FACTSHEET: GHANA

Last updated: 30 September 2019
Prepared by Justin Bryant

FAST FACTS

Population: 28,308,301
Capital: Accra
President: Nana Akufo-Addo
2019 Freedom House Score: 83/100
Data protection law? Enforced

LAW

In Ghana, the recognition of the right to privacy under Article 18(2) of the 1992 Constitution led to the passing of the Data Protection Act, 2012 (Act 843) to further guarantee the right to privacy. It came into force in October 2012, and applies both to data controllers based in Ghana and those who process data originating in Ghana.

Under the Act, data subjects has the right to:

- have their personal data corrected;
- access their personal data;
- prevent the processing of personal data that causes or is likely to cause unwarranted damage or distress to them;
- prevent the processing of personal data for purposes of direct marketing;
- not be subject to a decision by a data controller that would significantly affect them or have detrimental legal repercussions for them if the decision was solely based on automatic processing;
- exempt manual data; and
- be compensated for the data controller's failure to comply with the provisions of Act 843, upon proof of damages.

PERSONAL DATA

Personal data is data about an individual who can be identified either:

- from the data; or
- from the data and other information in the possession of, or likely to come into the possession of the data controller.

Special personal data is defined as personal data which relates to the following categories:

- a child who is under parental control in accordance with the law; or
- the **religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life or criminal behaviour of an individual.**

COLLECTION AND PROCESSING

The eight data protection principles enumerated in Act 843 mirror those in the OECD Guidelines and the EU Data Protection Directive (95/46/EC).

1. **Accountability**
    - Establishes that a data controller should be accountable for compliance with measures aimed at realising the data protection principles. Processors of personal data must ensure that data subjects' privacy rights are not infringed upon by using the data in a lawful and reasonable manner.
2. **Lawfulness of processing**
    - Necessitates that the purpose of personal data processing be necessary, relevant and not excessive.
3. **Specification of purpose**
    - Designed to guarantee that processing happens for specific purposes that are explicitly defined, lawful, and related to the functions or activities of the person collecting the data.
4. **Compatibility of further processing with purpose of collection**
    - Further processing of personal information must be compatible with the purpose for which it was initially obtained, but this requirement can be met if consent is given, if the data is in the public domain, or needed for the purposes of fighting crime, protection of tax revenue collection, the conduct of court proceedings, protection of national security, public health, or the life or health of the data subject or another person.
5. **Quality of information**
    - Data controllers must ensure that personal data is complete, accurate, up to date, and not misleading, having regard to the purpose for the collection or processing of the personal data.
6. **Openness**
    - Emphasises the need for data subjects to be made aware of the purpose for which their data is being collected, and gives a data subject the right to access and correct personal information.
7. **Data security safeguards**
    - Charges data controllers with a duty to prevent the loss of, damage to, or unauthorised destruction of personal data, as well as the unlawful access to or unauthorised processing of personal data. It demands that data controllers adopt appropriate, reasonable, technical, and organisational means to take necessary steps to ensure the security of personal data in their possession or control.
8. **Data subject participation**
    - The data controller must allow data subjects to exercise their rights under Act 843 regarding their personal data.

REGISTRATION AND ENFORCEMENT

The Data Protection Commission (Commission) is the regulatory body established under Act 843, tasked with implementing and monitoring compliance with the Act's provisions; making appropriate administrative arrangements for its duties, investigating complaints, serving enforcement notices, and maintaining the Data Protection Register. The body is overseen by a ten-member board appointed by the President.

As of **January 2015**, data controllers must register with the Commission and renew their registration every two years. All new data controllers are required to register within twenty days of the start of business. Data controllers who fail to register are liable on summary conviction to a fine of not more than two hundred and fifty penalty units, a term of imprisonment of not more than two years, or both.

Data controllers are expected to designate a data protection supervisor responsible for handling the data controller's compliance with Act 843. The Commission will provide criteria for the appointment of data protection supervisors, and individuals chosen for this role are expected to meet the criteria. Each government department is to be treated as a data controller and appoint a supervisor.

Individuals are entitled to compensation from data controllers for damage or distress caused by violations of Act 843.

CROSS-BORDER TRANSFER

While no provisions in Act 843 specifically pertain to transfer outside of national borders, selling or offering to sell the personal data of another person anywhere constitutes an offence punishable by a fine of not more than two thousand five hundred penalty units, a term of imprisonment of not more than five years, or both. An advertisement which indicates that personal data is or may be for sale is an offer to sell the data.

SECURITY AND BREACH PROTOCOL

In the event that the personal data of a data subject is believed to have been accessed or acquired by any unauthorised person, the data controller or authorised third party must notify the Commission and the data subject as soon as reasonably possible after the discovery of the data breach.

Read the legal notice and terms of use for this factsheet.