GHANA

LAW

The primary legislation governing privacy/data protection in Ghana is the Data Protection Act, 2012 (Act 843).

Other laws, examples of which are set out below, contain some privacy/data protection provisions:

1992 Constitution

Article 18(2) provides citizens with a fundamental right to privacy. The Article provides that “no person shall be subjected to interference with the privacy of his home, property, correspondence or communication except in accordance with law and as may be necessary in a free and democratic society for public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.”

Electronic Communications Act, 2008 (Act 775)

A network operator or a service provider who is a holder of a Class Licence shall not use or permit another person to use or disclose confidential, personal or proprietary information of a user, another network operator or service provider without lawful authority unless the use or disclosure is necessary for the operation of the network or service, the billing and collection of charges, the protection of the rights or property of the operator or provider, or the protection of the users or other network operators or service providers from the fraudulent use of the network or service.

A person who intentionally uses or discloses personal information in contravention of the Act commits an offence and is liable on summary conviction to a fine of not more than one thousand five hundred penalty units or to a term of imprisonment of not more than four years or both.

Act 775 defines a Class Licence as “a licence, other than an individual licence, granted on the same terms to each applicant in respect to a class of electronic communications networks or services or radio-communication services.”

Electronic Communications Regulations, 2011 (L.I. 1991)

The principle of privacy and secrecy in electronic communications applies to the National Communications Authority, operators of electronic communications networks and providers of electronic communications services.

The operator is required to comply with international best practices in the industry to promote privacy, secrecy and security of communications carried or transmitted by the operator or through the communications system of the operator, and the personal and accounts data related to subscribers.

Credit Reporting Act, 2007 (Act 726)

The Bank of Ghana has the overall supervisory and regulatory authority under the Act to: (a) register, license and regulate credit...
bureaus, data providers and credit information recipients and their agents; and (b) control and supervise activities of the credit bureaus, data providers, credit information recipients and their agents.

The Act requires the recipient of a credit report to keep such report confidential while ensuring that the information contained in it is used solely for its specified purpose. A credit bureau, data provider or credit information recipient is required to observe the principles of: (a) equality of credit information subjects; (b) confidentiality of information; (c) non-interference in the private life of citizens; (d) respect for the rights, liberties and lawful interests of persons and legal entities; (e) accuracy and transparency of information; and (f) privacy and secrecy of communication.

**Public Health Act, 2012 (Act 851)**

Article 45 of the International Health Regulations (2005) of World Health Organisation Regulations which is annexed to Act 851 as the Seventh Schedule provides that “health information collected or received by a State Party pursuant to these Regulations from another State Party or from WHO which refers to an identified or identifiable person shall be kept confidential and processed anonymously as required by national law.”

**Children’s Act, 1998 (Act 560)**

The purpose of this Act is to reform and consolidate the law relating to children, to provide for the rights of the child, maintenance and adoption, regulate child labour and apprenticeship, and provide for ancillary matters concerning children generally.

Act 560 provides that “a child’s right to privacy must be respected throughout the proceedings at a Family Tribunal”. In furtherance of this, the Act restricts participants to the sittings of the Family Tribunal to persons with an interest in the matter including parents of the child and officers of the Tribunal.

Act 560 further provides that it is an offence for any person to “publish any information that may lead to the identification of a child in any matter before a Family Tribunal except with the permission of the Family Tribunal.”

**DEFINITIONS**

- **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 or in common with other persons or as a statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed.

- **Data processor** in relation to personal data means any person other than an employee of the data controller who processes the data on behalf of the data controller.

- **Data subject** means an individual who is the subject of personal data.

- **Data supervisor** means a professional appointed by a data controller in accordance with section 58 to monitor the compliance by the data controller in accordance with the provisions of the Act.

- **Processing** means an operation or activity or set of operations by automatic or other means that concerns data or personal data and the:
  - collection, organisation, adaptation or alteration of the information or data;
  - retrieval, consultation or use of the information or data;
  - disclosure of the information or data by transmission, dissemination or other means available, or
  - alignment, combination, blocking, erasure or destruction of the information or data.

**Definition sensitive personal data**

The Data Protection Act does not make provision for 'sensitive personal data'. However 'special personal data', is defined as personal data which relates to:

- the race, colour, ethnic or tribal origin of the data subject;
the political opinion of the data subject;
the religious beliefs or other beliefs of a similar nature, of the data subject;
the physical, medical, mental health or mental condition or DNA of the data subject;
the sexual orientation of the data subject;
the commission or alleged commission of an offence by the individual; or
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.

NATIONAL DATA PROTECTION AUTHORITY

Data Protection Commission (‘Commission’)

Pawpaw Street
East Legon
Accra
Ghana
GPS: GA-414-1469

P.O. Box CT7195
Accra
Ghana

Tel: +233-(0)30 2222 929
Email: info@dataprotection.org.gh

REGISTRATION

A data controller who intends to process personal data is required to register with the Data Protection Commission. A data controller who is not incorporated in Ghana must register as an external company.

DATA PROTECTION OFFICERS

There is an obligation under the Act for data controllers to appoint data protection officers.

COLLECTION & PROCESSING

A person shall collect data directly from the data subject unless:

- the data is contained in a public record
- the data subject has deliberately made the data public
- the data subject has consented to the collection of the information from another source
- the collection of the data from another source is unlikely to prejudice a legitimate interest of the data subject
- the collection of the data from another source is necessary for a number of expressly designated purposes (for example the detection or punishment of an offence or breach of law)
- compliance would prejudice a lawful purpose for the collection
- compliance is not reasonably practicable.

A data controller must also ensure that the data subject is aware of:
the nature of the data being collected

the name and address of the person responsible for the collection

the purpose for which the data is required for collection

whether or not the supply of the data by the data subject is discretionary or mandatory

the consequences of failure to provide the data

the authorized requirement for the collection of the information or the requirement by law for its collection

the recipient of the data

the nature or category of the data

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

Where collection is carried out by a third party on behalf of the data controller, the third party must ensure that the data subject has the information listed above.

TRANSFER

There are no specific provisions in the Act on the transfer of personal data. However, the sale, purchase, knowing or reckless disclosure of personal data or information is prohibited.

A person who knowingly or recklessly discloses personal data is liable on summary conviction to a fine of not more than 250 penalty units or to a term of imprisonment of not more than 2 years or to both. A person who sells or offers for sale personal data is liable on summary conviction to a fine of not more than 2500 penalty units or to a term of imprisonment of not more than five years or to both a fine and a term of imprisonment.

A penalty unit is equivalent to GHS 12 (approximately USD 2.20).

SECURITY

- A person who processes data shall take into account the privacy of the individual by applying the data security safeguards.
- A data controller has an obligation to ensure that a data processor who processes personal data for the data controller, establishes and complies with the security measures provided for under the Act.

BREACH NOTIFICATION

Where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by an unauthorised person, the data controller or a third party who processes data under the authority of the data controller shall notify the Commission and the data subject of the unauthorised access or acquisition as soon as reasonably practicable after the discovery of the unauthorised access or acquisition of the data. The data controller shall take steps to ensure the restoration of the integrity of the information system.

The data controller shall delay the notification to the data subject where the security agencies or the Data Protection Commission inform the data controller that the notification will impede a criminal investigation.

ENFORCEMENT

Where the Commission is satisfied that a data controller has contravened or is contravening any of the data protection principles, the Commission shall serve the data controller with an enforcement notice to require the data controller to do any of the following:
• to take or refrain from taking the steps specified within the time stated in the notice;
• to refrain from processing any personal data or personal data of a description specified in the notice;
• 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.

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 one hundred and fifty penalty units or to a term of imprisonment of not more than one year or to both. A penalty unit is equivalent to GHS 12 (approximately USD 2.20).

Further, an individual who suffers damage or distress through the contravention of the data protection obligations by a data controller is entitled to compensation from the data controller for the damage or distress notice.

ELECTRONIC MARKETING

The Act prohibits a data controller from using, obtaining, procuring or providing information related to a data subject for the purpose of direct marketing without the prior written consent of the data subject. However, there are no specific provisions that relate to electronic marketing specifically.

ONLINE PRIVACY

There are no specific provisions in relation to on-line privacy. However, a data controller is generally required to take necessary steps to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate, reasonable, technical and organizational measures.

KEY CONTACTS

Reindorf Chambers
www.reindorfchambers.com

Kizzita Mensah
Partner
Reindorf Chambers
T +233 302 225 674
kizzita.mensah@reindorfchambers.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization’s level of data protection maturity.