ARRANGEMENT OF SECTIONS

Section

A

BILL

ENTITLED

CYBERSECURITY (AMENDMENT) BILL, 2025

AN ACT to amend the Cybersecurity Act, 2020 (Act 1038) to confer powers on the Cyber Security Authority to investigate and prosecute cybercrime on the authority of the Attorney-General and recover proceeds of cybercrime; to revise the object and functions of the Cyber Security Authority; to revise the governance and administration of the Cyber Security Authority; to revise the enforcement powers of the Cyber Security Authority and to provide for related matters.

Section 3 of Act 1038 Amended

1. The Cybersecurity Act, 2020 (Act 1038) referred to in the Act as the "principal enactment" is amended by substitution for section 3, of

"**Objects of the Authority**

3. The objects of the Authority are to:

(a) regulate cybersecurity activities in the country;
(b) prevent, manage and respond to cybersecurity threats and cybersecurity incidents;
(c) regulate owners of critical information infrastructure in respect of cybersecurity activities, cybersecurity service providers, cybersecurity professionals and practitioners, and cybersecurity establishments in the country;
(d) promote the development of cybersecurity in the country to ensure a secured and resilient digital ecosystem;
(e) prevent and detect cybercrime;
(f) to facilitate the confiscation of proceeds of cybercrime;
(g) establish a platform for cross-sector engagement on matters of cybersecurity for effective co-ordination and co-operation between key public institutions and the private sector;
(h) create awareness of cybersecurity matters; and
(i) collaborate with States, inter-governmental bodies, international organisations and international agencies to promote the cybersecurity of the country.".

Section 4A inserted

2. The principal enactment is amended by the insertion after section 4, of

"**Further Functions of the Authority**

4A. The Authority, shall in addition to the functions in section 4, carry out the following functions:

(a) subject to article 88 of the Constitution, to investigate and on the authority of the Attorney-General, prosecute cybercrime under this Act;
(b) establish standards for certifying the security of innovative products, Artificial Intelligence, cloud technology, quantum computing, big data, Internet of Things (IoT) , blockchain-based technology and any other emerging technologies;
(c) certify the security of innovative products Artificial Intelligence, cloud technology, quantum computing, big data, Internet of Things (IoT), blockchain-based technology and any other emerging technologies, in accordance with the standards established pursuant to paragraph (b);
(d) accredit the cybersecurity establishments of critical information infrastructure owners, cybersecurity service providers, cybersecurity practitioners and professionals and other relevant persons or institutions;
(e) accredit non-profit cybersecurity institutions and cybersecurity professional bodies;
(f) promote the online protection of women, elderly, persons with disabilities and underserved populations;
(g) collaborate with relevant institutions to develop mechanisms including technical security solutions and guidelines on the usage of smart technology and other emerging technologies; and
(h) promote the protection of digital rights as it relates to cybersecurity.".

Section 5 of Act 1038 amended

3. The principal enactment is amended in section 5 by the addition after subparagraph (iv) of paragraph (a) of subsection (1), of

"(v) Foreign Affairs and Regional Integration; and

(vi) Gender, Children and Social Protection.".

Section 13 of Act 1038 amended

4. The principal enactment is amended in section 13 by:

(a) the substitution for paragraph (d) of subsection (2), of

"(d) the Executive Director of the Data Protection Commission or any successor official or entity by whatever name designated, or a representative of the Executive Director with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Executive Director;";

(b) the substitution for paragraph (g) and (k) respectively of subsection (2), of

"(g) the Director of the National Intelligence Bureau or any successor official or entity by whatever name designated, or a representative of the Director with the requisite knowledge and skills in cybercrime, and cybersecurity matters, nominated by the Director;

(k) the Director General of National Signals Bureau or any successor official or entity by whatever name designated, or a representative of the Director with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Director;";

(c) the addition after paragraph (r) of subsection (2), of

"(s) Any other person the Minister may nominate, on the advice of the Authority.".

(d) the addition after subsection (13), of

"(14) A member of the JCC who is absent from three consecutive meetings without sufficient cause ceases to be a member of the JCC.

(15) Where there is a vacancy, the Minister shall notify the President of the vacancy, and the President shall appoint a person to fill the vacancy for the unexpired term.".

Section 14 of Act 1038 amended

5. The principal enactment is amended in section 14 by the substitution for subsection (1), of

"14 (1). The Joint Cybersecurity Committee shall collaborate with the Authority and the sectors or institutions represented on the Committee for the implementation of relevant cybersecurity measures including but not limited to the following ways:

(a) identification of cybersecurity risks that may affect critical information infrastructure or the overall cybersecurity of the country;
(b) development of cybersecurity policies and guidelines based on identified risks, best practices and international standards to mitigate cybersecurity risks;
(c) coordination of cybersecurity activities between sectors and entities to ensure that all cybersecurity efforts are aligned to prevent overlap and gaps;
(d) facilitate the sharing of information between sectors and entities in a secure manner and in compliance with relevant data protection laws;
(e) collaboration with sectors or institutions to tackle cybercrime including the provision of a platform for incidence sharing and incidence response mechanisms to facilitate;

(f) evaluation of the effectiveness of implemented cybersecurity measures based on established metrics with a view to continuously improve the cybersecurity measures; and

(g) collaboration with the Authority to educate the public on matters related to cybercrime and cybersecurity.".

Section 15A inserted

6. The principal enactment is amended by the insertion after section 15, of

"**Appointment of Deputy-Directors General**

15A. (1) The President shall in accordance with article 195 of the Constitution appoint such Deputy Directors-General as are necessary for the performance of the functions of the Authority.

(2) The Deputy Directors-General shall hold office on the terms and conditions specified in the letters of appointment.

(3) The Deputy Directors-General shall act in the absence of the Director-General and perform any other functions as determined by the Board.

(4) The Deputy Directors-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 or the Board may delegate to him;

(b) perform functions related to the object and functions of the Authority on the direction or authority of the Director-General or the Board; and

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

Section 20A inserted

7. The principal enactment is amended by the insertion after section 20, of

"**Terms and Conditions of Service of Staff of the Authority**

20A. (1) The terms and conditions of service of the staff of the Authority shall not be less favourable than the staff of the security and intelligence agencies.

(2) The conditions of service attached to posts of legal officers of the Authority shall not be less than that of the posts attached to that of legal officers of the Attorney-General of the same rank.

(3) Staff shall, in addition to monthly salaries, be eligible for the payment of any gratuity, allowance, pension, subsidy or benefit to members in respect of their service or resignation or retirement.".

Section 20B inserted

8. The principal enactment is amended by the insertion after section 20, of

"**Powers of police**

20B. (1) The Director-General, Deputy Director-General and other authorised officers shall exercise the powers of a Police Officer, including the powers of arrest, search and seizure and have the same rights, protections immunities conferred on a Police officer in the Criminal and Other Offences (Procedure) Act, 1960 (Act 30), the Police Service Act, 1970 (Act 350) and any other law related to a Police officer in the performance of their functions under the Act.".

Section 31 of Act 1038 amended

9. The principal enactment is amended by substitution for section 31, of:

"**Sources of money for the Fund**

31. The sources of moneys for the Fund include:

(a) seed money approved by Parliament;
(b) moneys which may become lawfully payable to the Authority for the Fund;
(c) 50% of all fines arising from criminal penalties under the Act;
(f) grants, gifts, donations and other voluntary contributions;
(g) 12% of the communications service tax for the Fund per annum;
(h) 9 % corporate tax for the Fund per annum;
(i) a charge determined by the Authority in accordance with the Fees and Charges (Miscellaneous Provisions) Act, 2018 (Act 983) and levied on persons licensed by the Bank of Ghana to carry on business;
(j) a proportion of the fees charged on all government electronic services determined by the Authority; and
(h) any other moneys approved by Parliament for the Fund.".

Section 35 of Act 1038 amended

10. The principal enactment is amended by substitution for section 35, of

"**Designation of critical information infrastructure**

35. (1) The Minister may, on the advice of the Authority, designate a computer system or computer network as a critical information infrastructure if the Minister considers that the computer system or computer network is essential for

(a) national security,
(b) the economic and social well-being of citizens, or
(c) public health and safety.

(2) Where the Minister designates a computer system or computer network as a critical information infrastructure, the Minister shall publish the sector of the designated critical information infrastructure in the *Gazette* and, the owner of the Critical Information Infrastructure shall be notified of the designation.

(3) The Minister shall, in making a determination under subsection (1), consider if the computer system or computer network is necessary for:

(a) the security, defence or international relations of the country;
(b) the production, preservation or identity of a confidential source of information related to the enforcement of criminal law;
(c) the provision of services directly related to
    (i) communications and telecommunications infrastructure;
    (ii) banking and financial services;
    (iii) public utilities
    (iv) public transportation; and
    (v) public key infrastructure;
(d) the protection of public safety and public health, including systems related to essential emergency services;
(e) an international business or communication affecting a citizen of Ghana or any other international business in which a citizen of Ghana or the Government has an interest;
(f) the Legislature, Executive, Judiciary, Public Services or security agencies; or
(g) digital services;
(h) services related to the supply chain in the critical information infrastructure ecosystem; and
(i) any other services determined by the Minister, on the advice of the Authority.

(4) The Minister shall, by publication in the *Gazette*, establish the procedure for the regulation of a critical information infrastructure.".

Section 36 of Act 1038 amended

11. The principal enactment is amended by substitution for section 36, of

"**Registration of critical information infrastructure**

36. (1) The Owner of the designated critical information infrastructure shall register their critical information infrastructure with the Authority, and shall pay the prescribed annual registration and designation fee as determined by the Authority or stipulated in a legislative instrument.

(2) For compliance purposes, the owner of an unregistered critical information infrastructure shall receive a notification of registration letter from the Authority to comply with the Act.

(3) During registration, the owner of a critical information infrastructure shall nominate a point of contact and submit details of the nominee to the Authority.

(4) The owner of a critical information infrastructure shall submit to the Authority, verified details of critical information infrastructure, through the channels and modalities determined by the Authority.

(5) The Authority shall validate the information submitted by the owner of a critical information infrastructure, and the owner shall receive a Certificate of Registration upon completion of registration requirements.

(6) The Authority shall through the issuance of guidelines or directives determine:

(a) further requirements for the registration of a critical information infrastructure;
(b) the procedure for the registration of a critical information infrastructure; and
(c) any other matter relating to the registration of a critical information infrastructure.

(7) Where there is any change in the legal ownership of a designated critical information infrastructure, the owner of the designated critical information infrastructure shall, within seven days after the change, inform the Authority of the change in ownership.

(8) An owner of a designated critical information infrastructure who contravenes subsection (1) and (3) is liable to pay to the Authority the administrative penalty specified in the Second Schedule.".

Section 37 of Act 1038 amended

12. The principal enactment is amended by substitution for section 37, of

"**Withdrawal of designation of critical information infrastructure**

"37. (1) The Minister may, on the advice of the Authority, withdraw the designation of a critical information infrastructure at any time if the Minister considers that

the computer or computer network no longer satisfies the criteria of a critical information infrastructure.

(2) The Minister may publish the withdrawal of critical information infrastructure sector in the *Gazette*.

(3) The owner of a designated critical information infrastructure shall receive notification of the withdrawal of the designation by letter from the Minister.".

Section 40 of Act 1038 amended

13. The principal enactment is amended in section 40 by substitution for subsection (2), of

"(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine of not less than four thousand penalty units and not more than twenty-five thousand penalty units, or both.".

Section 47 of Act 1038 Amended

14. The principal enactment is amended in section 47 by:

(a) the addition after subsection (6), of

"(7) A Sectoral Computer Emergency Response Team shall within twenty-four hours after receiving a report of a cybersecurity incident from the owner of a designated critical information infrastructure, a service provider, a licensee or any relevant person report the cybersecurity incident to the National Computer Emergency Response Team.".

(b) the addition after subsection (7), of

"(8) A Sectoral Computer Emergency Response Team who contravenes subsection (7) is liable to pay to the Authority the administrative penalty specified in the Second Schedule.".

Section 49 of Act 1038 Amended

15. The principal enactment is amended in section 49 by

(a) the substitution for subsection (1), of

"(1) A person shall not provide a cybersecurity service for a reward unless that person obtains a licence issued by the Authority in accordance with the Act.".

(b) the substitution for subsection (2), of

"(2) A person shall not provide a cybersecurity service on a not-for-profit basis unless that person obtains an accreditation issued by the Authority in accordance with the Act.".

(c) addition after subsection (2), of

"(3) A person who contravenes subsection (1) and (2) is liable to pay to the Authority the administrative penalty the equivalent to the cost of damage caused and value of the financial gain made, or an administrative penalty of not less than fifty thousand penalty units and not more than one hundred thousand penalty units.".

Section 57 of Act 1038 Amended

16. The principal enactment is amended by the substitution for section 57, of

(1) The Authority shall establish a mechanism for the accreditation of cybersecurity professionals and practitioners.

(2) An individual shall not practise as a cybersecurity professional or cybersecurity practitioner unless that individual has been accredited by the Authority;

(3) A person shall not knowingly engage the services of a cybersecurity professional or cybersecurity practitioner who has not been accredited by the Authority;

(4) A person who contravenes subsection (2) or (3) is liable to pay to the Authority an administrative penalty of not less than two hundred and fifty penalty units and not more than twenty thousand penalty units.

Section 57A inserted

17. The principal enactment is amended by the insertion after section 57, of

"**Cyber hygiene certification scheme**

57B. (1) The Authority shall establish a scheme for the certification of cybersecurity professionals and practitioners, and cybersecurity service providers who will be entrusted to perform cyber hygiene certification service as an alternative to other international best practice security frameworks.

(2) The Cyber Security Authority shall conduct periodic audits to ensure compliance with the cyber hygiene certification scheme and associated prescribed fees.

(3) Any complaints regarding non-compliance shall be investigated, and appropriate enforcement actions shall be taken.".

Section 57B inserted

18. The principal enactment is amended by the insertion after section 58A, of

"**Application for certification to provide the Cyber hygiene certification services**

57B. (1) A licensed cybersecurity service provider or accredited CP who seeks to provide the Authority's cyber hygiene certification 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 may determine.".

Section 57C inserted

19. The principal enactment is amended by the insertion after section 58B, of

"**Standardised, Review and Administration of Fees for Cyber Hygiene Certification Service**

57C. (1) A certified cybersecurity professional or practitioner or cybersecurity service provider shall charge a fee for cyber hygiene certification services as determined by the Cyber Security Authority.

(2) A certified cybersecurity professional or practitioner or cybersecurity service provider shall not charge fees exceeding the approved flat rate for cyber hygiene certification services.

(3) A certified cybersecurity professional or practitioner or cybersecurity service provider who fails to comply with subsection (2) shall be liable to pay to the Authority an administrative penalty specified in the Second Schedule (not less than two hundred and fifty penalty units and not more than five thousand penalty units)

(4) 30% of the revenue generated by a certified cybersecurity professional or practitioner or cybersecurity service provider under the scheme shall be paid into the cybersecurity fund.

(5) The Cyber Security Authority shall, by notice published in the Gazette, determine the applicable flat rate for cyber hygiene certification services.

(6) The flat rate shall be reviewed periodically based on, industry trends, and the affordability needs of stakeholders.".

Section 58A inserted

20. The principal enactment is amended by the insertion after section 58, of

"**Certification of the security of innovative and emerging technologies.**

58A. The Authority shall establish a mechanism for the certification of the security of innovative and emerging technologies.".

Section 58B inserted

21. The principal enactment is amended by the insertion after section 58A, of

"Accreditation of non-profit cybersecurity institutions

58B. The Authority shall establish a mechanism for the accreditation of non-profit cybersecurity institutions.".

Section 59 of Act 1038 Amended

22. The principal enactment is amended in section 59 by the addition after paragraph (e) of subsection (1), of

"(g) certification of the security of innovative and emerging technologies including Artificial Intelligence, cloud technology, quantum computing, big data, and blockchain-based technology.".

Section 59A inserted

23. The principal enactment is amended by the insertion after section 59, of

"**Enforcement powers**

59A. (1) A person who:

(a) knowingly fails to comply with or acts in contravention of this Act, regulations or directives issued under this Act;
(b) knowingly fails to comply with prescribed cybersecurity standards and requirements;
(c) provides cybersecurity services without a licence or acts as a cybersecurity professional or practitioner without accreditation;
(d) willfully obstructs, hinders, molests or assaults personnel of the Authority duly engaged in the exercise of power conferred on the Authority under this Act.

commits an offence and is liable on summary conviction to a term of imprisonment of not more than five years or to a fine of not more than twenty thousand penalty units, or to both.

(1) Where an offence is committed by a corporate entity, that entity is liable to a fine of not more than twenty thousand penalty units and each director of that entity shall be deemed to have committed the offence.

(2) Despite subsection (1), the Authority may, where a person has breached this Act, Regulations or directives or where a licensee, an accreditation holder has breached a condition contained in its licence or accreditation:

(a) warn the person, licensee, or accreditation holder,
(b) issue a cease-and-desist order,
(c) apply to the High Court for
  (i) an injunction to restrain the person, licensee, or accreditation holder from continuing the breach, or
  (ii) other appropriate order to enforce compliance with this Act,

(d) propose amendments to the licence or accreditation in accordance with this Act or Regulations
(e) suspend or terminate the licence or accreditation in accordance with this Act, or
(f) impose administrative penalties in accordance with the second schedule of the Act
(g) or take any other action that it considers appropriate and that is not contrary to this Act.

(4) Nothing shall prevent the Authority from pursuing only criminal enforcement actions under subsection (1) or only administration enforcement actions under subsection (2), or a combination of both.".

Section 59B inserted

24. The principal enactment is amended by the insertion after section 59A, of

"**Power to conduct investigations and to prosecute cybercrime**"

59B. (1) The Authority shall upon the occurrence of a cybersecurity incident or a cybercrime conduct criminal investigations and prosecute same."

(2) The Authority shall have the jurisdiction to prosecute all offences under the Electronic Transactions Act, 2008 (Act 772).

(3) Where a person is convicted of a cybercrime under this Act, the Authority may apply to the Court for an order to confiscate moneys, proceeds, benefits, properties and assets purchased by a person with proceeds derived from or in the commission of the cybercrime.

(4) Despite subsection (5), nothing shall prevent the Authority from instituting a civil action independently or at the same time as the prosecution to recover moneys, proceeds, benefits, properties and assets purchased by a person with proceeds derived from or in the commission of the cybercrime.

(5) In relation to subsection (6) if criminal prosecution fails, civil asset recovery should still proceed, and confiscation orders should have the effect of a civil judgment appealable from the High Court to the Court of Appeal.".

(6) Where the Authority considers that freezing of property is necessary to facilitate an investigation or prosecution, the Authority shall in writing direct the freezing of:

(a) the property of a person or entity being investigated; or
(b) specified property held by a person or entity other than the person or entity being investigated or prosecuted.

(7) The Authority shall within 14 days after the freezing of the property apply to the Court for a confirmation of the freezing.

Section 59C inserted

25. The principal enactment is amended by the insertion after section 59B, of

"Power to request for information

59C. (1) The Authority may, for the purposes of carrying out an investigation in respect of a contravention of the Act, Regulations or any other relevant enactment by the owner of a critical information infrastructure, a licensee, a service provider or any other person, by notice in writing, require a person to:

(a) attend at a time and place specified in the notice; and
(b) furnish the Authority with information related to a matter relevant to the investigation.

(2) A notice under subsection (1) shall indicate the subject matter and purpose of the request.".

(3) Where a person required to furnish the Authority with an information is under an obligation not to disclose, or asserts a right not to disclose, the Authority shall apply to the High Court for an order for the production of the information.

(4) Where an information is furnished to the Authority, the Authority shall make copies or extract from the Information and request the person

producing the information to provide an explanation on the content of the information where necessary.

(5) A person who appears before the Authority may be represented by a Counsel of the choice of that person at any stage of the process.

(6) Except as provided in subsection (2) where a person contravenes subsection (1) (a) and (b), that person commits an offence and is liable on summary conviction to a fine of not less than two hundred and fifty penalty units and not more than ten thousand penalty units or to a term of imprisonment of not less than one year and not more than two years or to both.".

Section 59D inserted

26. The principal enactment is amended by the insertion after section 59C, of

"**Application for Production Order to Collect Computer Data**

59D. (1) An investigative officer may apply *ex-parte* to the High Court for a production order to collect computer data.

(2) A production order under section (1) shall require a person in possession or control of a computer or computer system to submit specified computer data which is stored in the computer or computer system to the investigative officer.

(3) An investigative officer who makes an application under section (1) shall demonstrate to the satisfaction of the Court that there are reasonable grounds to believe that the computer data is reasonably required for the purposes of a specific criminal investigation.

(4) Where an investigative officer makes an application under section (1), that investigative officer shall:

(a) explain why the investigative officer believes the computer data sought, will be available to the person in control of the computer or computer system;
(b) identify and explain with specificity the type of computer data suspected to be found on the computer or computer system;
(c) identify and explain with specificity the computer data that may be found on a computer or computer system that is the subject of an investigation or prosecution;
(d) identify and explain with specificity the offences in respect of which the production order is sought; and
(e) indicate what measures shall be taken to ensure that the computer data will be procured

(i) whilst maintaining the privacy of other users, customers and third parties, and
(ii) without the disclosure of the computer data of any party not part of the investigation.".

Section 59E inserted

27. The principal enactment is amended by the insertion after section 59D, of

"Grant of production order

59E. (1) The High Court may grant an application for a production order under subsection (1) of section 59D, if the Court is satisfied that

(a) the investigative officer has complied with subsection (3) and (4) of section 59D;
(b) the information requested is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;
(c) measures shall be taken to ensure that the computer data is produced whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; and
(d) the investigation may be frustrated or seriously prejudiced unless the production of the information is permitted.

(2) The Court shall require the service provider to keep confidential the production order and the execution of the production order under this section.

(3) A production order granted under this Act shall be served on a domestic service provider, foreign service provider or both, or any other relevant person.".

Section 59F inserted

28. The principal enactment is amended by the insertion after section 59E, of

"**Application for Warrant to Access, Search and Seize Computer Data, Computer or Computer System**

59F. (1) An investigative officer may apply ex-parte to the High Court for a warrant to:

(a) access data on a computer or computer system;
(b) search and seize a computer or a computer system; or

(c) make or retain a copy of computer data on a computer or computer system;
(d) maintain the integrity of computer data on a computer or computer system;
(e) remove or render inaccessible computer data on a computer or computer system

that is suspected to contain information relevant to an investigation.

(2) A warrant under subsection (1) shall require a person who has knowledge about the functioning of the computer or computer system to provide the necessary information to enable an investigative officer undertake the actions required under paragraphs (a) to (e) of subsection (1).

(3) An investigative officer who makes an application under subsection (1) shall demonstrate to the satisfaction of the court that there are reasonable grounds to believe that the warrant is reasonably required for the purposes of a specific criminal investigation.

(4) A warrant under subsection (1) shall permit a law enforcement officer to expeditiously extend the search for data from a computer or computer system to another computer or computer system or part of it in Ghana where the law enforcement officer has reasonable grounds to believe that the data sought is accessible from or available to that other computer or computer system or part of it in Ghana.".

Section 59G inserted

29. The principal enactment is amended by the insertion after section 59F, of

"**Grant of warrant**

59G. (1) The High Court may grant an application for a warrant under subsection 1 of section 59F if the Court is satisfied that

(a) the investigative officer has complied with subsection (3) of section 59F.
(b) the information requested is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;
(c) measures shall be taken to ensure that the computer data is produced whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; and

(d) the investigation may be frustrated or seriously prejudiced unless the production of the information is permitted.

(2) The Court shall require the service provider to keep confidential the warrant and the execution of the warrant under this section.

(3) A warrant granted under this section shall be served on a domestic service provider, foreign service provider or both, or any other relevant person.".

Section 59H inserted

30. The principal enactment is amended by the insertion after section 59G, of

"**Application for preservation order to preserve computer data**

(1) A provider of wire or electronic communication services or a remote computing service on the written request of a law enforcement agency, shall take the necessary steps to preserve records and other evidence in its possession pending the issue of a Court order and shall take steps to ensure that the request by the law enforcement agency is not disclosed to third parties during the period.

(2) Where an order from the Court is not obtained and served for fourteen days after the receipt of the written request, the wire or electronic communication services, or remote computing service provider is not under any obligation to preserve the evidence.

(3) An investigative officer authorised by a designated officer may apply *ex-parte* to the Court for an order to require a service provider or any person in control of a computer or computer system to preserve specified computer data, including traffic data that has been stored by a computer system.

(4) An investigative officer who makes an application under subsection (1) shall demonstrate to the satisfaction of the Court that the computer data is particularly vulnerable to loss or modification.".

Section 59I

31. The principal enactment is amended by the insertion after section 59H, of

"**Grant of preservation order**

59I. (1) The High Court may grant an application for a preservation order under subsection (1) of section 59F if the Court is satisfied that:

(a) the designated officer has complied with subsection (2) of section 59H;

(b) the extent of the preservation order is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;

(c) measures shall be taken to ensure that the computer data is preserved whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; and

(d) the investigation may be frustrated or seriously prejudiced unless the preservation order is permitted.

(2) The preservation order issued under subsection (1)

(a) is valid for a period of ninety days, and

(b) may be renewed for a further period of ninety days upon application to the Court.

(3) The Court shall require the service provider to keep confidential a preservation order issued under this regulation.".

Section 59J

32. The principal enactment is amended by the insertion after section 59I, of

"Power of entry, inspection and audit

59J. (1) The Authority may designate a person as an inspector to inspect premises.

(2) A person designated as an inspector by the Authority may

(a) obtain a warrant to:

(i) enter and inspect premises; and

(ii) conduct an audit of a computer system

(b) at any reasonable time, enter inspect premises and conduct and audit of a computer system without a warrant where the inspector

(i) reasonably believes that an inspection of the premises is necessary to ensure compliance by the owner of a critical information infrastructure, a licensee or a service provider or any other relevant person with the Act or Regulations; and

(ii) has given the occupier of the premises seven days' notice in writing of the intention to enter, inspect the premises and conduct an audit of a computer system.

(3) An inspector shall, before exercising a power of entry and inspection,

(a) produce evidence of the identity of the inspector; and
(b) indicate the purpose of entry and inspection.

(4) An inspector may

(a) enter a premises;
(b) inspect the premises;
(c) inspect a document or equipment found on the premises;
(d) require a person on the premises to provide any information, or produce any document in the possession or control of that person that the inspector considers relevant to ensure compliance with the Act and Regulation and
(e) require any person on the premises to provide information in respect of a document or the location of a document.

(4) For the purpose of this regulation, "premises" does not include domestic premises.".

Section 59K inserted

33. The principal enactment is amended by the insertion after section 59J, of

"Witness and Informant Protection

59K. (1) Except with the written, informed, explicit and freely given consent of a witness or informant, no witness or informant who discloses information relating to cybercrime under this Act or administrative infractions under this Act, shall be obliged to disclose his name or address or other personal information, or state any matter which might lead to their discovery.

(2) Unless otherwise provided, the information and the identity of the witness or informant shall be held to be secret between the Authority and the witness or informer; and all matters relating to such information should be privileged and shall not be disclosed in any proceedings before any court, tribunal, commission, or authority.

(3) The Authority take all necessary and reasonable steps to protect the safety and welfare of a witness or informant, and such the protection shall extend to persons by virtue of being related to a witness or informant, or on account of a testimony given by a witness or informer, or for any other reason upon which the Authority may consider sufficient.".

Section 67 of Act 1038 amended

34. The principal enactment is amended by:

(a) the substitution for the heading before section 67 "Other Online Sexual Offences, of

"Other cybercrime".

(b) the substitution for subsection (2) of section 67, of

"(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a term of imprisonment of not less than three years and not more than ten years or a fine of not less than two hundred and fifty penalty units and not more than twenty-five thousand penalty units or to both.".

Section 67A inserted

35. The principal enactment is amended by the insertion after section 67, of

"**Cyberbullying and online harassment**

67A. (1) A person shall not use the internet or any form of electronic medium or technology to bully a child or an adult.

(2) A person shall not use a computer or any other electronic medium to

(a) send a threatening message or a lewd message to a child;

(b) make sexual advances towards a child; or

(c) persistently make contact with

(i) a child, whether or not the contact is acceptable; or

(ii) another person where the contact is unacceptable.

(3) A person shall not create a false identity online or a fake social media profile for the purposes of following

(a) a child, whether or not the contact is acceptable; or

(b) an adult, where the contact is unacceptable.

(4) A person shall not use any online computer service or any other electronic device to:

(a) track the location of a child;

(b) monitor the real-world activities of a child;

(c) track the location of another person without the consent of that person;

(d) monitor the real-world activities of another person without the consent of that person; or

(e) obsessively track the location of

(i) a child; or

(ii) another person without the consent of that person.

(5) Despite subsection (4), a parent or legal guardian may for the purposes of ensuring the safety of a child, track the location of the child, or monitor the real-world activities of the child.

(6) A person shall not use an electronic device or medium to send

(a) an unwanted,

(b) an unsolicited,

(c) a frightening,

(d) an obscene,

(e) a harassing, or

(f) a threatening electronic mail, text message or instant message to a child or an adult.

(7) A service provider of a user-to-user service including

(a) a chatroom,

(b) a social network site,

(c) an online gaming platform, or

(d) a virtual, augmented and mixed reality shall protect a child from all forms of online violence and cyberbullying from users of the user-to-user service.

(8) A person shall not use an electronic device or an electronic medium to deliberately spread false or misleading information with the intent to deceive or manipulate a person or a fact.

(9) A person who contravenes subsections (1), (2), (3), (4) or (6) commits an offence and is liable on summary conviction to a fine of not less than two thousand, five hundred penalty units and not more than five thousand penalty units or to a term of imprisonment of not less than one year and not more than three years or to both.

(10) A person who contravenes sub regulation (7) or (8) commits an offence and is liable on summary conviction to a fine of not less than five thousand penalty units and not more than twenty-five thousand penalty units or to a term of imprisonment of not less than three years and not more than five years or to both.

(11) For the purpose of this Act, "cyberbullying" includes any digital communication and any other activity which strips the recipient of the dignity of the recipient, or causes fear or physical or emotional harm such as

(a) repeatedly sending offensive, rude and insulting messages to a person;

(b) distributing derogatory information about a child or any other person;

(c) posting or sending offensive photos of a child or any other person, whether or not the photos

(i) have been digitally altered, or

(ii) were taken with the consent of the victim, with the intention to humiliate or embarrass the victim;

(d) breaking into an electronic mail, social networking or any electronic account and using the virtual identity of a victim to send, upload or distribute embarrassing materials to or about others;

(e) sharing sensitive personal information or any embarrassing information, or tricking a child or any person to reveal personal or embarrassing information about that child or any other person and sharing the information obtained with others;

(f) repeatedly sending threatening or intimidating messages with threats of harm, or engaging in online activities that cause fear in a child or puts any other person in fear;

(g) sending messages to another person telling the person to commit suicide;

(h) sending grossly offensive, indecent or obscene communication with the intention of causing emotional distress to a child or any other person; or

(i) sending electronic messages that denigrate a child or any other person on the basis of

(i) colour;

(ii) race;
(iii) ethnic or national origins;
(iv) religion;
(v) gender; or
(vi) disability.".

Section 67B inserted

36. The principal enactment is amended by the insertion after section 67A, of

"**Cyberstalking of a person**

"**67B.** (1) In furtherance of section 65 of the Act, a person shall not use the internet, chatroom, a social network site, an online gaming platform, or a virtual, augmented and mixed reality to

(a) harass or stalk a person;

(b) assume a false identity to anonymously harass or stalk a person;

(c) create false information about a person; or

(d) post or disseminate false information about a person.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a term of imprisonment of not less than one year and not more than ten years or a fine of less than one hundred penalty units and not more than ten thousand penalty units or to both.".

Section 68 of Act 1038 amended

37. The principal enactment is amended in section 68 by substitution for subsection (2), of

"(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a term of imprisonment of not less than three years and not more than ten years or a fine of less than two hundred and fifty penalty units and not more than twenty-five thousand penalty units or to both.".

Section 83 of Act 1038 amended

38. The principal enactment is amended in section 83 by:

(a) the substitution for paragraph (e) of subsection (4), of

"(e) requesting for information regarding domain name registration;".

(b) the addition after paragraph (e) of subsection (4), of

"(f) expedited disclosure of specified stored computer data in a service provider's possession or control in an emergency situation without a request for mutual assistance;".

(c) the addition after paragraph (f) of subsection (4), of

"(g) any other matter related to paragraphs (a) to (f).".

(d) the addition after paragraph (g) of subsection (4), of

"(5) For the purpose of this section an emergency means, a situation in which there is a significant and imminent risk to the life or safety of any natural person.".

Section 90 of Act 1038 amended

39. The principal enactment is amended in section 90 by the addition after subsection (2), of

"(3) Despite section 90(1) and section 90A, the Circuit Court shall have the jurisdiction to try an offence under sections 62 to 68A of this Act.".

Section 91 of Act 1038 amended

40. The principal enactment is amended in section 91 by the addition after paragraph (h), of

"(i) the designation of Sectoral Computer Emergency Response Team;
(j) the accreditation of Sectoral Computer Emergency Response Team;
(k) the accreditation of cybersecurity establishments;
(l) the accreditation of non-profit cybersecurity institution;
(m) the protection of children;
(n) safeguarding the development and deployment of innovative and emerging technologies or solutions;
(o) licensing of cyber security service providers;
(p) accreditation of cybersecurity professionals and practitioners;
(p) any other matter required for ensuring the cybersecurity of the country.".

Section 92 of Act 1038 amended

41. The principal enactment is amended in section 92 by:

(a) the substitution for subsection (1), of

"(1) the Authority may issue directives to an owner of a critical information infrastructure, a cybersecurity service provider or service provider, innovators, developers for the purpose of ensuring the cybersecurity of the country.

(b) the substitution for subsection (2), of

"(2) An owner of a critical information infrastructure, cybersecurity service provider or service provider, innovator, developer or any relevant person who fails to comply with the directives issued under this section is liable to pay to the Authority the administrative penalty specified in the Second Schedule.".

(c) the insertion after subsection (2), of

"(3) The Authority may issue directives to innovators, developers, service providers and cybersecurity service providers for the purpose of securing the adoption and deployment of innovative and emerging technologies or solutions.".

Section 94 of Act 1038 amended

42. The principal enactment is amended by the substitution for section 94, of

"(1) A person who, without lawful authority accesses or retrieves subscriber information or intercepts traffic data or content data, commits an offence and is liable on summary conviction to a fine of not less than two thousand five hundred penalty units and not more than fifteen thousand penalty units or to a term of imprisonment of not less than two years and not more than five years or, to both.

(2) An attempt to gain access to a critical information infrastructure or its dependencies, successful or not, constitutes an unlawful access to the critical information infrastructure.

(3) Any person who attempts to secure access to a critical information infrastructure or its dependencies, successful or not commits an offence and is liable on summary conviction to a term of imprisonment of not less than two years and not more than five years or a fine of not less than four thousand penalty units and not more than twenty-five thousand penalty units or to both.

(4) The tampering and or destruction of critical information infrastructure or its components which affects the confidentiality, integrity or availability of the critical information infrastructure constitutes unlawful access to critical information infrastructure, and a person shall be subject to the same criminal penalties specified in subsection (1).".

Section 94A inserted

43. The principal enactment is amended by the insertion after section 94, of

"**Computer related Forgery**

95A. (1) A person shall not intentionally and without right, input, alter, delete or suppress computer data resulting in inauthentic data with the intent that they be considered or acted upon for legal purposes as if they were authentic, regardless of whether or not the data are directly readable and intelligible."

(2) A person who contravenes subsection (1) commits an offence and shall be deemed to have committed the offence of forgery under Chapter Two of the

Criminal Offences Act, 1960 (Act 29), and shall liable on summary conviction to the same punishment for that particular kind of forgery under the law.".

Section 94B inserted

44. The principal enactment is amended by the insertion after section 94A, of

"Computer related Fraud

95B. (1) A person shall not intentionally and without right, cause the loss of property to another person by means of:

(a) Any input, alteration, deletion or suppression of computer data;

(b) Any interference with the functioning of a computer system;

(c) Any deception as to factual circumstances made through a computer system that causes a person to do or omit to do anything which that person would not otherwise do or omit to do; with the fraudulent or dishonest intent of procuring for oneself or for another person, without right, a gain in money or other property.

(2) A person who contravenes subsection (1) commits an offence and shall be deemed to have committed the offence of defrauding by false pretence under section 131 of the Criminal Offences Act, 1960 (Act 29), and shall liable on summary conviction to the same punishment for defrauding by false pretence under that law.".

Section 97 of Act 1038 amended

45. The principal enactment is amended in section 97 by:

(a) the insertion before "Authority", of

"Artificial Intelligence is technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision-making, creativity and autonomy;";

"block-chain based technology" means an advanced decentralised digital record or digital ledger of transactions, that enables recording of transactions, tracking of assets, and sharing of records across computer networks in a transparent and immutable way;".

"big data" means a collection of extremely large organized, semi-structured, and unstructured information that grows exponentially over time;";

(b) the insertion after "child", of

"cloud technology" means technology that delivers computing services and offers on-demand access to computing resources such as physical or virtual services, data storage, servers, databases, networking, intelligence, analytics, and software over the internet;";

(c) the insertion after "cloud technology", of

"confiscation", which includes forfeiture where applicable, shall mean the permanent deprivation of property by order of a court or other competent authority;";

(d) the insertion after "digital ecosystem" of

"digital services" 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;

(e) the insertion after "Director-General", of

"Emergency" shall mean a situation in which there is a significant and imminent risk to the life or safety of any natural person;";

(f) the insertion after "e-services", of

"Freezing" or "seizure" mean temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority;";

(g) the insertion after "interception of warrant", of

"Internet of Things (IoT) means a network of interrelated physical devices, vehicles, appliances and other physical objects that connect and exchange data with other devices and the cloud across wireless networks, and are typically embedded with sensors, processing ability and software and can include mechanical and digital machines and consumer objects;";

(h) the substitution for "computer system", of

"computer system" means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes

(a) an information processing system;
(b) an operational technology system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system; and

(c) dependency systems that support the functionality of a computer or computer network;";

(i) the substitution for "law enforcement agency", of

"law enforcement agency" means

(a) The Police
(b) The Customs Division of the Ghana Revenue Authority and
(c) Cyber Security Authority
(d) Any other agency authorised by law to exercise the powers of the Police

(j) the insertion after "prohibited intimate image and visual recording", of

"property" means assets of every kind, in the country or elsewhere whether corporeal or incorporeal, movable or immovable, tangible or intangible, including virtual assets, and legal documents or instruments evidencing title to, or interest in, such property assets;";

(k) the insertion after "property", of

"property of or in the possession or control of a person" includes a gift made by that person;

(l) the insertion after "publish", of

"quantum computing" means technology that solves complex problems based on principles of quantum mechanics;".

Section 98 of Act 1058 amended

46. The principal enactment is amended by substitution for section 98, of

"**Repeals and savings**

(1) Sections 118 and 136 of the Electronic Transaction Act, 2008 (Act 772) are repealed.

(2) Sections 35 to 40 this Act repeals sections 55 to 62 of the Electronic Transaction Act, 2008 (Act 772).

(3) Despite the repeal of sections, any Regulations, bye-laws, directives, notices, orders, directions, appointments or other acts lawfully made or done under the repealed enactment and in force immediately before the

coming into force of this Act shall be deemed to have been made or done under this Act and shall continue to have effect until instruments issued or made until revoked, cancelled, withdrawn or terminated.".

Section 99 of Act 1038 amended

47. The Extradition Act, 1960 (Act 22) is amended by:

(a) the addition after subsection (3) of section, of

"(4) Despite subsection (1), for the purposes of extradition, Cybercrime and Cyber Offences under the First Schedule to this Act, in the absence of a separate arrangement, bilateral or multilateral agreement between Ghana and another signatory of the Budapest Convention on Cybercrime or any other convention, extradition of fugitive criminals may still take place between Ghana and another signatory of the Budapest Convention on Cybercrime or any other convention and shall be governed by the provisions of the said convention.".

First schedule to Act 1038 amended

48. The principal enactment is amended by substitution for the preamble, of

"A service provided for reward or a not-for profit basis intended primarily for or aimed at ensuring or safeguarding the cybersecurity of a computer or computer system belonging to a person and includes.".

Second schedule to Act 1038 amended

49. The principal enactment is amended by substitution for administrative penalties for sections 36(4), 39(2)(a), 39(2)(b), 39(2)(c) and 92(2) and addition of administrative penalties for sections 36(1) and 39(3)(c).

No.	Sections of Act creating contravention	Contravention	Administrative Penalty
1.	36(1)	The Owner of the designated critical information infrastructure shall register their critical information infrastructure with the Authority, and shall pay the prescribed annual registration and designation fee as determined by the Authority or stipulated in a legislative instrument.	Not less than five thousand penalty units, not more than fifty thousand penalty units.
2.	36(4)	Owner of a registered critical information infrastructure failing to inform the Authority within seven days of the change in legal ownership of the registered critical	Not less than five thousand penalty units, not more than

		information infrastructure.	fifty thousand penalty units.
3.	39(2)(a)	Owner of a critical information infrastructure failing to report a cybersecurity incident.	Not less than ten thousand penalty units, not more than fifty thousand penalty units.
4.	39(2)(b)	Owner of a critical information infrastructure failing to cause an audit to be performed on the critical information infrastructure.	Not less than five thousand penalty units, not more than twenty thousand penalty units.
5.	39(3)(c)	Owner of a critical information infrastructure failing to submit a copy of the audit report to the Authority.	Not less than five thousand penalty units, not more than twenty thousand penalty units.
6.	92(2)	Owner of a critical information infrastructure, a cybersecurity service provider or a provider of a digital service failing to comply with a directive issued by the Authority.	Not less than ten thousand penalty units, not more than fifty thousand penalty units

Third schedule to Act 1038 amended

50. The principal enactment is amended by addition after the "Oath of Secrecy", of

The Official Oath
(section 5)

I,

……..……

do (in the name of the Almighty God swear) (solemnly affirm) that I will at all times well and truly serve the Republic of Ghana in the office of …….and that I will uphold, preserve, protect and defend the constitution of the Republic of Ghana as by law established (so help me God).