COMPLIANCE WITH THE PROTECTION OF PERSONAL INFORMATION ACT – LESSONS FROM TRANSUNION

Category: Privacy Law and POPIA,Privacy Law, Infosec, and POPIA
written by Tshepiso Hadebe | September 5, 2022

Introduction

On the 26th of March 2022, TransUnion South Africa issued a statement stating that it was the target of a cyber-attack. The credit bureau expressed that based on its investigations to date, it believes that the incident impacted an isolated server holding information from TransUnion South Africa. TransUnion further confirmed that to date that at least 3 million consumers have been impacted.

Notification of security compromises requirements under Protection of Personal Information Act ("POPIA")

Section 22 of the POPIA deals with notifications of security compromises. Section 22 (5) states that the notification provided must contain sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise.

Section 22 further lists the information that must be included in the notice to the data subjects. This includes:

a. a description of the possible consequences of the security compromise;
b. a description of the measures that the responsible party intends to take or has taken to address the security compromise;
c. a recommendation with regard to the measures to be taken by the data subject to mitigate the

possible adverse effects of the security compromise; and

d. if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

Section 22 (6) gives the Information Regulator of South Africa ("**Regulator**") the power to direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

The Information Regulator and TransUnion

The Regulator issued a media statement expressing dissatisfaction with TransUnion's response and expressing its intention to initiate an assessment into the security compromise.

According to the media statement issued by the Regulator on 25 March 2022, it is dissatisfied with the security compromise notification submitted by TransUnion after it called on it to explain the circumstances of the security compromise. The Regulator stated that the notification submitted by the TransUnion fell short of what is required in terms of POPIA.

The Regulator stated that the notification lacked sufficient details or a description of the remedies available to the data subjects. In addition, it omitted critical information to provide assurance on how the matter was managed. As a result, the notice fell short of the standards set out in POPIA. Furthermore, the notification did not provide any detail on how the credit bureau will mitigate subsequent risks nor information on how TransUnion will remedy the crisis.

The Regulator has now instructed TransUnion to provide it with a detailed description of the possible consequences of the security compromise and its impact on data subjects. TransUnion is also required to provide the Regulator with advice and recommendations on the measures to be taken by the data subjects to mitigate the potential adverse effects of the security compromise. Furthermore, TransUnion must provide the Regulator with measures that it intends to take, or it has taken to address the security compromise.

Given the nature of the security compromise, the Regulator has directed TransUnion to, in addition to the means of notification that it has employed, use radio stations that broadcast in each official language and publish the notification in newspapers. In addition, TransUnion must drive communication on various social media platforms to provide sufficient notification to data subjects about this security compromise.

Moreover, the Regulator has advised that after the careful assessment of the contents of TransUnion's security compromise notification and the extent and severity of the security compromise, it will conduct an assessment on its own initiative into the appropriateness of TransUnion's security measures on integrity and confidentiality of personal information of data subjects in its possession or under its control.

Conclusion

A lesson for responsible parties and operators alike is the importance of compliance with POPIA provisions. This includes compliance with procedures for notification of security compromises and to take extra precaution in ensuring that the notifications meet all the requirements set out in POPIA. Where there is failure to do so, severe consequences might result. In addition, they should endeavour to regularly review their compliance with POPIA as TransUnion is a lesson on the high standard adopted by the Regulator in its approach to non-compliance with POPIA.

Contact us for more good, clear, precise advice.