



# LEGISLATIVE DIGEST

An assessment of Data Protection  
legislative framework in Ghana

## Contributors



**Richard Nunekpeku**  
Managing Partner

richard@sustineriattorneys.com



**Gafaru Ali**  
Senior Associate

gafaru@sustineriattorneys.com



**Andrews Kweku  
Benin Aning**

Associate  
andrews@sustineriattorneys.com



**Cecilia Antwi  
Kyem**

Trainee Associate  
cecilia@sustineriattorneys.com



**Harold Kwebena  
Fearon**

Trainee Associate  
harold@sustineriattorneys.com

### Legislation

### Data Protection Act, 2012 (Act 843)

#### Purpose of the legislation

An Act to establish a Data Protection Commission, to protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use, or disclose personal information and for related matters.

#### Implementing institution

#### The Data Protection Commission

#### Affected industry<sup>1</sup>

1. Data Controller (individuals and entities) established in Ghana which processes data in Ghana.
2. Data Controller not established in Ghana but uses equipment or a data processor carrying on business in Ghana to process data
3. Processing of information which originates partly or wholly from Ghana

## KEY DEFINITIONS UNDER THE ACT<sup>2</sup>

**Business:** includes trade or profession

**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 (a) and (b)

**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

<sup>1</sup>Section 45(1), Data Protection Act, 2012 (Act 843)

<sup>2</sup>Section 96, Data Protection Act, 2012 (Act 843)

- 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 paragraphs (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 protection functions:** means functions that relate to the protection of personal data in the course of data processing

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

**Data supervisor:** means a professional appointed by a Data controller to monitor the compliance by the data controller in accordance with the Data Protection Act.

**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:** mean any failure to comply with or a violation of any of the data protection principles, enforcement, or other notices issued by the Data Protection Commission.

**Good practice:** means the practice of the processing of personal data in a way that the likelihood of causing substantial damage or distress is reduced

**Personal data:** means data about an individual who can be identified,

- a) From the data, or
- b) From the data, or other information in the possession of, or likely to come into the possession of the data controller

**Processing:** means an operation or activity or set of operations by automatic or other means that concerns data or personal data and the

- a) Collection, organization, adaptation, or alteration of the information or data,
- b) Retrieval, consultation, or use of the information or data
- c) Disclosure of the information or data by transmission, dissemination, or other means available or
- d) Alignment, combination, blocking, erasure, or destruction of the information or data



**Public 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, journalist, literary or artistic material

**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.

**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.

**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 religious beliefs or other beliefs of a similar nature, of the data subject
- d) The physical, medical, mental health or mental condition or DNA of the data subject
- e) The sexual orientation of the data subject
- f) The commission or alleged commission of an offence by the individual or
- g) 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
- d) Literary purposes

**Subject information provisions:** means the provisions which deal with the right of a data subject to access information from a data controller

**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 a particular individual 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

**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 persons authorized to process data for the data controller or processor.

## **THE APPLICATION OF DATA PROTECTION PRINCIPLES UNDER THE ACT<sup>3</sup>**

### **1. Privacy of the individual<sup>4</sup>**

A person who processes data shall take into account the privacy of the individual by applying the following principles:

- a) Accountability,
- b) Lawfulness of processing,
- c) Specification of purpose,
- d) Compatibility of further processing with purpose of collection,
- e) Quality of information,
- f) Openness,
- g) Data security safeguards, and
- h) Data subject participation.

### **2. Processing of personal data<sup>5</sup>**

A person 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 manner, and
- c) In a reasonable manner.

In respect of foreign data subjects, a data controller or process shall ensure that the personal data is processed in compliance with data protection legislation of the country of the subject where the personal data originating from that country is sent to Ghana for processing.<sup>6</sup>

---

<sup>3</sup>Section 17 – 26, Data Protection Act, 2012 (Act 843)

<sup>4</sup>Section 17, Data Protection Act, 2012 (Act 843)

<sup>5</sup>Section 18, Data Protection Act, 2012 (Act 843)

<sup>6</sup>Section 18 (2), Data Protection Act, 2012 (Act 843)

### 3. Minimality<sup>7</sup>

Personal data may only be processed if the purpose for which it is to be processed, is necessary, relevant, and not excessive.

### 4. Consent, justification, and objection<sup>8</sup>

**Consent<sup>9</sup>:** A person shall not process personal data without the prior 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) Authorized or required by law
- c) To protect a legitimate interest of the data subject
- d) Necessary for the proper performance of a statutory duty or
- e) Necessary to pursue the legitimate interest of the data controller or a third party to whom the data is supplied.

**Objection<sup>10</sup>:** A data subject may object to the processing of personal data unless otherwise provided for or required by law and 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. Collection of Personal Data<sup>11</sup>

The collection of personal data shall be directly from the data subject.<sup>12</sup> However, personal data may be collected indirectly where:<sup>13</sup>

- 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

<sup>7</sup>Section 19, Data Protection Act, 2012 (Act 843)

<sup>8</sup>Section 20, Data Protection Act, 2012 (Act 843)

<sup>9</sup>Section 20(1), Data Protection Act, 2012 (Act 843)

<sup>10</sup>Section 20(2) (3), Data Protection Act, 2012 (Act 843)

<sup>11</sup>Section 21, Data Protection Act, 2012 (Act 843)

<sup>12</sup>Section 21(1), Data Protection Act, 2012 (Act 843)

<sup>13</sup>Section 21(2), Data Protection Act, 2012 (Act 843)

- f) Compliance would prejudice a lawful purpose for the collection or
- g) Compliance is not reasonably practicable.

## **6. Collection of data for specific purpose<sup>14</sup>**

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.

## **7. Data subject to be made aware of the purpose of collection of data <sup>15</sup>**

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

## **8. Retention of records<sup>16</sup>**

Except for records retained for historical, statistical or research purposes which does not contain personal information, 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 authorized 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.

***NB. A data controller shall destroy or delete a record of personal data or de-identify the record at the expiry of the retention period and the destruction or deletion shall be done in a manner that prevents its reconstruction in an intelligible form.***

## **9. Further processing to be compatible with the purpose of collection<sup>19</sup>**

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.

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:

---

<sup>14</sup>Section 22, Data Protection Act, 2012 (Act 843)

<sup>15</sup>Section 23, Data Protection Act, 2012 (Act 843)

<sup>16</sup>Section 24, Data Protection Act, 2012 (Act 843)

<sup>17</sup>Section 24(5), Data Protection Act, 2012 (Act 843)

<sup>18</sup>Section 24(6), Data Protection Act, 2012 (Act 843)

<sup>19</sup>Section 25, Data Protection Act, 2012 (Act 843)

<sup>20</sup>Section 25(3), Data Protection Act, 2012 (Act 843)



- 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
- e) 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
- f) The further processing of the data is in accordance with the Data Protection Act.

## **10. Quality of information<sup>21</sup>**

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.

### **REGISTRATION REGIME UNDER THE ACT<sup>22</sup>**

Registration with the Data Commission: A data controller intends to process personal data shall register with the Commission subject to renewal of certificate every two years.<sup>23</sup>

### **RESPONSIBILITIES OF THE DATA CONTROLLER AT THE TIME OF COLLECTION OF PERSONAL DATA<sup>24</sup>**

Where data is collected from a third party or a data controller who intends to collect personal data he shall ensure that the data subject is aware of:

---

<sup>21</sup>Section 26, Data Protection Act, 2012 (Act 843)

<sup>22</sup>Section 27, Data Protection Act, 2012 (Act 843)

<sup>23</sup>Section 27(1), Section 47, 48, 49 and 50, Data Protection Act, 2012 (Act 843)

<sup>24</sup>Section 27(2), Data Protection Act, 2012 (Act 843)



- a) The nature of the data being collected
- b) The name and address of the person responsible for the collections
- 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 authorized 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.

## OBLIGATIONS IMPOSED UNDER THE ACT

### Obligations of the Data Controller:

**1. Data Protection – Security Measures<sup>25</sup>:** The data controller shall 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 to prevent:

- a) Loss of, damage to, or unauthorized destruction, and
- b) Unlawful access to or unauthorized processing of personal data.

To give effect to this obligation, the data controller shall take reasonable measures to<sup>26</sup>:

- a) Identify reasonably foreseeable internal and external risks to personal data under the data controller’s possession or control.
- 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.

Additionally, the data controller shall observe<sup>27</sup>:

- a) Generally accepted information security practices and procedures, and
- b) Specific industry or professional rules and regulations.

**2. Notification of security compromises<sup>28</sup>:** Where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by an unauthorized person, the data controller or a third party who processes data under the authority of the data controller shall notify (as soon as practicable) the following of the unauthorized access or acquisition:

- a) The Data Protection Commission and
- b) The data subject (affected person)

*(the notification to the data subject shall be delayed where the data controller is informed by the security agencies or the Data Protection Commission that such notification shall impede a criminal investigation<sup>29</sup>)*

<sup>25</sup>Section 28, Data Protection Act, 2012 (Act 843)

<sup>26</sup>Section 28(2), Data Protection Act, 2012 (Act 843)

<sup>27</sup>Section 28(3), Data Protection Act, 2012 (Act 843)

<sup>28</sup>Section 31, Data Protection Act, 2012 (Act 843)

<sup>29</sup>Section 31(4), Data Protection Act, 2012 (Act 843)

Further, the data controller shall take steps to ensure the restoration of the integrity of the information system<sup>30</sup>.

**3. Access to personal information<sup>31</sup>:** This is the obligation of the data controller to confirm at a reasonable cost to the data subject whether or not the data controller holds the personal data of the data subject; 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; correct data held on the data subject where the data subject presents proof of his or her identity.

**4. Correction of personal data<sup>32</sup>:** This is the obligation of the data controller to 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 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 authorization to retain on the request of the data subject.

**5. Notification of changes<sup>33</sup>:** Within 14 days of changes in registered particulars, a data controller shall notify the Commission of such changes.

### **Obligations of a data processor or an authorized person:**

**1. Processing data with consent<sup>34</sup>:** A person who processes personal data on behalf of a data controller (including the data controller) shall process data only with the prior knowledge or authorization of the data controller and treat the personal data which comes to the knowledge of the data processor or the other person as confidential.

Processed data shall not be disclosed unless:

- a) Required by law or
- b) In the course of the discharge of a duty.

**2. Compliance with security measures<sup>35</sup>:** A data processor shall comply with the security measures imposed by the Act.

Also, the processing of personal data by the processor for the data controller must be governed by a written contract<sup>36</sup> with the contract requiring the processor to establish and maintain the confidentiality and security measures necessary to ensure the integrity of the personal data<sup>37</sup>.

Additionally, where the data processor is operating out of Ghana, the Data controller shall ensure compliance with the relevant laws of Ghana.

<sup>30</sup>Section 31(3), Data Protection Act, 2012 (Act 843)

<sup>31</sup>Section 32(1), Data Protection Act, 2012 (Act 843)

<sup>32</sup>Section 33(1), Data Protection Act, 2012 (Act 843)

<sup>33</sup>Section 55, Data Protection Act, 2012 (Act 843)

<sup>34</sup>Section 29(1)(2) Data Protection Act, 2012 (Act 843)

<sup>35</sup>Section 30, Data Protection Act, 2012 (Act 843)

<sup>36</sup>Section 30(2), Data Protection Act, 2012 (Act 843)

<sup>37</sup>Section 30(3), Data Protection Act, 2012 (Act 843)

## RIGHTS OF DATA SUBJECTS UNDER THE ACT

### 1. **Right of access to personal data<sup>38</sup>: This right includes:**

- a. The right to information on the processing of personal data either by the data controller or another person acting on behalf of the data controller.
- b. The description of personal data of the data subject, the purpose for which the data is being or is to be processed, and the recipient or class of recipients to whom the data may be disclosed.
- c. Communication in an intelligent form about information which constitutes personal data of the data subject, information which is available to the data controller as to the source of the data and
- d. Inform 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 the data subject. (this does not apply where data constitutes a trade secret)

Compliance with the request for access is subject to the supply of data which the data controller may reasonably require to identify the person making the request and to locate the data which that person seeks.<sup>39</sup>

The data controller can reject the request where compliance will involve the disclosure of data relating to another person unless the other person consents to the disclosure to the person who made the request, or it is reasonable in all circumstances to comply with the request without the consent of the other person<sup>40</sup>

**2. Right to prevent the processing of personal data<sup>41</sup>:** By notice in writing, the data subject can require a data controller to cease or not begin the processing for a specified purpose or in a specified manner, personal data which causes or is likely to cause unwarranted damage or distress to the data subject<sup>42</sup> and within 21 days of receipt of such notice, the data controller shall inform the data subject of compliance or intention to comply with such notice or of reasons for non-compliance<sup>43</sup>. (*the Commission may order the data controller to comply<sup>44</sup>*).

**3. Right to prevent the processing of personal data for direct marketing<sup>45</sup>:** A data controller shall not provide, use, obtain, procure, or provide information related to a data subject for the purposes of direct marketing without the prior written consent of the data subject<sup>46</sup> and the data subject is entitled at any time

---

<sup>38</sup>Section 35, Data Protection Act, 2012 (Act 843)

<sup>39</sup>Section 35(3), Data Protection Act, 2012 (Act 843)

<sup>40</sup>Section 35(4)(a)(b), Data Protection Act, 2012 (Act 843)

<sup>41</sup>Section 39, Data Protection Act, 2012 (Act 843)

<sup>42</sup>Section 39(1), Data Protection Act, 2012 (Act 843)

<sup>43</sup>Section 39(2)(a)(b), Data Protection Act, 2012 (Act 843)

<sup>44</sup>Section 39(3), Data Protection Act, 2012 (Act 843)

<sup>45</sup>Section 40, Data Protection Act, 2012 (Act 843)

<sup>46</sup>Section 40(1), Data Protection Act, 2012 (Act 843)



by notice in writing to require the data controller not to process his or her personal data for the purposes of direct marketing<sup>47</sup>. *(the Commission may order the data controller to comply with the notice<sup>48</sup>).*

**4. Rights in relation to automated decision-taking<sup>49</sup>:** By notice in writing to a data controller to ensure that any decision taken by or on behalf of the data controller which significantly affects the data subject is not based solely on the processing by automatic means of personal data in respect of data subject<sup>50</sup>.

**5. Rights in relation to exempt manual data<sup>51</sup>:** By notice in writing, a data subject is entitled at any time to require a data controller to rectify, block, erase or destroy exempt manual data which is inaccurate or incomplete or to cease to hold exempt manual data in a manner which is incompatible with the legitimate purposes pursued by the data controller<sup>52</sup> and the said notice shall state the reasons for believing that the data is inaccurate or incomplete or held in a manner which is incompatible with the legitimate purposes pursued by the data controller<sup>53</sup>.

**6. Rights to compensation for the failure to comply<sup>54</sup>:** Where a data subject suffers damages or distress through the contravention by a data controller of any provisions of the Act, the individual is entitled to compensation from the data controller for the damage or distress<sup>55</sup>.

**7. Rights to rectification, blocking, erasure, and destruction of personal data<sup>56</sup>:** Where the personal data of a data subject is inaccurate, on a complaint, the Commissioner may order the data controller to rectify, block, erase, or destroy the data<sup>57</sup>.

## PROHIBITIONS AND SANCTIONS IMPOSED UNDER THE ACT

1. A person shall not purchase the personal data or information contained in the personal data of another person; knowingly obtain or knowingly or recklessly disclose the personal data or information contained in the person data of another person or disclose or cause to be disclosed to another person the information contained in the personal data of another<sup>58</sup>.

A person who engages in the above act commits an offence and is liable on summary conviction to a fine of not more than 250 penalty units or a term of imprisonment of not more than 2 years or to both<sup>59</sup>.

2. A person who sells or offers to sell the personal data of another person commits an offence and is liable on summary conviction to a fine of not more

<sup>47</sup>Section 40(2), Data Protection Act, 2012 (Act 843)

<sup>48</sup>Section 40(3), Data Protection Act, 2012 (Act 843)

<sup>49</sup>Section 41, Data Protection Act, 2012 (Act 843)

<sup>50</sup>Section 41(1), Data Protection Act, 2012 (Act 843)

<sup>51</sup>Section 42, Data Protection Act, 2012 (Act 843)

<sup>52</sup>Section 42(1)(a)(b), Data Protection Act, 2012 (Act 843)

<sup>53</sup>Section 42(2), Data Protection Act, 2012 (Act 843)

<sup>54</sup>Section 43, Data Protection Act, 2012 (Act 843)

<sup>55</sup>Section 43(1), Data Protection Act, 2012 (Act 843)

<sup>56</sup>Section 44, Data Protection Act, 2012 (Act 843)

<sup>57</sup>Section 44(1), Data Protection Act, 2012 (Act 843)

<sup>58</sup>Section 88(1), Data Protection Act, 2012 (Act 843)

<sup>59</sup>Section 88(2), Data Protection Act, 2012 (Act 843)

than 250 penalty units or to a term of imprisonment of not more than 5 years or to both<sup>60</sup>.

3. A person who commits an offence under the Act in respect of which a penalty is not specified, shall be liable on summary conviction to a fine of not more than 5000 penalty units or a term of imprisonment of not more than 10 years or to both<sup>61</sup>.

4. A person who fails to comply with an enforcement notice or an information notice commits an offence and is liable on summary conviction to a fine of not more than 150 penalty units or to a term of imprisonment of not more than 1 year or to both<sup>62</sup>.

A person who, in compliance with an information notice makes a statement which that person knows to be false in a material respect or recklessly makes a statement which is false in a material respect commits an offence and is liable on a summary conviction to a fine of not more than 150 penalty units or to a term of imprisonment of not more than 1 year or to both<sup>63</sup>

*(it is a defence to prove that the person exercised due diligence to comply with the notice in question<sup>64</sup>)*

5. A data controller who has not been registered with the Data Protection Commission shall not process any personal data<sup>65</sup>. A person who fails to register as a data controller, but processes personal data commits an offence and is liable on summary conviction to a fine of not more than 250 penalty units or a term of imprisonment of not more than 2 years or to both<sup>66</sup>.

6. A data controller who contravenes the provisions on assessable processing commits an offence and 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<sup>67</sup>.

## EXEMPTIONS UNDER THE ACT

**1. National Security<sup>68</sup>:** The processing of personal data is exempt from the provisions of the Act for the purposes of:

- a) Public order
- b) Public safety
- c) Public morality
- d) National security or
- e) Public interest.

**2. Crime and Taxation<sup>69</sup>:** the processing of personal data is exempt from the provisions of the Act for the purposes of:

<sup>60</sup>Section 89(1), Data Protection Act, 2012 (Act 843)

<sup>61</sup>Section 95, Data Protection Act, 2012 (Act 843)

<sup>62</sup>Section 80 (1), Data Protection Act, 2012 (Act 843)

<sup>63</sup>Section 80(2), Data Protection Act, 2012 (Act 843)

<sup>64</sup>Section 80(3), Data Protection Act, 2012 (Act 843)

<sup>65</sup>Section 53, Data Protection Act, 2012 (Act 843)

<sup>66</sup>Section 56, Data Protection Act, 2012 (Act 843)

<sup>67</sup>Section 57(6), Data Protection Act, 2012 (Act 843)

<sup>68</sup>Section 60(1), Data Protection Act, 2012 (Act 843)

<sup>69</sup>Section 61(1)(2), Data Protection Act, 2012 (Act 843)

- 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

Personal data is exempt from the non-disclosure provisions of the Act in any case in which the disclosure is for a purpose mentioned above and the application of the provisions relative to disclosure is likely to prejudice any of the matters mentioned above.

**3. Health, Education, and Social Work<sup>70</sup>:** Person data on the following subject 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
- c. Personal data of similar description

**4. Regulatory Activity<sup>71</sup>:** The provisions of the Act do not apply to the processing of personal data for the 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. 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.

The processing of personal data is exempt from the subject information provisions of the 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.

**5. Journalism, Literature, and Art<sup>72</sup>:** A person shall not process personal data unless:

- a. the processing is undertaken by a person for the publication of a literary or

---

<sup>70</sup>Section 62, Data Protection Act, 2012 (Act 843)

<sup>71</sup>Section 63, Data Protection Act, 2012 (Act 843)

<sup>72</sup>Section 64, Data Protection Act, 2012 (Act 843)



- 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.

**6. Research, History, and Statistics<sup>73</sup>:** The further processing of personal data for a research purpose in compliance with the relevant conditions of the Act is not to be regarded as incompatible with the purpose for which the data was obtained.

**7. Disclosure required by law or made in connection with a legal proceeding<sup>74</sup>:** Personal data is exempt from the provisions of the Act on non-disclosure where the disclosure is required by or under an enactment, any rule of law or by the order of a court.

**8. Domestic purposes<sup>75</sup>:** 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.

**9. Confidential references given by data controller<sup>76</sup>:** Personal data is exempt from the data protection principles if it consists of a reference given in confidence by the data controllers 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 provisions of any service by the data subject

**10. Armed Forces<sup>77</sup>:** 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 Ghana <sup>78</sup>

**11. Judicial appointment and honors<sup>79</sup>:** Personal data processed to:

- a. Assess a person's suitability for judicial office or
- b. Confer a national honour is exempt from the subject information provisions of the Act.

**12. Public Service or Ministerial Appointment<sup>80</sup>:** Is subject to any legislative instrument exempting the individual from such subject information provisions. A person's suitability for employment by the government or any office to which

---

<sup>73</sup>Section 65, Data Protection Act, 2012 (Act 843)

<sup>74</sup>Section 66, Data Protection Act, 2012 (Act 843)

<sup>75</sup>Section 67, Data Protection Act, 2012 (Act 843)

<sup>76</sup>Section 68, Data Protection Act, 2012 (Act 843)

<sup>77</sup>Section 69, Data Protection Act, 2012 (Act 843)

<sup>78</sup>Section 69, Data Protection Act, 2012 (Act 843)

<sup>79</sup>Section 70, Data Protection Act, 2012 (Act 843)

<sup>80</sup>Section 71, Data Protection Act, 2012 (Act 843)

appointments are made by the President.

**13. Examination Marks<sup>81</sup>:** Personal data is exempt from the provisions of the Act if it relates to examination marks processed by a data controller to determine the results of an academic, professional, or other examination or to enable the results of the examination to be determined or in consequence of the determination of the results.

**14. Examination Scripts<sup>82</sup>:** Personal data which consists of information recorded by candidates during an academic, professional, or other examination is exempt from the provisions of the Act.

**15. Professional privilege<sup>83</sup>:** 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 a client and a professional adviser could be maintained in legal proceedings.

---

<sup>81</sup>Section 72, Data Protection Act, 2012 (Act <sup>843</sup>)

<sup>82</sup>Section 73, Data Protection Act, 2012 (Act <sup>843</sup>)

<sup>83</sup>Section 74, Data Protection Act, 2012 (Act <sup>843</sup>)

## THE PUBLISHER'S NOTICE OR DISCLAIMER

The information provided in this document does not, and is not intended to, constitute legal advice; instead, all information, content, and materials are for general informational purposes only.

Readers should contact their lawyers to obtain advice with respect to any particular legal matter. No reader or user should act or refrain from acting on the basis of information in this document without first seeking legal advice from his or her lawyers.

The use of, and access to, this document or any other resources by the firm does not create an attorney-client relationship between the reader or user and the firm, key contacts, and contributors.

All liability with respect to actions taken or not taken based on the contents of this document is hereby expressly disclaimed. The content in this document is provided "as is" and no representations are made that the content is error-free or may be affected by subsequent changes in legislation on the subject matter.

### For more information,

visit

**[www.sustineriattorneys.com](http://www.sustineriattorneys.com)**

or follow us on



**@SustineriAttorneys**

or call **+233302553892**