within the applicable jurisdictions;

(d) all actions requiring the application of reasonable technical measures to forget personal data from all systems;

(e) all actions to maintain records of efforts of forgetting personal data from all systems;

(f) all actions to forget personal data from all systems without delay and within a 30-day window of request by the data subject, unless complexity is justified to the Authority.

(5) A data controller who is obliged to act on the right to be forgotten is expected to take all reasonable steps, including technical measures, taking into account available technology and cost of implementation, to inform other data controllers and data processors who are processing personal data that the data subject has requested the right to be forgotten.

(6) Subject to subsection (7), where the data controller is of the view that cost of implementation of the right to be forgotten exceeds the capacity of the data controller which could not have been reasonably predicted, the data controller shall request the Authority to make an assessment of the technology and cost of implementation of the right to be forgotten without delay and within a 30-day window of request by the data subject.

(7) The technology and cost of implementation of the right to be forgotten shall be borne by the data controller even if the cost exceeds the expected expenses, but where the technology and cost of implementation of the right to be forgotten exceeds the capacity of the data controller which could not have been reasonably predicted according to the Authority, the data subject shall bear not less than 30% of the total expenditure assessed by the Authority.

(8) The right of erasure and to be forgotten shall not apply where:

(a) personal data must be retained in accordance with the laws of the country; or

(c) after diligent efforts to inform or compel third-party data controllers to erase the personal data of the subject, it is technically proven difficult erase or forget the personal data.

(9) Despite subsection (1) and (2), the data subject shall bear the consequences of a erasure or forgetting of personal data that is essential for a service, purpose, or objective, or if it results in a breach of law, breach of legal obligations between parties, invalidation of service or application, ineligibility for a service, denial of service, unreliability of record, incorrect and incomplete outcomes.

Right to amend

62. (1) A data subject shall have the right to request change of personal data or removal of information held by the data controller.

(2) Notwithstanding subsection (1), a data subject has the right to request amendment of personal data held by the data controller.

(3) The data controller shall rectify such data within three working days of receiving a valid request.

(4) Despite subsection (1), the data subject shall bear the consequences of a deletion or destruction of personal data that is essential for a service, purpose, or objective, or if it results in a breach of law, breach of legal obligations between parties, invalidation of service or application, ineligibility for a service, denial of service, unreliability of record, incorrect and incomplete outcomes.

Right to prevent processing of personal data for direct marketing

63. (1) A data controller shall not provide, use, obtain, procure or provide personal data related to a data subject for the purposes of direct marketing without the prior written, free, explicit and informed consent of the data subject, and proof of consent shall be maintained for audit purposes.

(2) Where prior written, free, explicit and informed consent of the data subject, adata subject is entitled at any time by notice in writing to a data controller to require the data controller not to process personal data of that data subject for the purposes of direct marketing.

(3) Without prejudice to subsection (1) and (2), unidentifiable data or information of a person may be used direct marketing.

(4) Where the Authority is satisfied on a complaint by a person who has given notice in subsection (1), that the data controller has failed to comply with the notice, the Authority may order that data controller to comply with the notice.

(5) No data controller shall transmit marketing via telecommunication networks without the prior written, free, explicit and informed consent of the data subject.

Right to control processing of personal data for election campaign

64. (1) A data controller shall provide an opportunity for a person to optout of processing of their personal data for purposes of election campaign in national, district, organisational, institutional or student election, and proof of opt-out shall be maintained for audit purposes.

(2) A data subject is entitled at any time by notice in writing to a data controller to require the data controller not to process personal data the purposes of election campaigning.

(3) Where the Authority is satisfied on a complaint by a person who has given notice in subsection (1), that the data controller has failed to comply with the notice, the Authority may order that data controller to comply with the notice.

Rights in relation to automated decision-taking

65. (1) An individual is entitled at any time by notice in writing to a data controller to require the data controller to ensure that any decision taken by or on behalf of the data controller which significantly affects that individual is not based solely on the processing by automated means of personal data, in respect of which that individual is the data subject.

(2) Automated processing shall include auto-filling user data into forms; spam filtering in email systems; automatically generated invoice; auto-tagging of photos; emerging technology systems; automated chatbots; facial and emotional recognition.

(3) To give effect to subsection (1) a data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which affects the data subject.

(4) Despite the absence of a notice, where a decision which significantly affects an individual is based solely on that processing

(a) the data controller shall as soon as reasonably practicable notify the individual that the decision was taken on that basis, and

(b) the individual is entitled, by notice in writing to require the data controller to reconsider the decision within twenty-one days after receipt of the notification from the data controller.

(4) The data controller shall within twenty-one days after receipt of the notice, inform the individual in writing of the steps that the data

controller intends to take to comply with the notice. (5) This section does not apply to a decision made

(a) in the course of considering whether to enter into a contract with the data subject,

(b) with a view to entering into the contract,

(c) in the course of the performance of the contract,

(d) for a purpose authorised or required by or under an enactment, or

(e) in other circumstances prescribed by the Minister.

(6) Where the Authority is satisfied on a complaint by a data subject that a person taking a decision has failed to comply, the Authority may order the data controller to comply.

(7) An order for compliance under subsection (5) shall not affect the rights of a person other than the data subject or the data controller.

Rights in relation to manual data

66. (1) A data subject is entitled at any time by notice in writing to require a data controller

(a) to rectify, block, erase or destroy manual data which is inaccurate or incomplete, or

(b) to cease to hold manual data in a manner which is incompatible with the legitimate purposes pursued by the data controller.

(2) A notice under subsection (1) shall state the reasons for believing that the data

(a) is inaccurate or incomplete, or

(b) is held in a way incompatible with the legitimate purposes pursued by that data controller.

(3) Where the Authority is satisfied on a complaint by a person who has given notice that the data controller has failed to comply with the notice, the Authority shall give appropriate direction to the data controller to comply with the notice.

(4) For the purposes of this section, personal data is incomplete if the data is of the kind that its incompleteness would constitute a contravention of data protection principles provided in this Act.

Processing of Special Personal Data

Processing of special personal data prohibited

67. (1) Unless otherwise provided by this Act, a data controller shall not process personal data which relates to

(a) a child in accordance with the Constitution, or

(b) the religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life or criminal behavior of an individual.

(2) A data controller may process special personal data in accordance with this Act where

(a) processing is necessary, or

(b) the data subject explicitly consents to the processing.

(3) The processing of special personal data is necessary where it is for the exercise or performance of a right or an obligation conferred or imposed by law on an employer.

(4) Special personal data shall not be processed unless the processing is necessary for the protection of the vital interests of the data subject where

(a) it is impossible for consent to be given by or on behalf of the data subject,

(b) the data controller cannot reasonably be expected to obtain the consent of the data subject

(5) Special personal data shall not be processed unless the processing is carried out for the protection of the legitimate activities of a body or association which

(a) is established for non-profit purposes,

(b) exists for political, philosophical, religious or trade union purposes;

(c) relates to individuals who are members of the body or association or have regular contact with the body or association in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

(6) The processing of special personal data shall be presumed to be necessary where it is required

(a) for the purpose of or in connection with a legal proceeding,

(b) to obtain legal advice,
(c) for the establishment, exercise or defence of legal rights,
(d) in the course of the administration of justice, or
(e) for medical purposes and the processing is
(i) undertaken by a health professional, and
(ii) pursuant to a duty of confidentiality between patient and health professional.

(7) In this section, "medical purposes" includes the purposes of preventive medicine, medical diagnosis, medical research, provision of care and treatment and the management of healthcare services by a medical or dental practitioner or a legally recognised traditional healer.

(8) A person shall not process special personal data in respect of race or ethnic origin unless the processing of the special personal data is

(a) necessary for the identification and elimination of discriminatory practices, and
(b) carried out with appropriate safeguards for the rights and freedoms of the data subject.

(9) The collection of biometric data for subscriber registration shall require explicit consent and must be in accordance with the principles outlined in this Act.

(10) The Minister may in consultation with the Authority by legislative instrument prescribe further conditions which may be taken by a data controller for the maintenance of appropriate safeguards for the rights and freedoms of a data subject related to processing of special personal data.

Consent for the processing of personal data of a child

68. (1) A data controller shall obtain the consent of a parent or legal guardian before processing the personal data of a child for any purpose, unless such processing is permitted or required by law.

(2) The consent obtained shall be clear, explicit, specific, informed, and freely given, and shall be obtained in a manner that is appropriate to the age and maturity of the child.

(3) A data controller shall make reasonable efforts to verify that consent has been given by a parent or legal guardian before processing personal data of a child, considering appropriate technology and best practices.

(4) Parents or legal guardians shall have the right to withdraw consent for the processing of their child's personal data at any time.

(5) A data controller shall provide parents or legal guardians with easy and accessible means to withdraw consent and shall immediately cease processing the child's data upon receipt of a withdrawal request.

(6) Where a child provides personal data directly to an application or platform, the data controller shall implement age verification mechanisms to determine whether parental consent is necessary.

Demand for medical information or health records

69. (1) Except provided by law, a data controller is not required to disclose medical data or health records to third parties.

(2) A contract that demands the disclosure of medical data without free, explicit and informed consent of the data subject shall be unenforceable.

(3) Subject to subsection (4) and (5), a data subject shall not be required to provide medical data or health records to any person which

(a) consist of information related to the physical, mental health or mental condition of that data subject, or

(b) has been made by or on behalf of a health professional in connection with the care of that data subject.

(4) In accordance with the Public Health Act, 2012 (Act 851), medical data shall be processed without consent of the data subject if it necessary for contact tracing and outbreak control.

(5) A person other than healthcare providers and medical administrators, shall not process information relating to medical data or health records unless it is reasonably necessary for the:

(a) Certification as to medical fitness for work under law;

(b) Performance of an employer's reporting obligations on persons with disabilities under law;

(c) Payment of compensation as required by law; and *(d)* Enforcement of a court order.

Exemption related to religious or philosophical beliefs of data subject

70. (1) The prohibition on processing of personal data related to religious or philosophical beliefs does not apply in specific circumstances where:

(a) processing is carried out by a spiritual or religious organization or its branch concerning its members.

(b) processing is carried out by an institution founded on religious or philosophical principles, provided it aligns with the institution's objectives and is necessary to achieve its aims.

(2) These exemptions are not to be misused to obstruct essential data processing.

Rectification, blocking, erasure and destruction of personal data

71. (1) Where the Authority is satisfied on a complaint of a data subject that personal data on that data subject is inaccurate, the Authority may order the data controller to

(a) rectify,

(b) block,

(c) erase, or

(d) destroy the data.

(2) Subsection (1) applies whether or not the data is an accurate record of information received or obtained by the data controller from the data subject or a third party.

(3) Where the data is an accurate record of the information, the Authority may make an order requiring the data controller to supplement the statement of the true facts which the Authority considers appropriate.

(4) Where the data complained of has been rectified, blocked supplemented, erased or destroyed, the data controller is required to notify third parties to whom the data has been previously disclosed of the rectification, blocking, supplementation, erasure or destruction.

(5) To determine whether it is reasonably practicable to require the notification, the Authority shall have regard to the number of persons to be notified.

Data Protection Register

Establishment of Data Protection Register

72. (1) There is established by this Act a register of data controllers to be known as the Data Protection Register.

(2) The Authority shall keep and maintain the Register.

(3) A data controller shall register with the Authority.

Application for registration

73. (1) An application for registration as a data controller shall be made to the Authority and the applicant shall furnish the following particulars:

(a) the business name and address of the applicant;

(b) the name and address of the company's representative within Ghana where the company is an external company;

(c) a description of the personal data to be processed and the category of persons whose personal data are to be collected;

(d) an indication as to whether the applicant holds or is likely to hold special personal data.

(e) a description of the purpose for which the personal data is being or is to be processed;

(f) a description of a recipient to whom the applicant intends to disclose the personal data.

(g) the name or description of the country to which the applicant may transfer the data;

(h) the class of persons or where practicable the names of persons whose personal data is held by the applicant.

(i) a general description of measures to be taken to secure the data; and

(j) any other information that the Authority may require.

(2) An applicant who knowingly supplies false information in support of an application for registration as a data controller and knowingly causes fraud in relation to the application commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than one year or to both.

(3) A data controller's headquarters shall be registered separately from its branches, each maintaining independent compliance with the provisions of this Act.

(4) A parent company and its subsidiary companies shall each register as separate data controllers, ensuring distinct legal and operational responsibilities under this Act.

Right to refuse registration

74. (1) The Authority shall not grant an application for registration under this Act where

(a) the particulars provided for inclusion in an entry in the Register are insufficient.

(b) the appropriate safeguards for the protection of the privacy of the data subject have not been provided by the data controller; and

(c) in the opinion of the Authority, the person making the application for registration does not merit the grant of the registration.

(2) Where the Authority refuses an application for registration as a data controller, the Authority shall inform the applicant in writing within twenty-one working days after submission of an application

(a) of its decision and the reasons for the refusal, and

(b) the applicant may apply for judicial review to the High Court against the refusal.

(3) A refusal of an application for registration is not a bar to reapplication.

Grant of certificate of registration

75. (1) The Authority shall

(a) register an applicant if the applicant has satisfied the conditions required for registration

(b) provide the applicant with a certification of registration upon approval of the application.

(2) The applicant shall pay a prescribed fee upon registration.

(3) The Authority shall issue a registration certificate within a period no longer than seven working days after approval of application.

(4) Upon receipt of certificate, copies of the certificate shall be displayed at all outlets of the data controller.

(5) A certificate of registration issued under this Act shall be valid for a period of twelve months.

Renewal of registration

76. (1) Registration shall be renewed every twelve months.

(2) A data controller whose registration certificate has expired shall cease processing of personal data until after renewal of registration certificate.

(3) A data controller in the process of renewing their registration shall have to produce a compliance report.

(4) A data controller who fails to renew their registration or delays the renewal process for a period longer than three months shall be subject to an administrative penalty of five thousand penalty units which will attract a five percent monthly interest.

Removal from register

77. The Authority shall, at the request of the data controller to whom an entry in the Register relates and after submission of necessary documentation, remove the data controller's name from the Register at any time.

Cancellation or suspension of registration

78. (1) The Authority has the power to cancel a registration for good cause.

(2) A registered data controller shall may have their registration cancelled or suspended under the following circumstances:

(a) failure to adhere to prescribed standards for data processing and security.

(b) supplying inaccurate details during registration or renewal processes.

(c) handling personal information without the necessary legal basis or consent.

(d) inadequate safeguards leading to unauthorized access, loss, or exposure of personal data.

(e) neglecting to update or maintain registration information within the mandated period.

Processing of personal data without registration prohibited

79. A data controller who has not been registered under this Act shall not process personal data.

Access by the public

80. (1) The Authority shall provide facilities to make the information contained in the Register available for inspection by members of the public.

(2) The Authority shall supply a member of the public with a copy of the particulars contained in an entry made in the Register on payment of the prescribed fee.

Duty to notify changes

81. (1) A data controller shall notify the Authority of changes in the registered particulars within ten working days.

(2) A data controller who contravenes subsection (1) shall be subject to an administrative penalty of five thousand penalty units.

Failure to register

82. (1) A person who fails to register as a data controller but processes personal data shall be subject to an administrative penalty of not less than two thousand penalty units and more than a hundred thousand penalty units.

(2) A person who fails to register as a data controller within three months after incorporation shall be subject to an administrative penalty of not less than two thousand penalty units and not more than hundred thousand penalty units.

Assessable processing

83. (1) The Minister may by Executive Instrument specify actions which constitute assessable processing if the Minister considers the assessable processing likely to

(a) cause substantial damage or substantial distress to a data subject, or

(b) otherwise significantly prejudice the privacy rights of a data subject;

(2) On receipt of an application for registration, the Authority shall consider

(a) whether the processing to which the notification relates is assessable, or

(b) if the assessable processing complies with the provisions of this Act.

(3) The Authority shall within twenty-eight days from the day of receipt of the application, inform the data controller whether the processing is likely to comply with the provisions of this Act.

(4) The Authority may extend the initial period by a further period which does not exceed fourteen days or other period that the Authority may specify.

(5) The assessable processing in respect of which a notification has been given to the Authority shall not be carried on unless

(a) the period of twenty-eight days has elapsed, or

(b) before the end of that period, the data controller receives a notice from the Authority under subsection (3).

(6) A data controller who contravenes this section commits an of- fence and is liable on summary conviction to a fine of not more than one hundred and fifty thousand penalty units or to a term of imprisonment of not more than five years or to both.

Appointment of data protection officers

84. (1) A data controller shall appoint a certified and qualified person to serve as a data protection officer.

(2) A person appointed as a data protection officer shall be trained and certified by the Authority.

(3) The data protection officer is responsible for

(a) Monitoring the data controller's compliance with the provisions of this Act.

(b) Updating the data controller or processor on regulatory changes and updates.

(c) Advising the data controller or processor on their obligations under the Act.

(d) Acting as the primary liaison between the data controller or processor and the Authority.

(4) An authorisation under this section may

(a) impose a duty on a data protection officer in relation to the Authority, and

(b) confer a function on the Authority in relation to a data protection officer.

(5) A data protection officer may be an employee of the data controller.

(6) The Authority shall provide the needed guidelines for the qualification to be appointed as a data protection officer.

(7) A person shall not be appointed as a data protection officer unless the person satisfies the criteria set by the Authority.

(8) A data controller who fails to appoint a data protection officer shall be subject to an administrative penalty of not less than two thousand penalty units and not more than fifty thousand penalty units.

Fees

85. The Authority, in consultation with the Minister shall prescribe fees for the purpose of its functions.

Accreditation of data protection service providers

Accreditation of data protection service providers

86. (1) An individual or institution shall not provide a data protection service within the country unless that person obtains a licence issued by the Authority in accordance with this Act.

(2) A person who contravenes (1) by providing data protection services without a licence issued by the Authority shall be subject to an administrative penalty of not more than fifty thousand penalty units.

Application for accreditation

87. (1) A person who seeks to provide a data protection service shall apply in writing to the Authority.

(2) The application shall be made in the prescribed form and accompanied by the:

(a) supporting documentation, and

(b) prescribed fee, that the Authority shall determine.

(3) An individual seeking accreditation as a data protection service provider shall be required to undergo training and obtain certification from the Authority as a certified data protection professional, or possess an equivalent certification recognised by the Authority.

(4) The Authority shall issue further guidelines in support of the application process.

Grant of accreditation

88. (1) Where the Authority is satisfied that

(a) the applicant meets the requirements of the Authority for the grant of a licence,

the Authority may grant the licence to the applicant,

(2) Upon receiving an application for a licence, the Authority shall provide written notification of its decision to the applicant within thirty working days.

(3) An accreditation granted by the Authority is subject to the terms and conditions specified by the Authority.

(4)

(5) An accredited institution who uses a licence for a purpose other than that for which the licence was granted shall have the licence revoked.

Non transferability of accreditation

89. (1) A person granted an accreditation shall not transfer that licence to another person.

(2) A person who transfers a licence contrary to subsection (1) commits an offence and is liable on summary conviction to a fine of not less than five thousand penalty units and not more than ten thousand
penalty units.

Validity of accreditation

90. (1) A licence granted under this Act is valid for twelve months from the date that the licence is granted.

(2) An accredited institution who intends to continue operations as a data protection service provider shall, not later than one month before the expiration of the licence, apply to the Authority in writing for a renewal of the licence.

(3) An accredited institution who intends to continue operations as a data protection service provider and fails to begin the renewal process within the timeline stipulated in (2) may be subject to an administrative penalty.

Suspension of accreditation

91. (1) The Authority may suspend a licence issued under this Act for a period of not more than six months where the accredited institution fails to comply with a condition specified in the licence.

(2) The Authority shall, before exercising the power of suspension under this section,

(a) give the accredited institution thirty days' notice in writing of the intention to do so, and

(b) specify in the notice the grounds on which the Authority intends to suspend the licence.

(3) The Authority shall, within twenty-eight days of the suspension of a licence, notify the data protection service provider concerned of the suspension.

Revocation of accreditation

92. (1) The Authority may revoke a licence issued under this Act if the Authority considers that

(a) the licence has been obtained by fraud or misrepresentation.

(b) the licensee has ceased to carry on the business for which the licensee is licensed.

(c) the licensee has been convicted of an offence under this Act or an offence involving fraud, dishonesty or moral turpitude.

(d) a circumstance existed at the time the license was granted or renewed that the Authority was unaware of, which would have prevented the Authority from granting or renewing the licence of the licensee if the Authority had been aware of the circumstance at that time.

(e) the licensee no longer meets the requirements for holding the licence; or

(f) it is not in the public interest for the licensee to continue to carry on the business of a licensee.

Direct Sanctioning Powers of the Authority

Sanctions and penalties

93. (1) Administrative penalties imposed under this section shall be paid within twenty-one working days of issuance of the penalty notice.

(2) Any individual or entity subject to an administrative penalty under this section may appeal against the decision to impose the penalty through the established review mechanism outlined in Section 89.

General penalty

94. A person who contravenes a section of this Act for which a penalty is not provided shall be subject to an administrative penalty of not less than fifty thousand penalty units and not more than hundred thousand penalty units.

Review mechanism

95.(1) In the event that a data controller is dissatisfied with a determination made by the Authority pursuant to this Act, the data controller shall have the right to request a review of the said determination.

(2) The data controller shall submit a written request for review to the Authority within seven working days from the date of receiving the determination.

(3) The request for review shall clearly outline the grounds for the request and any supporting evidence.

(4) Upon receipt of the request for review, the Authority shall promptly acknowledge the request and provide the data controller with information regarding the process.

(5) The Authority shall review the determination and make a decision within thirty working days, which shall be communicated to the data controller.

(6) If the data controller is dissatisfied with the decision on the review, they may seek further redress on appeal through judicial review or other legal remedies available in the High Court.

Cross-Border Transfers of Personal Data

Basis for cross border transfer of personal data

96. (1) Notwithstanding the opportunity to under a cross-border transfer personal data under subsection (3), a data controller shall make reasonable efforts to localise data provided that data localisation does not impair its business or operations.

(2) There shall be no requirement for a data controller to localise personal data unless:

(a) the personal data is critical to national defence, security and intelligence of the country; or

(b) the personal data concern national identity ID systems and civil registration systems including voter databases

(c) the personal data concerns children's data, biometric data, health records and genetic data.

(3) Subject to subsection (2), the Authority may grant approval to a data controller for the cross-border transfer children's data, biometric data, health records and genetic data with the consent of the data subject or any other person under an obligation in law to make decisions for the data subject for the time-being.

(4) A data controller shall transfer personal data outside Ghana only if the following conditions are met:

(a) the data subject has provided written, free, explicit and informed consent to the proposed transfer after being informed of the possible risks involved;and

(b) *(i)* the transfer is necessary for the performance of a contract, for administrative, educational, financial, medical or professional reasons, between the data subject and the data controller or for the implementation of pre-contractual measures taken at the data subject's request; or

(ii) the transfer is necessary for the conclusion or performance of a contract concluded, or for administrative, educational, financial, medical or professional reasons in the interest of the data subject between the data controller and a third party; or

(iii) or the transfer is necessary for the establishment, exercise, or defense of legal claims; or

(iv) the transfer is necessary to protects the vital interests of the data subject or other individuals where the data subject is physically or legally incapable of giving consent; and

(c) the transfer is authorised by the Authority where it involves large-scale data, and in all cases, following an assessment that adequate safeguards for the protection of personal data are in place, including appropriate contractual clauses and binding corporate rules or other mechanisms approved by the Authority.

(3) In all cases, personal data emanating from Ghana shall be processed in accordance with the provisions of this Act.

Safeguards prior to transfer of personal data out of Ghana

97. (1) A data controller shall process special personal data out of Ghana upon obtaining consent of all affected data subjects and upon obtaining approval from the Authority.

(2) The Authority may request a person who transfers data to another country to demonstrate the effectiveness of security safeguards and the existence of compelling legitimate interests.

(3) The Authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined by the Authority.

(4) A data controller that processes large-scale data where a data processing activity is likely to pose real risk to the rights and freedoms of a data subject, shall conduct a Transfer Impact Assessment on all data transfers in or outside the jurisdiction subject to the approval of the Authority.

(5) The Authority shall provide relevant guidelines in support of subsection (4).

Exemptions

National security

98. (1) The processing of personal data is exempt from the provisions of this Act for the purposes of

(a) public order,

(b) public safety,

*(c)*public morality,

(d) national security, or *(e)* public interest.

(2) Despite, subsection (1), nothing shall prevent a person from pursuing an action in court whether by injunction or otherwise that their rights have been unfairly prejudiced.

Crime and taxation

99. (1) The processing of personal data is exempt from the provisions of this Act for the purposes of

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of an offender, or

(c) the assessment or collection of a tax or duty or of an imposition of a similar nature.

(2) Personal data is exempt from the non-disclosure provisions in any case in which

(a) the disclosure is for a purpose mentioned in subsection (1), and

(b) the application of those provisions in relation to the disclosure is likely to prejudice any of the matters mentioned in that subsection.

Health, education and social work

100. Personal data on the following subjects shall not be disclosed except where the disclosure is required by law:

(a) personal data which relates to the physical, mental health or mental condition of the data subject,

(b) personal data in respect of which the data controller is an educational institution and which relates to a pupil at the institution, or

(c) personal data of similar description.

Regulatory activity

101. (1) The provisions of this Act do not apply to the processing of personal data for protection of members of the public

(a) against loss or malpractice in the provision of

(i) banking,

(ii) insurance,

(iii) investment,

(iv) other financial services, or

(v) digital services
(vi) management of a body corporate;

(b) against dishonesty or malpractice in the provision of professional services;

(c) against the misconduct or mismanagement in the administration of a non-profit making entity;

(d) to secure the health, safety and welfare of persons at work; or

(e) to protect non-working persons against the risk to health or safety arising out of or in connection with the action of persons at work.

(2) The processing of personal data is exempt from the subject information provisions of this Act if it is for the discharge of a function conferred by or under an enactment on

(a) Parliament,

(b) a local government authority,

(c) the administration of public health or public financing of health care, prevention, control of disease and the monitoring and eradication of disease.

Journalism, literature and art

102. (1) A person shall not process personal data unless

(a) the processing is undertaken by a person for the publication of a literary or artistic material;

(b) the data controller reasonably believes that publication would be in the public interest; and

(c) the data controller reasonably believes that, in all the circumstances, compliance with the provision is incompatible with the special purposes.

(2) Subsection (1) does not exempt a data controller from compliance with the data principles related to

(a) lawful processing,

(b) minimality,

*(c)*further processing,

(d) data subject participation

*(e)*information quality, and *(f)* security safeguards.

(3) For the purposes of subsection (1) *(b)*, in considering whether the data controller believes that the publication would be in the public interest or

is reasonable, regard may be had to the compliance by the data controller with any code of practice which is

(a) relevant to the publication in question, and

(b) designated by the Minister for purposes of this subsection.

Research, history and statistics

103. (1) The further processing of personal data for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which the data was obtained.

(2) Personal data processed for research purposes in compliance with the relevant conditions may be kept indefinitely.

(3) Personal data which is processed only for research purposes is exempt from the provisions of this Act if

(a) the data is processed in compliance with the relevant conditions, and

(b) the results of the research or resulting statistics are not made available in a form which identifies the data subject or any of them.

(4) Personal data is not to be treated as processed otherwise than for research purposes merely because the data is disclosed

(a) to any person for research purposes only,

(b) to the data subject or a person acting on behalf of the data subject,

(c) at the request or with the consent of the data subject or a person acting on behalf of the data subject, or

(d) in circumstances in which the person making the disclosure has reasonable grounds to believe that the disclosure falls within this section.

Disclosure required by law or made in connection with a legal proceeding **104.** Personal data is exempt from the provisions on non-disclosure where the disclosure is required by or under an enactment, any rule of law or by the order of a court.

Domestic purposes

105. Personal data which is processed by an individual only for the purpose of that individual's personal, family or household affairs is exempt from the data protection principles.

Confidential references given by data controller

106. Personal data is exempt from the data protection principles if it consists of a reference given in confidence by the data controller for the purposes of

(a) education, training or employment of the data subject,

(b) the appointment to an office of the data subject, or

(c) the provision of any service by the data subject.

Armed Forces

107. Personal data is exempt from the subject information provisions where the application of the provisions is likely to prejudice the combat effectiveness of the Armed Forces of the Republic.

Judicial appointments and honours **108.**

Personal data processed to:

(a) assess a person's suitability for judicial office, or

(b) confer a national honour,exempt from the subject information provisions of this Act.

Public service or ministerial appointment

109. The Minister may by legislative instrument make Regulations to prescribe exemptions from the subject information provisions of personal data processed to assess a person's suitability for

(a) employment by the government, or

(b) any office to which appointments are made by the President.

Examination marks

110. Personal data is exempt from the provisions of this Act if it relates to examination marks processed by a data controller

(a) to determine the results of an academic, professional or other examination or to enable the results of the examination to be determined, or

(b) in consequence of the determination of the results.

Examination scripts

111. Personal data which consists of information recorded by candidates during an academic, professional or other examination is exempt from the provisions of this Act.

Professional privilege

112. Personal data is exempt from the subject information provisions if it consists of information in respect of which a claim to professional privilege or confidentiality between client and a professional adviser could be maintained in legal proceedings.

Miscellaneous and general provisions

General duties of the Authority

113. (1) The Authority shall provide guidelines and promote the observance of good practice to ensure compliance with this Act.

(2) The Authority may charge the fees that the Authority in consultation with the Minister determines for the provision of services by the Authority.

(3) The Authority is responsible for conducting public education and awareness campaigns to the public on data subject rights and data controllers' obligations under this Act.

Codes, guidelines and certification

114. (1) The Director-General may, for the purpose of this Act—

(a) issue guidelines or codes of practice for the data controllers, data processors and data protection officers;

(b) offer data protection certification standards and data protection seals and marks in order to encourage compliance of processing operations with this Act;

(c) require certification or adherence to code of practice by a third party;

(d) develop sector specific guidelines in consultation with relevant stakeholders in areas such as health, financial services, education, social protection and any other area the Director General may determine.

International co-operation

115. In relation to international organizations, the Authority shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including jurisdictional conflicts with third countries.

Prohibition to purchase, obtain or disclose personal data 116. (1)

A person shall not

(a) purchase the personal data or the information contained in the personal data of another person;

(b) knowingly obtain or knowingly or recklessly disclose the personal data or the information contained in the personal data of another person; or

(c) disclose or cause to be disclosed to another person the information contained in personal data.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine of not more than twenty thousand

penalty units or to a term of imprisonment of not more than two years or to both.

Prohibition of sale of personal data

117. (1) A person who sells or offers to sell personal data of another person commits an offence and is liable on summary conviction to a fine of not more than fifty thousand penalty units.

(2) For this section's purposes, an advertisement indicating that personal data is or may be for sale is an offer to sell the data.

Conditional request for personal data prohibited

118. (1) A person who provides goods, facilities or services to the public shall not require a person to supply or produce a particular record as a condition for the provision of the goods, facilities or services to that person.

(2) Subsection (1) does not apply where the imposition of the requirement is required or authorised under an enactment, rule of law or in the public interest.

(3) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine of not more than fifty thousand penalty units.

Transmission of notices by electronic or other means

119. (1) A requirement that a notice, request, particulars or application to which this Act applies shall be in writing is satisfied where the text of the notice, request, particulars or application

(a) is transmitted by electronic means in a manner specified by the Authority,

(b) is received in legible form, and

(c) is capable of being used for subsequent reference.

(2) The Minister may by Regulations exempt a notice, request, particulars or application from these requirements.

Service of notices by the Authority

120. (1) A notice authorised or required by this Act to be served on or given to a person by the Authority may

(a) if that person is an individual, be served on that individual by delivery to that individual,

(i) by post addressed to that individual at that Individual's usual or last known place of residence or business,

(ii) by leaving the notice at that individual's usual or last known place of residence or business, or

(iii) by sending it to an electronic mail address specified by the individual for service of notices;

(b) if that person is a body corporate or unincorporated, be served on that body

(i) by post to the principal officer of the body at its principal office,

(ii) by addressing it to the principal officer of the body and leaving it at that office, or

(iii) by sending it to an electronic mail address specified by the body for service of notices under this Act; and

(c) if that person is a partnership, be served on that partnership

(i) by post to the principal office of the partnership,

(ii) by addressing it to that partnership and leaving it at that office, or

(iii) by sending it to an electronic mail address specified by that partnership for service of notices under this Act.

(2) This section does not limit any other lawful method of serving or giving a notice.

Regulations

121. (1) The Minister may in consultation with the Authority by legislative instrument make Regulations to

(a) extend the transitional period for a data controller in existence at the commencement of this Act,

(b) specify the conditions that are to be satisfied for consent to be given,

(c) prescribe further conditions which may be taken by a data controller for the maintenance of appropriate safeguards, for the

rights and freedoms of a data subject related to the processing of special personal data,

(d) make different provisions for different situations,

(e) exempt notices, requests, particulars or applications from the requirements under the Act, and

(f) provide generally for any other matter necessary for the effective implementation of the provisions of this Act.

(2) A person who commits an offence under the Regulations is liable on summary conviction to a fine of not more than five thousand penalty units.

Interpretation

122. In this Act unless the context otherwise requires

"assessable processing" means processing of a description specified in an Executive Instrument made by the Minister under section 83(1);

"bias" means a distorted inclination or prejudice in support or against a thing, perspective, idea, person or a group in an unfair way;

"biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a person, which allows or confirms the unique identification of that person and includes but not limited to; physical traits, fingerprints, facial images, iris or retina scans, palm or hand geometry, and behavioral traits like voice patterns;

"binding corporate rules" means personal data protection laws, rules, administrative decisions or judicial order or judgments, guidelines, regulations, directives or policies which are adhered to by a data controller or data processor established in another country for cross-border transfers of personal data;

"business" includes trade, vocation, enterprise or profession;

"child" refers to an individual under the age of eighteen as defined by the Constitution;

"consent" means voluntary agreement given by individuals either in writing or electronically, for the processing of their personal data, based on clear and informed understanding of the purposes and consequences;

"corporate finance service" means a service which consists of

(a) underwriting in respect of the issue or the placing of issues of any instrument;

(b) advice to undertakings on capital structure, industrial strategy and related matters and advice and service related to mergers and the purchase of an undertaking, or

(c) services related to the underwriting referred to in paragraphs *(a)* and *(b);*

"cross-border" refers to the transfer, processing, or sharing of personal data beyond the jurisdiction in which it was originally collected;

"data" means information which

(a) is processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or

(d) does not fall within paragraph *(a),(b)* or *(c)* but forms part of an accessible record;

"data controller" 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 protection impact assessment" means an assessment of the impact of the envisaged processing operations on the protection of personal data;

"data protection principles" means the principles set out in sections 37 to 44 of this Act;

"data processor" means any person other than an employee of the data controller who processes the data on behalf of the data controller;

"data protection functions" means functions that relate to the protection of personal data in the course of data processing;

"data protection officer" means a professional appointed by a data controller in accordance with section 84 to monitor the compliance by the data controller in accordance with the provisions of the Act;

"data protection service provider" means an individual or an institution accredited by the Authority to offer data protection services;

"data protection services" means except for legal, compliance and policy consultancy advice, a range of activities and solutions designed to provide technical tools for personal data management.

"data protection system" means a multifaceted system of strategies, policies, laws, processes and technologies designed to protect and manage personal data and to meet compliance requirements under the Act;

"data subject" means an individual who is the subject of personal data;

"direct marketing" includes the communication by whatever means of any advertising or marketing material which is directed to particular individuals;

"digital service" means services delivered electronically whether traditionally or by internet with minimal physical interaction, and includes

(a) social media platforms;
(b) e-commerce platforms;
(c) video-on-demand or streaming platforms;

(d) messaging applications,
(e) fintech software platforms;
(f) online banking platforms;

"emerging technologies" means new and evolving technological innovations, including but not limited to artificial intelligence, blockchain, the Internet of Things, and other cutting-edge digital technologies that may impact data processing, protection, and security;

"emotional recognition" means a form of data processing detects the emotional state of a data subject using common sources such as facial expressions, voice patterns, text, psychological signals, body language or other behavioural indicators;

"enactment" includes an enactment passed after the commencement of this Act;

"entity" refers to an organisation, company, or individual that is involved in processing personal data. This includes data controllers and data processors.

"examination" includes any process for determining the knowledge, intelligence, skill or ability of a candidate by reference to the candidate's performance in a test, work or other activity;

"exempt manual data" means information in respect of which a controller is not required to register before manual processing or use;

"foreign data subject" means data subject information regulated by laws of a foreign jurisdiction sent into Ghana from a foreign jurisdiction wholly for processing purposes;

"good cause" means any failure to comply with or a violation of any of the data protection principles, enforcement or other notices issued by the Authority;

"good practice" means the practice in the processing of personal data in a way that the likelihood of causing substantial damage or distress is reduced; "government department" includes a Ministry, Department or Agency and a body or authority exercising statutory functions on behalf of the State;

"harm" means injury whether physical, psychological or reputational, financial or social which causes loss or suffering;

"health professional " means a registered medical practitioner or a recognised traditional healer or any person who is registered to provide health services under any law for the time being in force;

"information notice" means notice given by the Authority pursuant to a determination under section 28;

"instrument" means any instrument related to a publicly traded security;

"intelligence" or "counterintelligence" means processing of personal data for purposes related to national security, defense, public safety, or the prevention, detection, investigation, or prosecution of criminal offenses authorised by the Republic's security and intelligence agencies;

"international business or economic transaction means any business where the subject matter of the transaction is international or either of the parties to the transaction have a foreign nationality or reside in different countries or, in the case of companies, the place of their central management and control is outside the country;

"legitimate interest" means a genuine, necessary and justifiable reason for a data controller to process personal data, not limited to commercial, marketing or security or administrative purposes, that does not override the data subject's rights and freedoms or harm the data subject;

"large-scale data" means vast amounts of personal data whether or not retrieved from different geographical areas that require complex processing, and includes personal data processed by video-on-demand

platforms or streaming services, messaging applications, social media platforms and financial systems;

"medical data" means special personal data that identifies a natural person and indicates either a diagnosis, test results, symptoms and complaints, prescriptions, progress report, medical history, family medical history, behavourial lifestyle, biometric data, medical information related to insurance claims, information relating to health care services or information relating to overall physical, mental and emotional wellbeing, including anatomical and physiological information.

"Minister" means the Minister responsible for Communications;

"monitoring" means, the tracking of an individual or observation with data processing techniques, whether or not to make decisions concerning him or her;

"person" means any natural or legal person, including individuals, corporations, and other entities recognised by law;

"personal data" means any information relating to an identified or identifiable natural person, and includes one or combination of the following, whether identified by manual or automated processing:

(a) direct identifiers including 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 including 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 including 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 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.

"personal data management" means the practices and systems individuals use to control their personal data, including how the data is processed i.e., collected, stored, accessed, and shared.

"prescribed fee" means a fee set out in relation to any Regulations on fees made pursuant to this Act;

"principal office" in relation to a registered company, means the registered office or other address that the company may specify for the delivery of correspondence;

"principal officer" in relation to a body, means the secretary or other executive officer charged with the conduct of the general affairs of the body;

"privacy" means the right of individuals to control the access and use of their personal information, ensuring confidentiality and security;

"processing" means an operation or activity or set of operations by electronic or other means that concerns data or personal data and the

(a) collection, organisation, 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;

"profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects

concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, language or birth; personal preferences, interests, behaviour, location or movements;

“public funds” has the same meaning assigned to it in Article 175 of the 1992 Constitution;

"public interest" means any lawful and necessary data processing activity that supports the collective good of society such as protecting national security, promoting public health, or ensuring justice—while still respecting the fundamental rights of data subjects;

“public register” means a register which pursuant to a requirement imposed

(a) by or under an enactment, or

(b) in pursuance of any international agreement is open to

(i) inspection by the public, or

(ii) inspection by a person who has a legitimate interest;

“publish” in relation to journalistic, literary or artistic material means to make available to the public or any class of the public, journalistic, literary or artistic material;

“pupil” in relation to a school in this country means a registered person within the meaning of the Pre-Tertiary Education Act, 2020 (Act 1049) of any registered school;

“recipient” means a person to whom data is disclosed including an employee or agent of the data controller or the data processor to whom data is disclosed in the course of processing the data for the data controller, but does not include a person to whom disclosure is made with respect to a particular inquiry pursuant to an enactment;

“registered company” means a company registered under any enactment related to an incorporated or unincorporated entity for the time being in force in the country;

"Regulations" means Regulations made under this Act; "relevant authority" means

(a) a government department,
(b) local authority, or
(c) any other statutory authority;

"relevant filing system" means any set of data that relates to an individual which although not processed by means of equipment operating automatically in response to instructions given for processing that data, the set is structured, either by reference to an individual or by reference to a criteria that relates to the individual in a manner that specific information which relates to a particular individual is readily accessible;

"relevant function" means

(a) a function conferred on a person by or under an enactment,
(b) a function of the government, a Minister of State or a government department, or
(c) any other function which is of a public nature and is exercised in the public interest;

"relevant record" means any record that relates to a conviction or caution held by a law enforcement agency or security agency;

"research purposes" includes statistical or historical purposes;

"security agency" means an agency connected with national security as determined by the National Security Council;

"special personal data" means personal data which consists of information that relates to

(a) the race, colour, ethnic or tribal origin of the data subject;
(b) the political opinion of the data subject;
(c) the biometric data of the data subject;
(d) the religious beliefs or other beliefs of a similar nature, of the data subject;

(e) the physical, medical, mental health or mental condition or DNA of the data subject;
(f) the sexual orientation of the data subject;
(g) the Authority or alleged Authority of an offence by the individual; or
(h) proceedings for an offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in the proceedings; "special purposes" means any one or more of the following:
(a) the purpose of journalism,
(b) where the purpose is in the public interest,
(c) artistic purposes, and
(d) literary purposes;

"subject information provisions" means the provisions under this Act which deal with the right of a data subject to access information from a data controller;

"subsequent processing" means after the data has arrived in or passed through the country, it is subjected to any operation or set of operations within the country in a way that is described as "processing" under this Act;

"teacher" includes a head teacher and the principal of a school to whom disclosure is or may be made as a result of, or with a view to, an inquiry by or on behalf of that person made in the exercise of a power conferred by law;

"the Act" refers to the Data Protection Act, 2012 (Act 843);

"the Authority" refers to the Data Protection Authority of Ghana established under section 3 of this Act;

"the Constitution" refers to the 1992 Constitution of Ghana;

"the relevant conditions" in relation to the processing of personal data, means the conditions

(a) that the data is not processed to support measures or decisions with respect to particular individuals, and

(b) that the data is not processed in the way that substantial damage or distress is caused or is likely to be caused to the data subject; and

"third party" in relation to personal data, means a person other than

(a) the data subject,

(b) the data controller, or

(c) any data processor or other person authorised to process data for the data controller or processor.

Repeals and savings

123. The Data Protection Act, 2012 (Act 843) is hereby repealed.

Transitional Provisions

124. Any decision, authorisation, permit or certificate issued by the predecessor of the Authority in respect of data protection shall remain valid until it is revoked, cancelled, terminated by the Authority, or expires in accordance with its terms.

Commencement

125. The Minister shall specify the date when this Act shall come into force by publication in the *G*azette.