FORM 15
ENFORCEMENT NOTICE IN TERMS OF SECTION 95 OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 12(2)(c)]

Reference number: CI 317-22

A	DETAILS OF DATA SUBJECT
Name(s) and surname/ registered name of data subject/complainant/aggrieved party:	Own initiative investigation in terms of section 76 (3) of the Protection of Personal Information Act 4 of 2013 (POPIA)
Unique Identifier/ Identity Number	
Residential, postal or business address:	JD House 27 Stiemens Street Braamfontein Code (2001)
Contact number(s):	010 023 5200
Fax number E-mail address:	enquiries@infoRegulator.org.za
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	Lt-General Sehlahle F Masemola The National Police Commissioner South African Police Service (SAPS)
Residential, postal or business address:	Maupa Naga Building 3rd Building 3 Troye Street Pretoria Code ( )
Contact number(s):	
Fax number/ E-mail address:	selepemashadi@saps.gov.za

A. Be pleased to take notice that the Information Regulator (Regulator) after having considered the report of the Enforcement Committee hereby decides that the protection of personal information of the data subjects has been interfered with as follows:

subject has been interfered with as follows:

X	A breach of the conditions for the lawful processing of personal information.
X	Non-compliance with the duty to notify security compromises (section 22 of the Protection of Personal Information Act 4 of 2013)
	Non-compliance with the duty of confidentiality (section 54 of the Protection of Personal Information Act 4 of 2013)
	Non-compliance with obligations for direct marketing by means of unsolicited electronic communications (section 69 of the Protection of Personal Information Act 4 of 2013)
	Non-compliance with obligations regarding the inclusion of personal information in directories (section 70 of Protection of Personal Information Act 4 of 2013)
	Non-compliance with obligations regarding automated decision making (section 71 of the Protection of Personal Information Act 4 of 2013)
	Non-compliance with obligations regarding personal information outside the Republic of South Africa (section 72 of the Protection of Personal Information Act 4 of 2013)
	Breach of the provision of a code of conduct issued in terms of section 60: Code of Conduct ……. of (Reference)

B. The reasons for reaching this conclusion are:

1. The responsible party did not meet the requirements for exclusion under section 6 (1) (c) (ii) of Protection of Personal Information Act 4 of 2013 (POPIA) because it failed to demonstrate that it has any safeguards in place, let alone safeguards established in legislation as intended by section 6 (1) (c) (ii) of POPIA.

2. The responsible party has breached the following conditions for the lawful processing of personal information:

Section 8 of POPIA.

The responsible party did not ensure that the conditions for the lawful processing of personal information stipulated in Chapter Three (3) of POPIA were complied with, as it is enjoined to do so in terms of section 8 POPIA. For this reason, the responsible party has breached section 8 of POPIA.

Section 9 of POPIA

Section 9 of POPIA provides that personal information of data subjects must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject. By distributing the personal information of data subjects on WhatsApp, the responsible party was not doing so for the proper performance of a public law duty by a public body and did so without the consent of the data subject. The responsible party failed to comply with sections 10,11, 15,19 and 22 of POPIA as stated hereunder. Consequently, the responsible party processed the personal information of the data subjects unlawfully and unreasonably in a manner which infringed their privacy in violation of section 9 of POPIA.

Section 10 of POPIA

Section 10 of POPIA provides that the responsible party's explanation included the following: that it distributed the personal information of data subjects on various WhatsApp groups to alert the respective stations and units of a serious crime which happened in the West Rand District and to mobilise the available resources to respond accordingly and trace possible suspects and to source information from the members of the public which included cleaners and administrative clerks in the police station .The Regulator fails to understand how the detailed personal information of data subjects, which included their ages, occupations and residential addresses was relevant to the mobilisation of resources or in the tracing of the suspects. In the premise, the responsible party did not comply with section 10 of POPIA because the personal information of data subjects that was distributed on WhatsApp was excessive and not relevant for the purpose for which it was distributed.

Section 11 of POPIA

Section 11 of POPIA provides that personal information of a data subject may only be processed if at least one of the six (6) grounds for justification provided for in section 11 (1) (a) – (f) are met. If none of these grounds is applicable, then consent of the data subject is required. The processing of personal information of data subjects by distribution on WhatsApp was not done for the proper performance of a public law duty on the part of the responsible party. Therefore, such processing had to be done with the consent of the data subjects. In the premise, the responsible party did not comply with section 11 of POPIA.

Section 15 of POPIA

Section 15 of POPIA provides that further processing of personal information must be compatible with the purpose for which the personal information was collected. The personal information of data subjects was collected for the investigation and prosecution of crimes committed against data subjects. Section 15(2) of POPIA details the factors that must be taken into account to assess whether the further processing of personal information is compatible with the purpose for which the information was collected. Section 15(3)(c) of POPIA gives instances in which further processing is not incompatible with the purpose of collection. These include the fact that further processing is necessary to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences.

The responsible party conceded that the excessive processing of personal information of data subjects distributed on WhatsApp does not enhance their investigation, that it was an unintentional oversight on their part as this was done in breach of POPIA, and that they failed to consider compliance with conditions 4 and 7 of POPIA. In its own words, the responsible party in its submission, stated that "*there may have been a lapse of judgement by individuals within the SAPS by further processing the information incorrectly. Such actions were unintentional*". These concessions demonstrate that the distribution of personal information of data subjects on WhatsApp was not compatible with the purpose for which the information was collected.

Furthermore, as a consequence of the wide and indiscriminate distribution of the WhatsApp message, it was leaked from its intended communication channels which resulted in the message being shared widely on various social media platforms, such as Facebook, which does not in any way relate to the purpose for which the personal information was collected. For these reasons, the Regulator finds that the responsible party did not comply with section 15 of POPIA.

Section 19 of POPIA

Section 19 of POPIA sets out the measures to be taken to ensure the integrity and confidentiality of personal information and the duty of a responsible party to take appropriate, reasonable, technical and organisational measures to prevent *inter alia* the loss and unlawful access to or processing of personal information.

The personal information of the data subjects was included in a WhatsApp message, a social media platform, that was forwarded by a senior officer of the SAPS to the Provincial Commissioner of the SAPS and subsequently to the Gauteng Generals' WhatsApp Group, comprising of thirty (30) participants, the West Rand District Commissioner's WhatsApp Group, comprising of seventy-seven (77) participants and the Randfontein SAPS Station group, comprising of one hundred and forty-eight (148) participants. Ultimately, the message also circulated on social media platforms such as Facebook.

The message was not circulated via an official authorised police messenger service with unique user and security features, and prescribed content and distribution protocols.

Although certain security measures are built into the WhatsApp platform, the message was unlawfully processed by some of the individuals to whom it was distributed.

The responsible party did not provide any relevant documentary evidence with reference to protocols, management supervision, content management, usage, and distribution policy of specifically WhatsApp messages within SAPS applicable at the time of the incident.

The absence of an official documentary instrument and clear guidelines for content management and usage of WhatsApp within the responsible party may have contributed to the occurrence of the incident.

The responsible party did not provide any relevant documentary evidence with relation to a risk management plan and risk mitigation strategy in relation to the specific usage of WhatsApp as a communication tool within SAPS. The possible leak of personal information via WhatsApp was not foreseen by the management of the responsible party and no pro-active measures were put in place for such an event, notwithstanding the possible internal and external risks posed by the usage of the WhatsApp platform as a mode of communication. The absence of sufficient managerial oversight in the compilation and distribution of the message is an indication of the lack of appropriate safeguards and the ineffective implementation of safeguards to secure the personal information of data subjects.

Although the new improved security measures were said to have been introduced by the SAPS after the incident, regrettably these measures were not disclosed to the Regulator.

In the premise, the Regulator finds that:

There is no relevant evidence that the processing of the personal information of data subjects by the senior officers who distributed the WhatsApp message was in accordance with appropriate, reasonable technical and organisational measures as envisaged in section 19(1) of POPIA.

There is no relevant evidence provided by the responsible party of reasonable measures to identify foreseeable internal and external risks to personal information under its control, to establish and maintain appropriate safeguards, regularly verifying the safeguards and ensuring updating in response to new risks with specific reference to WhatsApp, in terms of section 19(2).

Section 22 of POPIA

Section 22 sets out the duties and obligations of the responsible party in the case of security compromises and the accessing of personal information of data subjects by unauthorised persons. The responsible party is required to notify the Regulator and the data subjects, respectively.

Regarding the measures that have been taken by the SAPS to comply with section 22 of POPIA to protect the data subjects from the consequences of the publication of their personal information in the public domain, the SAPS stated that they did not take any steps envisaged in section 22(1)(a) and (b) of POPIA by notifying the Regulator and the data subjects of the security compromise because this was overtaken by events.

In the premise, the Regulator finds that the responsible party did not comply with sections 22(1)(a) and 22(1)(b) of POPIA.

C. The responsible party is hereby ordered to:

Take the following specified steps:

1) Notify the Regulator and the data subjects of the security compromise of their personal information in compliance with section 22 of POPIA within thirty-one (31) days of the date of receipt of this Enforcement Notice.
2) Publish an apology to data subjects for processing their personal information in a manner that breached the conditions for the lawful processing of personal information stipulated in this Enforcement Notice. The apology must be published prominently in all major national weekly newspapers and in all social media platforms such as Facebook and Twitter. The apology must not contain the personal information of the data subjects. Proof of the publication of the apology must be submitted to the Regulator within thirty-one (31) days of the date of receipt of this Enforcement Notice.
3) Investigate the conduct of the SAPS members who were involved in the unlawful processing of personal information of data subjects on WhatsApp and, if necessary, take appropriate action against the members involved. The report of the outcome of the investigation must

also specify the measures which the SAPS has taken to ensure that this incident or any incident of a similar nature does not recur. The report must be submitted to the Regulator within ninety (90) days of the date of receipt of this Enforcement Notice.

4) Include training on POPIA in all the training programmes provided to the members of the SAPS and submit a copy of this programme to the Regulator within one hundred and twenty (120) days of the date of receipt of this Enforcement Notice.
5) Submit to the Regulator the SAPS's Privacy Policy within ninety (90) days of the date of receipt of this Enforcement Notice.

D. Right of Appeal

The responsible party may appeal against this Enforcement Notice within thirty (30) days of the date of receipt of this Enforcement Notice as provided for in section 97(1) of POPIA.

E. CONSEQUENCES FOR NON-COMPLIANCE WITH AN ENFORCEMENT NOTICE

Please note that a responsible party which fails to comply with this Enforcement Notice is guilty of an offence and liable upon conviction to fine or to imprisonment for a period not exceeding ten (10) years or to both such a fine and such imprisonment.

DATED at **JOHANNESBURG** on this the **4th** day of **April** 2023

……

ADV. PANSY TLAKULA

CHAIRPERSON OF THE INFORMATION REGULATOR