INFORMATION REGULATOR (SOUTH AFRICA)
Ensuring protection of your personal information and effective access to information

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 462-22, CI 491-22, and CI 519-22

A	DETAILS OF DATA SUBJECT
Name(s) and surname/ registered name of data subject/complainant/aggrieved party:	[redacted]
Unique Identifier/ Identity Number	
Residential, postal or business address:	Code ()
Contact number(s):	
Fax number E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	Central Johannesburg TVET College
Residential, postal or business address:	Code ( )
Contact number(s):	[redacted]
Fax number/ E-mail address:	[redacted]

A. Be pleased to take notice that the Information Regulator (Regulator) after having considered the report of the Enforcement Committee hereby decides that the Central Johannesburg TVET College (*"Responsible Party")* has interfered with the protection of personal information of the data subjects 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. REASONS FOR THE FINDINGS

1. The Responsible Party has breached the following conditions for the lawful processing of personal information:

1.1 Condition 1: Accountability - section 8 of the Protection of Personal Information Act 4 of 2013 *("POPIA")*

1.1.1. The Responsible Party must ensure that the conditions for the lawful processing of personal information set out in Chapter 3 POPIA and all the measures that give effect to such conditions are complied with and must demonstrate compliance with such conditions.

1.1.2. The Responsible Party **does not comply** with the condition of accountability by failing to register the Information Officer with the Regulator and to designate deputy information officer(s) and register them with the Regulator. The Information Officer is responsible for ensuring compliance with POPIA. The Responsible Party has failed to comply with some of the conditions for the lawful processing of personal information as illustrated hereunder.

1.2. Condition 4: Further Processing limitation- section 15 of POPIA.

1.2.1. Section 15 (1) of POPIA provides that further processing of personal information must be compatible with the purpose for which personal information was collected in terms of section 13. Section 15 (2) details the factors that must be considered to assess whether further processing of personal information is compatible with the purpose for which the information was collected.

1.2.2. According to the Responsible Party, it processed personal information of the complainants, [redacted] in the context of the employer-employee relationship to restore good governance after it had come to its attention that a sizeable number of employees had failed to declare their criminal records and possible conflict of interest such as doing business with the employer. As a result, the responsible party was placed under administration to investigate and address these problems.

1.2.3. The terms of reference of the Administrator included the restoration of good governance and ensuring that all employees declared their previous criminal records and interests. He also had to review and develop policies where there was a gap. The Acting Chief Financial Officer was tasked with the responsibility of reviewing, developing and implementing Finance Policies.

1.2.4. The personal information of the complainants was collected for the purpose of the verification of their academic qualifications and criminal records. This was done through the issuing of the Personal Credential Verification Report (Verification Report) by a company called the [redacted]

1.2.5. By his own admission, the Administrator of the Responsible Party confirmed that in the course of communicating with her team the urgent need to implement the policies, the Acting Chief Financial Officer had erroneously included the Verification Reports of the complainants in the folder that contained finance policies and this information was sent by email to various employees by email.

1.2.6. The complainants learnt about the email containing their personal information when it was sent to some staff members on 6 September 2022. This email was recalled by the Administrator on 8 September 2022 with an explanation that the document was erroneously distributed and was not intended for staff use. He even took corrective action against those who had erroneously sent the document to other staff members.

1.2.7. The sharing of the Verification Reports of the complainants with other staff of the responsible party constitutes further processing. In terms of section 15 (1) of POPIA, further processing (sharing) of personal information, in this instance the Verification Report of the complainants, must be in accordance or compatible with the purpose for which the personal information was collected. The Verification Reports were collected for the purpose of strengthening governance within the institution.

1.2.8. The sharing of these reports with other employees who were not involved in the strengthening of governance of the institution, albeit by mistake, was incompatible with the purpose for which the personal information in the Verification Reports was collected. The

contention of the Responsible Party that the complainants were not part of the recipients of the email communication mistakenly issued by the Acting CFO and that their possession of the email contravened the Electronic Communication Policy and Transmission Policy of the institution is not relevant and cannot be used as a justification for non-compliance with POPIA.

1.2.9. Section 15 (3) of POPIA provides for the legal bases for further processing of personal information. One of these bases is consent. The Responsible Party did not obtain the consent of the complainants for the further processing of their personal information. In addition to this, none of the other legal bases for further processing provided for in section 15 (3) of POPIA are applicable.

1.2.10. The Regulator finds that the Responsible Party has contravened section 15 (1) of POPIA. The Regulator disagrees with the Enforcement Committee's finding that the CJC "has not contravened section 15 (1) by further processing the personal information of the data subjects, in that further processing of personal information is compatible with the purpose of collection, in that the personal information was processed for a legitimate purpose and is in the public interest". Section 15 (3) of POPIA provides instances in which further processing is compatible with the purpose of collection. "Legitimate purpose and public interest" are not mentioned in section 15 (3).

1.3. Condition 7: Security Safeguards - Sections 19 and 22 of POPIA

1.3.1. Section 19 (1) (b) of POPIA provides that the Responsible Party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent unlawful access to or processing of personal information.

1.3.2. Although there is no evidence that documents such as personal information policies, procedures and frameworks, security safeguards to control access to personal information, evidence of the training of staff in POPIA were requested during the investigation, failure by the Responsible Party to keep separate files for the complainant's Verification Reports containing their personal information and the financial policies, coupled with failure to register the

Information Officer with the Regulator, points to the absence of organisational measures to prevent unlawful access or processing of personal information, leading to the personal information of complainants being shared and eventually unlawfully accessed by unauthorised parties.

The Regulator finds that the Responsible Party violated section 19 (1) of POPIA.

1.3.3. Section 22 of POPIA sets out the duties and obligation of the Responsible Party where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person. In such a case, the Responsible Party must inform the Regulator and the data subject affected of the security compromise.

1.3.4. It is common cause that the personal information of the complainants contained in the Verification Report was shared with other employees of the Responsible Party who were not authorised to access this information. This constituted a security compromise, which triggered the obligation of the Responsible Party to inform the Regulator and the complainant of the security compromise. Neither the Regulator nor the complainants were informed of the security compromise.

1.3.5. Although, an email was issued to all employees to alert them to the fact that personal information of the complainants was shared by mistake, that an investigation was launched to understand the circumstances under which the error occurred and that corrective action was taken, this did not absolve the Responsible Party from its obligation to inform the Regulator and the complainant of the security compromise.

In the premise, the Regulator finds that the responsible party has violated section 22 (1) of POPIA.

2. Condition 2: Processing Limitation- section 11 of POPIA

2.1. Section 11 (1) of POPIA provides that personal information may only be processed with the consent of a data subject or a competent person if the data subject is a child. As stated above, the institution was placed under administration to address governance failures. To this end, the Responsible Party decided to verify the qualifications of all employees, who were also required to declare all their interests. This was done through the collection of the personal information of the complainants using the Personal Confidential Verification Report. It was not necessary for the Responsible Party to obtain the consent of the complainant to process their personal information for the purpose of the verification of their qualifications and criminal records. The Responsible Party had a lawful basis for such processing, namely the pursuance of its legitimate interest. The Regulator could not find any complaint regarding the violation of section 11 of POPIA. However, since the Enforcement Committee dealt with this section in its report, the Regulator concurs with the Committee that the Responsible Party did not violate section 11 (1) of POPIA.

3. Prohibition on processing of special personal information -Section 26 (b) of POPIA

3.1. Section 26 (b) of POPIA prohibits the processing of personal information of a data subject concerning the criminal behaviour of a data subject if such information relates *inter alia,* to the alleged commission of any offence by a data subject.

3.2. The complainants had alleged that the Responsible Party had processed their special personal information without their consent and knowledge. However, upon the perusal of the MIE report of one of the complainants, [redacted] whose MIE Report was the only one which was in the Investigation Report submitted by the POPIA Division, the Enforcement Committee found that the report did not contain any special personal information, and contained information such as his name, identity number, date of birth and contact number. According to the Enforcement Committee, the MIE reports of the other two complainants, [redacted] were not included in the Investigation Report.

3.3. The Regulator concurs with the Enforcement Committee that the MIE Report of [redacted] did not contain any special personal information and therefore the responsible party did not violate section 26 (b) of POPIA.

C. RECOMMENDATIONS

4. Based on the above-mentioned Findings, the Regulator orders the Responsible Party to take the following actions –

4.1 The Responsible Party must provide confirmation to the Regulator that:

4.1.1 It has registered the Information Officer with the Regulator as stipulated in section 55 (2) of POPIA and provide the Regulator with proof of registration within 31 days of the date of receipt of this Enforcement Notice.

4.1.2 It has designated deputy information officer(s) and registered them with the Regulator and provide proof the Regulator with proof of this within 31 days of the date of receipt of this Enforcement Notice.

4.2 The Responsible Party must notify the Regulator and the data subjects of the security compromise of their personal information in compliance with section 22 of POPIA and provide proof thereof within 31 days of the date of receipt of this Enforcement Notice.

4.3 The Responsible Party must submit a written apology to the complainants for processing their personal information in a manner that breached the conditions for the processing of personal information stipulated in this Enforcement Notice. The apology must also be sent by email to all the employees of the responsible party and must be published through all other communication channels used by the Responsible Party. The apology must not contain the personal information of the complainants, other than their names and surnames. Proof of the written apology and the publication thereof as directed above must be submitted to the Regulator within 31 days of the date of receipt of this Enforcement Notice.

4.4 The Responsible Party must take appropriate action against the employee who had unlawfully processed (shared) personal information of the complainants and submit proof thereof to the Regulator within 60 days of the date of receipt of this Enforcement Notice.

4.5 The Responsible Party must submit its POPIA Compliance Framework to the Regulator within 31 days of the date of receipt of this Enforcement Notice. The Framework should include the following: the Privacy Policy, the Retention Policy and Schedule, the Incident Response Policy and the Information Privacy and Security Policy.

4.6 In the event that the Compliance Framework has not been developed, the Responsible Party must develop same and submit a copy thereof to the Regulator within 120 days of receipt of this Enforcement Notice.

4.7 The Responsible Party must conduct internal public awareness and training programmes on POPIA for all the employees of the Responsible Party. Copies of these programmes and proof that they have been conducted (e.g. attendance register of the participants) must be submitted to the Regulator within 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 31 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 ENFORCEMENT NOTICE

Please note that the 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 10 years or to both a fine and imprisonment.

DATED at **JOHANNESBURG** on **22 May 2026**

.....

ADV. PANSY TLAKULA

CHAIRPERSON OF THE INFORMATION REGULATOR