

10 Key considerations for data protection in a pandemic situation - COVID-19

In the context imposed by the novel coronavirus pandemic, the Data Protection Act, 2012 contains useful recommendations for proper protection of personal data, adapted to the new global challenges

All companies are advised to implement specific measures (e.g. limiting travel and physical meetings, respecting hygiene measures and working from home) to limit the spread of the novel coronavirus, but must also treat with the utmost care the privacy and personal data of each individual.

The provisions of the Data Protection Act, 2012 on data privacy are not a hindrance in the fight against the COVID-19 pandemic, but amidst a critical health crisis period, companies are to ensure the protection of the personal data handled and processed in this context.

All principles, Rights of data subjects and Exemptions under the Data Protection Act, 2012 (DPA) are applicable, especially the principles of lawful processing, minimality and purpose limitation.

These are questions that need to be asked:

01

What data are we processing?

Some of the data processed by companies in the context of limiting the spread of the COVID-19 virus are health data. This is a special category of personal data which should be collected in a limited manner and with care by companies. However, not all data processed in this context is health data but may still qualify as personal data.

Example:

Information that a person is infected with COVID-19 is considered health data but, information that a person has returned from a “red area” or has been quarantined (but without giving details of the cause) is not health data but it is still (general) personal data and requires adequate security measures and safeguards to be put in place.

02

Why are we processing such data?

In the context of epidemics, personal data may be processed by companies and competent public health authorities without the need to obtain the consent of the data subject but based on other grounds provided by Section 63 of the DPA. Nevertheless, for the processing of health data, a legal basis needs to be identified, in accordance with Section 25 of the DPA, since COVID-19 may be considered “imminent threat to public health or safety” and the measures taken by companies are meant to protect the health of their employees and the general public. However, these extraordinary grounds for data processing do not justify any type of measures, but only necessary and reasonable measures.

03

Is all that data needed?

Despite the ruckus of the COVID-19 pandemic, companies must ensure that in their efforts to support the government in contact tracing and mitigation activities, they do not trample on the rights of data subjects. Companies must ensure that data collected and handed over to health and government officials are relevant and not excessive in line with the minimality principle and with respect to privacy of the individual as stated in the DPA.

Example:

Disclosing employee’s family records, past transactions amongst others when health officials ask for a specific data reference.

04

What should we do?

Organisations should employ the use of safer and less invasive methods to solicit information about employees, customers and visitor movements. The company has the obligation under Section 28 of the DPA to:

- a. Ensure the integrity of such data in their possession
- b. Prevent unlawful access to or unauthorised processing of the collected data
- c. Fully assess and understand the internal and external risks to the data under its control
- d. Implement appropriate measure to protect the data against the identified risks
- e. Observe generally accepted information security practices and procedure
- f. Register with the DPC as a Data Controller to avoid sanctions as detailed in Section 56 of the DPA whilst benefitting from defence for breaches provided under Section 43.

05

What shouldn't we do?

Companies should avoid the following decisions with respect to their employee’s, visitor’s or customer’s data:

- a. Do not collect data such as temperature readings and symptoms from people in secret.
- b. Unless authorised by law or under an order of the Court, do not disclose the health records of the employee to other employees inside the company and external parties.
- c. Do not make health readings a mandatory routine to be sent to a dedicated person in the company
- d. Do not retain personnel records for a period longer than is necessary to achieve the purpose for which the data was collected and processed.

06

Who can know what we know?

Should a COVID-19 case occur on premise, the company is required to inform its employees. Disclosure of the employee's identity to other employees or third parties outside the company is a breach of confidentiality unless it is required by law according to Section 62 of the DPA.

07

What can we disclose?

The DPA highlights that public disclosure may be made in support of public interest. The Government of Ghana has not made any open recommendations as to what extent of an individual's information is necessary for disclosure. However, recent trends only depict disclosure of statistical data (for example, area case count, national case count, recoveries, and fatalities).

08

What should my employees/customers know?

Companies must ensure that employees/customers know the following:

- a. The data being processed
- b. The purpose for which the data is being or is to be processed
- c. The recipient or recipients to whom the data may be disclosed
- d. 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.

09

Is the data safe in our possession?

Companies should ensure that personal data are adequately protected against access or use for unauthorised purposes. Companies should also ensure data are complete, accurate, up to date and not misleading having regard to the purpose for the collection or processing of the personal data. It is also advisable that companies ensure the proper recording of all data processing activities carried out for the purpose of limiting the spread of the virus.

10

What rights do our employees/customers have?

Companies should respect all data subjects' rights as provided under the DPA.

Andrew Akoto
Partner & Head
Advisory Services

Tel: +233 (302) 770454,770618
E: aakoto@kpmg.com

Samuel Aluko
Associate Director
IT Advisory

Tel: +233 (302) 770454,770618
E: samuelaluko@kpmg.com

Tobi Ogunbadejo
Manager
IT Advisory

Tel: +233 (302) 770454,770618
E: tobiogunbadejo@kpmg.com

kpmg.com/socialmedia



kpmg.com/app



© 2020 KPMG, a partnership registered in Ghana and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Ghana.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.