

DISPUTES

The right to privacy and the Amendments to the Disaster Management Regulations

8 April 2020 10 min read

by Jones Antunes, Director; Innocentia Moele; Senior Associate; and Danielle Hertz, Candidate Attorney

1. On 1 April 2020 the Minister of Cooperative Governance and Traditional Affairs amended the regulations issued in terms of the Disaster Management Act, 2002, by, inter alia, introducing Chapter 3 into the Amended Disaster Regulations (“**the Amended Disaster Regulations**”).
2. Chapter 3 of the Amended Disaster Regulations provide, inter alia, for the monitoring and tracing of the location or movements of any person known or reasonably suspected to have contracted COVID-19 or the location or movements of any person known or reasonably suspected to have come into contact with a person known or reasonably suspected to have contracted COVID-19, to be tracked through their mobile phones.
3. The amendment to the Amended Disaster Regulations provide for the establishment of the “**COVID-19 Tracing Database**”.
4. The National Department of Health shall develop and maintain the national database to enable the tracing of persons who are known or reasonably suspected to have come into contact with any person known or reasonably suspected to have contracted COVID-19.
5. The COVID-19 Tracing Database must include all information considered necessary for the contact tracing process to be effective including but not limited to:
 - a. the first name and surname, identity or passport numbers, residential address and other address where such person could be located and cellular phone numbers of all persons who have been tested for COVID-19;
 - b. the COVID-19 test results of all such persons; and
 - c. the details of the known or suspected contacts of any person who tested positive COVID-19.
6. The information contained in the COVID-19 Tracing Database and any information obtained through the Amended Disaster Regulations is confidential and no person may disclose any information contained in the COVID-19 Tracing Database or any information obtained through the Amended Disaster Regulations unless authorised to do so and unless a disclosure is necessary for the purpose of addressing, preventing or combating the spread of COVID-19.
7. Where any person is to be tested for COVID-19, the person taking the sample for purposes of testing must obtain as much of the following information as is available at the time of taking the sample:
 - a. the first name and surname, identity or passport number, residential address and cellular phone number of the person tested; and
 - b. a copy of photograph of the passport, a drivers licence, identity card or identity book of the person tested, and properly submit this information, along with any information it has regarding likely contacts of the person tested, to the Director General: Health (“**the DGH**”), for inclusion in the COVID-19 Tracing Database.
8. Where any laboratory has tested a sample for COVID-19, the laboratory must properly transmit to the DGH for inclusion in the COVID-19 Tracing Database:
 - a. all details the laboratory has, including the first name and surname, identity or passport numbers, residential address and cellular phone numbers, regarding the person tested; and
 - b. the COVID-19 test result concerned.

9. The National Institute for Communicable Diseases (“**NICD**”) must transmit to the DGH for inclusion in the COVID-19 Tracing Database:
 - a. all details the NICD has, including the first name and surname, identity or passport numbers, residential address and cellular phone numbers of any person tested for COVID-19; and
 - b. the results of the COVID-19 test concerned and any information the NICD has regarding likely contacts of the person tested.
10. The DGH may in writing and without prior notice to the person concerned, direct an electronic communication service provider licenced under the Electronic Communications Act, 2005 to provide him / her for inclusion in the COVID-19 Tracing Database with such information as the Electronic Communications provider has available to it regarding:
 - a. the location of movements of any person known or reasonably suspected to have contracted COVID-19; and
 - b. the location of movements of any person known or reasonably suspected to have come into contact during the period 5 March 2020 to the date on which the national state of disaster has lapsed or has been terminated, with a person contemplated in sub-paragraph 10.1; and the electronic communications service provider must properly comply with the directive concerned.
11. The information referred to in paragraph 10 above:
 - a. may only be obtained in relation to the location or movements of persons during the period 5 March 2020 to the date on which the national state of disaster has lapsed or has been terminated;
 - b. may only be obtained, used or disclosed by authorised persons and may only be obtained, used and disclosed when necessary for the purposes of addressing, preventing or combating the spread of COVID-19 through the contact tracing process;
 - c. where relevant to the contact tracing process must be included in the COVID-19 Tracing Database;
 - d. apart from what is included in the COVID-19 Tracing Database, may only retained by the DGH for a period of six weeks after being obtained and shall thereafter be destroyed.
12. The regulations provide further for the Cabinet member responsible for Justice and Correctional Services to designate a retired Judge as the COVID-19 Designated Judge.
13. Former Constitutional Court Judge Catherine O'Regan has been appointed as the COVID-19 Designated Judge.
14. In terms of the Amended Disaster Regulations, the DGH must file a weekly report with the COVID-19 Designated Judge setting out the names and details of all persons whose location of movements were obtained in terms of the Amended Disaster Regulations.
15. The COVID-19 Designated Judge may make such recommendations to the Cabinet members responsible for Cooperative Governance and Traditional Affairs, Health and Justice and Correctional Services as she deems fit regarding the amendment or enforcement of the Amended Disaster Regulations in order to safeguard the right to privacy while ensuring the ability of the Department of Health to engage in urgent and effective contact trading to address, prevent and combat the spread of COVID-19.
16. The DGH shall, within six weeks after the national state of disaster has lapsed or has been terminated, notify every person whose information has been obtained in terms of the Amended Disaster Regulations, that information regarding their location or movements was obtained in terms of the Disaster Management Regulations.
17. Within six weeks after the national state of disaster has lapsed or has been terminated:
 - a. the information on the COVID-19 Tracing Database shall be de-identified;
 - b. the de-identified information on the COVID-19 Tracing Database shall be retained and used only for research, studying and teaching purposes;
 - c. all information on the COVID-19 Tracing Database which has not been de-identified shall be destroyed; and
 - d. the DGH shall file a report with the COVID-19 Designated Judge recording the steps taken in this regard.
18. Upon receipt of the report, the COVID-19 Designated Judge shall be entitled to give directions as to any further steps to be taken to protect the right to privacy of those persons whose data has been collected, which directions must be complied with.
19. There is some concern that the Amended Disaster Regulations will be abused by the State to spy on people and that the Amended Disaster Regulations infringes Section 14 of the Constitution which provides, that everyone has a right to privacy, which includes the right not to have the privacy of their communications infringed.
20. It appears however that the Amended Disaster Regulations have been carefully crafted so as to ensure that the right to privacy is only limited, insofar as it is necessary to control the spread of COVID-19. This limitation on privacy is therefore only justifiable to the extent

- that the collection and processing of personal information takes place with the express purpose of detecting, containing and preventing the spread of COVID-19. Moreover, the potential for abuse has been limited by the appointment of the COVID-19 Designated Judge.
21. To further guard against the unlawful use of the personal information collated and processed in accordance with the Amended Disaster Regulations, on 6 April 2020, The Information Regulator ("**the Information Regulator**") issued a Guidance Note on the processing (e.g. collection, receipt, usage) of personal information of data subjects (owners of personal information) in the management and containment of COVID 19 ("**the Guidance Note**").
22. The Guidance Note states that the Information Regulator is mindful of the fact that not all of the provisions of the Protection of Personal Information Act, 2013 ("**POPIA**") have not yet come into effect. However, the Regulator nonetheless encourages proactive compliance by responsible parties when processing personal information of data subjects who have tested or are infected with COVID-19, or who have been in contact with such data subjects.
23. The Guidance Note has been issued to:
- give effect to the right to privacy as it relates to the protection of personal information;
 - provide guidance to the public and private bodies and their operators on the limitation of the right to privacy when processing personal information of data subjects for the purpose of containing the spread and reduce the impact of COVID-19.
24. In terms of the Guidance Note, Responsible Parties must process personal information of data subjects in a responsible, lawful and reasonable manner during the management of Covid-19.
25. Furthermore, the Guidance Note provides that it is not necessary for a responsible party to obtain consent from a data subject to process his or her personal information in the context of COVID-19, when:
- processing complies with the obligation imposed by law on the responsible party;
 - processing protects a legitimate interest of the data subject;
 - processing is necessary for the proper performance of a public law duty by a public body; or
 - processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.
26. Responsible parties must not retain records of personal information of data subjects for longer than authorised to achieve the purpose of detecting, containing and preventing the spread of COVID-19 unless such information is required for historical, statistical or research purposes and provided that adequate safeguards are in place.
27. Further, it is required that when the party responsible for the information is no longer authorised to retain the record, must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable. The destruction or deletion of personal information must be done in a manner that prevents its reconstruction in an intelligible form.
28. The overriding principle in the processing of the personal information of Data Subjects is that such use must be tied to a specific purpose, which is to contain and prevent the spread of COVID-19 and the only time that a responsible party may process the personal information outside of this "original purpose" for which it was collected if:
- it is necessary to prevent a serious and imminent threat to public safety or public health, the life or health of a data subject or another individual;
 - the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for that purpose and will not be published in an identifiable form.
29. A responsible party:
- should ensure that the personal information is complete, accurate, not misleading and updated where necessary, taking into consideration the purpose for which the information was further processed.
 - must maintain the documentation of all processing operations which relate to detecting, containing and preventing the spread of COVID-19.
 - must take appropriate, reasonable technical and organisational measures to prevent the loss or damage to or unauthorised access of personal information.
30. It appears therefore that a sensible balance has been achieved between the right to privacy and the need to prevent and control the spread of Covid-19.



Jones Antunes

Director

[View Profile](#)