

REPUBLIC OF KENYA
OFFICE OF THE DATA PROTECTION COMMISSIONER
GUIDANCE NOTE ON PERSONAL DATA PROTECTION ON COVID-19 RESPONSES

1. INTRODUCTION

The declaration of the COVID-19 as a global pandemic by the World Health Organization and the subsequent acknowledgement of the same by the Government of Kenya, has led to stringent measures being put in place to combat the effects of the Pandemic.

- a.1. Mitigating the effects of the Covid-19 pandemic on livelihoods of individuals and communities includes scaling the local innovations and products, job creation, sustainability of micro, small and medium enterprises, boosting the digital economy and assuring consumer protection.
- a.2. There are a number of Government initiatives that promote innovative responses to mitigate the effects of the COVID-19. Cognizance is given to the ICT Advisory Committee that was established by the Cabinet Secretary Ministry of ICT, Innovations and Youth Affairs, in recognition of the critical role of ICT's during the pandemic, to coordinate ICT specific responses to mitigate the effects of Covid-19.
- a.3. Innovations and Interventions, whether ICT based or otherwise, are necessary to enhance the quality of life and ensure continuity of jobs, business and learning, ensure provision of universal and affordable health care, amongst others.
- a.4. For some of these aspirations to materialize, access and processing of personal data of individuals is necessary to appropriately respond to the pandemic. For instance, health data and geo-location may be necessary for contact tracing. Innovations built in response to pandemic including apps and related services, may request some access to personal data from a government or private entities to enable the development of a product.
- a.5. In these initiatives, assuring privacy of individuals through the protection of their personal data is paramount. To this extent, the processing of personal data has to be guided by the Data Protection Act No. 24 of 2019.
- a.6. This note offers policy guidance to any person processing personal data of individuals to actualize responses and research, on the pandemic, including data requests by innovators and any other use, to give effect to the right to privacy as it relates to the protection of personal information.

2. APPLICABLE LAW

- 2.1 The applicable law that guides the use of personal data of individuals is the Data Protection Act No. 24 of 2019.
- 2.2 Every person who requires or utilizes personal data has to comply with the Data Protection Act, in addition to any other sectorial law that may apply.

3. KEY PRINCIPLES

- 3.1 Responsible parties must process personal data in an accountable manner. Every personal data collection, use, sharing, storage and other processing of Personal data shall be based on the principles of data processing provided in the Data Protection Act.
- 3.2 Responsible parties must collect personal information of an individual for a specific purpose, which in this context is to detect, contain and prevent the spread of COVID-19.
- 3.3 Personal Data requested shall only be that which is adequate, relevant and limited to what is necessary in relation to the purpose for which the personal data is requested.
- 3.4 Personal data shall not be kept for longer periods than is necessary to achieve the purpose for which the data was collected and processed.
- 3.5 Once the purpose for which the data is collected is achieved, the data shall be destroyed. The person responsible shall ensure that the personal data is de-identifiable.
- 3.6 Personal data on record must be correct, complete, and be kept up to date.
- 3.7 Personal data must be processed securely to retain confidentiality and integrity in consistency, accuracy, and trustworthiness over its entire life cycle.
- 3.8 Any person who has access to personal data shall be responsible for its protection and demonstrate having put in place proactive mechanism to appropriately safeguard the personal data.

4. MECHANISM OF DATA REQUEST

- 4.1 To the extent possible, personal data shall be collected directly from individuals subject to their express consent in form of the **DATA REQUEST FORM** annexed to this guidance note.
- 4.2 Any personal data sharing between parties has to be guided by a valid agreement including nondisclosure, data confidentiality provisions, data protection safeguard provisions including the data destruction technique to be used, data protection impact

statement based, a data responsibility matrix, and should be approved by the Office of the Data Protection Commissioner

- 4.3 An access to personal data must be limited to those who need the information to conduct treatment, research or other responses that are addressing the crisis or any other relevant exemption.
- 4.4 Personal data shall, to the largest extent possible, be in anonymized format and in a manner that individuals cannot be re-identified.
- 4.5 For the applications requesting access to personal data, the concerned person shall publish policies on what information is being collected and with whom the information may be shared.
- 4.6 Any personal data kept for a longer duration shall be non-identifiable information.
- 4.7 Under no circumstances should the data collected be sold to third parties or transferred out of the country, unless the concerned individual consents to the transfer. The transfer of personal data to another country shall only take place where sufficient proof has been given on the appropriate safeguards with respect to the security and protection of the personal data.

5. IMPLEMENTATION

- 5.1 For public entities, requests for personal data shall be channeled through the relevant agencies. For example, health data shall be sourced from the Ministry of Health; telecommunications data from the Communications Authority of Kenya, transport data from the National Transport and Safety Authority, among others.
- 5.2 A person requesting personal data is expected to enter into a data protection and sharing agreement with the entity or person having control of the personal data.
- 5.3 A person possessing personal data of individuals is expected to demonstrate compliance to the Data Protection Act, and may be called upon by the Data Protection Commissioner to do so.
- 5.4 This framework may undergo changes as appropriate, to be consistent with future developments, industry trends and/or any changes in legal or regulatory requirements.

IMMACULATE KASSAIT
Data Protection Commissioner

January 2021