



**INFORMATION
REGULATOR
(SOUTH AFRICA)**

*Ensuring protection of your personal information
and effective access to information*

Address: 316 Thabo Sehume Street
Tel: 012 406 4818
Fax: 0865003351
E-mail: infoereg@justice.gov.za

MEDIA STATEMENT

ALLEGED CAMBRIDGE ANALYTICAL DATA BREACH - FACEBOOK

The Information Regulator (Regulator) has noted various media reports which allege a material data breach by Facebook. The spokesperson of Facebook is reported to have said that the data of 59 777 of South Africans users was potentially shared with the data firm called Cambridge Analytica.

Although not all the sections of the Protection of Personal Information Act No. 4 of 2013 (POPIA) have come into effect, the Regulator has decided to proactively and voluntarily engage Facebook with regards to the alleged data breach.

In this regard the Regulator has written to Facebook to establish amongst others:

1. if the alleged data breach indeed occurred and how the alleged breach occurred;
2. the extent and materiality of the alleged data breach;
3. interim measures put in place by Facebook to prevent further compromise;
4. security measure that Facebook has put in place to prevent a recurrence of such an alleged breach; and
5. an undertaking by Facebook to inform affected data subjects of the breach to allow these data subjects to take proactive measures against potential consequences of the compromise.

In terms of Section 19 of POPIA Facebook must:

1. Put in place measures to 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:–
 - 1.1 either loss of, damage to or unauthorised destruction of personal information or
 - 1.2 unlawful access to or processing of personal information.
2. Ensure that the aforementioned is achieved by taking reasonable measures to: –
 - 2.1 identify all reasonably foreseeable internal and external risks to personal information in its possession or under its controls;
 - 2.2 establish and maintain appropriate safeguards against the risks identified;
 - 2.3 regularly verify that its safeguards are effectively implemented; and
 - 2.4 ensure that safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
3. Have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and standards.

It is the Regulator's view that Facebook must remove all personal information of inactive and dormant account users who have deactivated their accounts.

The alleged Facebook data breach follows the data breach which occurred in mid-October 2017 in which it was reported that 27.2 GB database file name: “masterdeeds” compromised on the Go Vault platform operated by Dracore.

Following these reports the Regulator wrote to all the parties that were implicated in the alleged breach and subsequently convened a meeting of various government institutions involved in the investigation of the alleged material data breach. These institutions include the South African Police Service specifically the HAWKS, the National Prosecuting Authority (NPA), Department of Rural Development, the National Credit Regulator and the Association of Credit Bureaus. The meeting agreed to establish a Task Team comprising of the representatives of the above mentioned institutions to ensure a multi-disciplinary approach to the investigation.

Any person affected (either personally or acting on behalf of affected party) as a result of the alleged data breach at Facebook is welcome to lay a formal complaint with the Regulator through its website: www.inforeg.gov.za

The Regulator remains committed to resolve any data breach.

ISSUED BY THE CHAIRPERSON OF THE INFORMATION REGULATOR



ADVOCATE PANSY TLAKULA

10 APRIL 2018