**MEDIA STATEMENT**

**THE REGULATOR ACTS ON ALLEGED SECURITY COMPROMISE INCIDENT SUFFERED BY THE DEPARTMENT OF BASIC EDUCATION REGARDING MATRIC RESULTS**

**13 JANUARY 2025**

On Sunday, 12 January 2025, the Information Regulator (Regulator) became aware of social media posts alleging that matric results were being made available to the public, ahead of the official release of the results by the Minister of Basic Education, upon payment of a fee of R100 to a private website (name withheld). The Regulator is concerned that the personal information of data subjects may have been unlawfully accessed and compromised. Therefore, the Regulator wrote to the Department of Basic Education (DBE) to request confirmation of the incident as reported in social media posts and provide it with more information regarding the alleged security compromise incident (see Annexure 1). In light of the urgency of this matter, the Regulator required the DBE to provide it with the requested information by the end of business on Tuesday 14 January 2025.

On Monday, 13 January 2025, the Regulator became aware of a public announcement by the Minister of Basic Education that there was a “breach of the (DBE’s) information” through the leaking of the matric results on a private website.

The Regulator cannot yet address the specifics of the recent allegations of a security compromise on personal information of learners held by the DBE until the DBE has fulfilled its obligations under Section 22 of the Protection of Personal Information Act 4 of 2013 (POPIA). Section 22 of POPIA states that when a responsible party has suffered a security compromise, the public or private body must notify the Regulator within a reasonable time. Section 22 also requires that the responsible party, such as the DBE, should notify both the Regulator and data subject(s) of the security compromise that it has suffered. The Regulator has not yet received such a notification from the DBE.

Any unlawful access to, and usage of, personal information of data subjects is treated with extreme seriousness and concern by the Regulator. The security compromise of learners' personal information under the custody of the DBE is no different.

**For media enquiries or interviews contact Mukelani Dimba on 083 525 2361 / mdimba@inforegulator.org.za or Tshegofatso Letshwiti on 083 702 7833 / tletshwiti@inforegulator.org.za**

**ISSUED BY THE INFORMATION REGULATOR OF SOUTH AFRICA.**

## ANNEXURE 1: INFORMATION REQUESTED BY THE REGULATOR FROM THE DBE

1. Confirmation and subsequent reporting of the security compromise as is required by section 22 of POPIA.
2. Details of the provision of sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise including:
3. a description of the possible consequences of the security compromise.
   - 3.1 the measures to be taken by responsible party to mitigate the possible adverse effects of the security compromise.
   - 3.2 the measures advised by the responsible party to the data subjects to mitigate the effects of the security compromise.
   - 3.3 if known to the responsible party, the identity of the unauthorised person(s) who may have accessed or acquired the personal information.
4. Whether all the affected data subjects (if any) have been advised of the security compromise. If so, when and how?
5. Details as to the specific types of personal information of data subjects that has been unlawfully accessed.
6. Details as to the number and/or nature of the persons to whom the personal information of data subjects may have been disseminated by the unauthorised person.
7. Whether an internal or external investigation into the compromise has been initiated; If so, provide the Regulator with an update of such investigation.
8. Whether the affected data subjects have been updated on the progress into the investigation by the responsible party. If so, when and how?
9. Whether or not there have been any complaints lodged by data subjects in respect of the security compromise.
10. Details as to the manner of unlawful access to and/or unlawful processing of personal information by the unauthorised person.
11. The consequences of the security compromise for the responsible party.
12. The incident response proceedings during the incident until resolution.
13. Details as to the technical and organisational measures that the responsible party has implemented to mitigate against the affected data subjects' personal information being unlawfully accessed and/or unlawfully processed.
14. Details as to the law enforcement and other government agencies that the responsible party is engaging with or has engage in respect of the security compromise(s).