

GUIDANCE NOTE ON THE PROCESSING OF PERSONAL INFORMATION IN THE MANAGEMENT AND CONTAINMENT OF COVID-19 PANDEMIC IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 (POPIA)

1. INTRODUCTION

1.1. The World Health Organization (WHO) declared the CoronaVirus (COVID-19) a pandemic. Countries across the world, including the Republic of South Africa, are racing to slowdown the spread of the virus by testing and treating patients, carrying out contact tracing and declaring a lockdown. COVID-19 has the potential to create social and economic calamity if not managed.

1.2. As a result, and in order to manage and curb the spread of COVID-19, the South African Government has issued Regulations in terms of section 27(2) of the Disaster Management Act 57 of 2002 (Regulations).

1.3. In terms of section 10(8) of the Regulations of 18 March 2020:

“ *any Minister may issue and vary directions, as required, within his or her mandate, to address, prevent and combat the spread of COVID-19, from time to time as may be required, including-*

a) *Disseminating information required for dealing with the national state of disaster;*

b) *Implementing emergency procurement procedures;*

c) *Taking any other steps that may be necessary to prevent an escalation of the national state of disaster; or*

d) *Taking steps to facilitate international assistance.”*

1.4. The National Command Council (NCC) is tasked with the coordination and implementation of measures to contain the spread and to mitigate the impact of COVID-19.

2. **PURPOSE:**

2.1. The Information Regulator (Regulator) is mindful of the fact that not all the sections of POPIA have come into effect. The Regulator 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.

2.2. The Regulator is issuing this Guidance Note to-

2.2.1. give effect to the right to privacy as it relates to the protection of personal information;

2.2.2. 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.

2.3. The Regulator recognises the need to effectively manage the spread of COVID-19, which has necessitated the limitation of various constitutional rights of data subjects. The Regulator therefore supports the need to process personal information of data subjects in order to curb the spread of COVID-19.

3. **RELEVANT DEFINITIONS**

3.1. “**data subject**” means the person to whom personal information relates.

3.2. “**operator**” means a person who processes personal information for a responsible party in terms of a contract or a mandate.

3.3. “**personal information**” means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –

- a) information relating to race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.
- b) information relating to the education or the medical, financial, criminal, or employment history of the person.
- c) any identifying number, symbol, e-mail addresses, physical address, telephone number, location information, online identifier or other particular assignment to the person.
- d) the biometric information of the person.
- e) the personal opinions, views or preferences of the person.
- f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.
- g) the views or opinions of another individual about the person.
- h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

3.4. **“private body”** means—

- a) natural person who carries or has a carried on any trade, business or profession, but only in such capacity;
- b) a partnership which carries or has carried any trade, business or profession;
- c) any former or existing juristic person, but excludes a public body.

3.5. “**processing**” means any operation or activity or any set of operations whether or not by automatic means concerning personal information, including:

- a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
- b) dissemination by means of transmission, distribution or making available in any form; or
- c) merging, linking, as well as restriction, degradation, erasure or destruction of the information.

3.6. “**public body**” means—

- a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
- b) any other functionary or institution when –
 - (i) exercising a power or performing a duty in terms of the constitution in terms of the constitution; or
 - (ii) exercising a public power or performing a public function in terms of any legislation.

3.7. “**responsible party**” means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information. The following are examples of responsible parties in the context of the management of COVID-19 and include but not limited to, the NCC, National Department of Health, Provincial Department, Local Government, National Institute of Communicable Disease (NICD), National Health Laboratories Services (NHLS), Independent laboratories, Mobile Network Operators, Voluntary Organizations.

- 3.8. **“special personal information”** means personal information concerning-
- a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
 - b) the criminal behaviour of a data subject to the extent that such information relates to-
 - i. the alleged commission by a data subject of any offence; or
 - ii. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

4. **RESPONSIBLE PARTIES MUST ADHERE TO THE FOLLOWING CONDITIONS WHEN PROCESSING PERSONAL INFORMATION OF DATA SUBJECTS**

4.1. **Accountability**

Responsible parties must process personal information of data subjects in a responsible manner during the management of COVID-19.

4.2. **Lawfulness of processing**

Responsible parties must process the personal information of data subjects in a lawful and reasonable manner in order to detect, contain and prevent the spread of COVID-19.

4.3. **Consent, justification and objection**

4.3.1. 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:

- 4.3.1.1. processing complies with the obligation imposed by law on the responsible party;

- 4.3.1.2. processing protects a legitimate interest of the data subject;
- 4.3.1.3. processing is necessary for the proper performance of a public law duty by a public body; or
- 4.3.1.4. processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

4.4. **Collection for a specific purpose**

Responsible parties must collect personal information of a data subject for a specific purpose, which in this context is to detect, contain and prevent the spread of COVID-19.

4.5. **Retention and restriction of records**

4.5.1. 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.

4.5.2. A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record.

4.5.3. The destruction or deletion of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

4.6. **Further processing to be compatible with purpose of collection**

A responsible party may further process personal information of a data subject notwithstanding the fact that such processing is not compatible with the 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. This exception also applies if 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.

4.7. Quality of Information

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.

4.8. Documentation

A responsible party must maintain the documentation of all processing operations which relate to detecting, containing and preventing the spread of COVID-19.

4.9. Security measures on integrity and confidentiality of personal information

- 4.9.1. In order to secure the integrity and confidentiality of personal information collected in relation to COVID-19, a responsible party must take appropriate, reasonable technical and organisational measures to prevent the loss or damage to or unauthorised access of personal information.
- 4.9.2. An operator must only process personal information with the knowledge or authorisation of a responsible party and should treat such information as confidential, and only disclose such information if required to do so by law, or in the course of the proper performance of their duty.
- 4.9.3. The responsible party must enter into a written contract with an operator to ensure that the operator establishes and maintains appropriate, reasonable, technical and organisational security measures when processing personal of data subjects.

4.9.4. In the event of a unauthorised access to the system of the operator, such an incident should be reported immediately to the responsible party by the operator.

4.9.5. A responsible party must report any unauthorised access of personal information of a data subject to the Regulator and the data subjects within reasonable time.

4.10. **Access to personal information**

A responsible party must upon request confirm whether or not it holds personal information about a data subject.

4.11. **Special personal information**

4.11.1. Although a responsible party is not allowed to process special personal information of a data subject, medical professionals, healthcare institutions or facilities or social services may process special personal information of a data subject, if such processing is necessary for the proper treatment and care of a data subject in the context of COVID-19.

4.11.2. A responsible party may only process special personal information subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between a responsible party and a data subject.

5. **SHARING OF LOCATION BASED DATA**

5.1. **Can Electronic Communication Service Providers process (provide) location-based data to the Government to process (use) for the purpose of tracking data subjects to manage the spread of COVID-19?**

Yes, The Electronic Communication Service Providers must provide the Government with mobile location-based data of data subjects and the Government can use such personal information in the management of the spread of COVID19 if:

- a) processing complies with an obligation imposed by law on the responsible party; or
- b) processing protects the legitimate interest of a data subject; or
- c) processing is necessary for the proper performance of a public law duty by a public body; or
- d) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

However, the Government must still comply with all the applicable conditions for the lawful processing as set out in this Guidance Note.

5.2. **Can Electronic Communication Service Providers process (provide) location-based data to the Government to process (use) for the purpose of conducting mass surveillance of data subjects to manage the spread of COVID-19?**

Yes, Electronic Communication Service Providers can provide the Government with location-based data of data subjects and the Government can use such personal information for the purpose of conducting mass surveillance of data subjects if the personal information is anonymised or de-identified in a way that prevents its reconstruction in an intelligible form.

6. **EMPLOYMENT**

6.1. **Can the employer request specific information on the health status of an employee in the context of COVID-19?**

Yes, the employer is obliged to maintain a safe and hazardous free working environment in terms of the Occupation Health and Safety Act 85 of 1993 read together with the Employment Equity Act 55 of 1998, if an employee's health status may endanger other employees. The disclosed information should not be used to unfairly discriminate against such an employee.

6.2. **Can the employer force an employee to undergo testing for the COVID-19 virus?**

Yes, the employer can force an employee to undergo testing in order to maintain a safe working environment.

7. **CONSENT**

7.1. **Can a data subject refuse to give consent to be tested for COVID-19?**

No, the Regulations require any data subject to undergo mandatory testing in order to manage the spread of COVID-19.

8. **GENERAL**

8.1. **Does a person who has tested positive for COVID-19 have a duty to disclose his or her status?**

Yes, a person who has tested positive has a duty to disclose his or status to enable the Government to take appropriate measures to combat the spread of COVID-19.

9. **CONCLUSION**

The South African Government have issued Regulations in terms of section 27(2) of the Disaster Management Act 57 of 2002 to combat the spread of COVID-19. The Regulations should be implemented in conjunction with the applicable conditions for the lawful processing of personal provided for in POPIA to ensure respect for the right to privacy.

Information Regulator