WERKSMANS
ATTORNEYS

REGULATORY

The Facebook data breach – #thisisyourdigitallife

6 June 2018 *5 min read*

by Ahmore Burger-Smidt, Head of Data Privacy Practice

WHAT MESSAGE DOES THE FACEBOOK DATA BREACH HOLD FOR SOUTH AFRICA AS A SOCIETY AND THE BUSINESS COMMUNITY IN GENERAL?

The millions of Facebook profiles analysed by Cambridge Analytica constitute one of the biggest breaches of personal information to date. The data was collected through an application accessed by Facebook users in terms of which these users agreed to have their data collected for academic use. What was also collected by the application was information from the Facebook users' friends.

Facebook has acknowledged that more than 87 million of the 2.2 billion Facebook users' personal information may have been shared with Cambridge Analytica. It is estimated that almost 93 000 South African Facebook users' personal information could potentially have been shared with Cambridge Analytica.

The question to consider is, to what extent Facebook users and businesses in South Africa are aware of the impact of the Protection of Personal Information Act, 2013 ("**POPIA**") on their daily actions and interactions.

The Preamble to POPIA clearly sets out the aims and objectives of the Act, which are to protect personal information processed by public and private bodies and to introduce certain conditions detailing the minimum requirements for the processing of personal information.

The establishment of minimum requirements for the lawful processing of personal information requires all responsible parties (the parties responsible for the processing of information) to comply with conditions 1 to 8 of POPIA.

The definition of processing personal information as set out in POPIA, clearly shows that information sent or received by a user of social media is subject to the statutory provisions of POPIA.[1] This means that:

- the collection, receipt, recording, organisation and other methods of processing set out in section 1 of the POPIA, must be in compliance with the provisions of the Act;
- personal information must be lawfully processed in a reasonable manner that does not infringe the privacy of the data subject (the person to whom the data relates);
- personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive;
- the requirement of consent. This is probably the most important question regarding the lawfulness of processing – whether the data subject has consented to the processing of his, her or its personal information;
- the personal information must be collected directly from the data subject;
- personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party;
- the further processing of personal information must be in accordance or compatible with the purpose for which it was collected;
- a responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated, where necessary;
- the notification of the collection of personal information must be communicated to the data subject; and

- the responsible party must comply with certain security safeguards.

The requirements for the lawful processing of personal information set out in conditions 1 to 8, apply to social media users and Facebook as a social network. It also applies to public and private entities that process information.

In other words, when processing personal information of individuals, Facebook is a responsible party in terms of POPIA. This means that Facebook may only collect/receive the personal information of its users if all the requirements for the lawful processing of personal information have been complied with. Also, it will be deemed problematic in instances where Facebook forwards the personal information to third parties, without the consent of the user. POPIA expressly excludes the transfer of personal information about a data subject to a third party who is in a foreign country, unless the recipient of the information is subject to an adequate level of protection which effectively upholds the principles of reasonable processing of information that are substantially similar to the South African conditions for lawful processing.

However, POPIA has not been fully enacted as yet. This will only happen once promulgated by the President. The Information Regulator issued draft Regulations during the latter part of 2017 and it is anticipated that the final Regulations will be published over the next few months. Despite this vacuum, the Information Regulator proactively and voluntarily engaged with Facebook with regards to the alleged data breach, and Facebook has responded with answers to the questions posed.

This however does not mean that companies can ignore POPIA. Companies should review their business operations and determine and understand the applicable legal obligations in terms of POPIA. In addition, the EU General Data Protection Regulation ("GDPR") comes into force on 25 May 2018, and will have implications for South African companies in many instances. The GDPR places onerous accountability obligations on companies processing information.

Facebook is a warning to all. Now is the time to fully unpack POPIA and understand your rights, obligations and duties. Not only as far as it relates to South Africa, but at least to Europe, if not the world.

---

[1] The definition of processing relates to the operation or activity or any set thereof, whether or not by automatic means, concerning personal information relating to the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; or the merging, linking, as well as restriction, degradation, erasure or destruction of information (section 1 of POPIA).



Ahmore Burger-Smidt

Head of Regulatory

View Profile