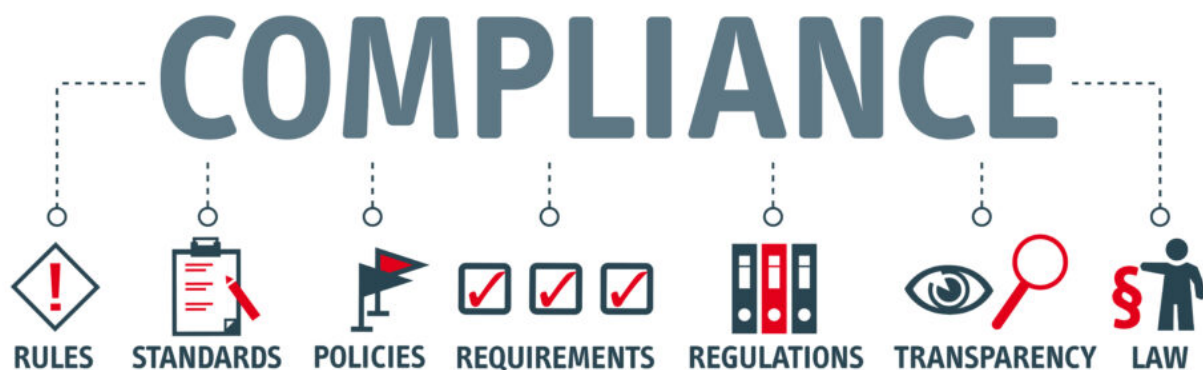


TIKTOK ON THE CLOCK OF DATA PRIVACY CONCERNS

Category: Privacy Law and POPIA, Privacy Law, Infosec, and POPIA
written by Tshegofatso Phahlamohlaka | November 28, 2023



Recently, TikTok has faced [bans](#) and restrictions in several countries across the world over data privacy and security concerns. In 2020, India declared a total ban on TikTok and other Chinese-owned applications over concerns relating to security. Similarly, the United States of America has implemented restrictions on the use of the application on government devices citing national security concerns over the Chinese government accessing user data.

The South African government has not yet subscribed to the global TikTok ban trend. Nevertheless, the issue of bans underlines the importance of addressing privacy and security concerns on social media platforms like TikTok. Some authors argued over imposing bans on TikTok because it does not remedy the privacy and security concerns and suggested that a different approach be adopted to address privacy and security concerns. Once such suggestion is that privacy and security legislation should more effectively be enforced on social media applications, especially as people rely on these platforms to communicate, connect, and share information.

TikTok, like all other social media platforms, is required to comply with data privacy and data protection laws in the countries in which it operates in. In South Africa, the responsible party being TikTok is required to comply with the provisions of the *Protection of Personal Information Act 4 of 2013* ("**POPIA**"). POPIA guards against the unlawful processing of individuals' data and gives individuals control over the collection and processing of their data. POPIA essentially protects users' data and provides for lawful processing of personal information. Against this backdrop, TikTok is required to ensure that it collects, processes, and protects its users' information in accordance with POPIA to avoid regulatory fines or legal proceedings. Additionally, as a responsible party, it is required to align its privacy policy and procedures to the requirements of POPIA.

TikTok requires that users provide personal information such as their name and email address to create an account. It allows users to create content in a form of short videos and share them on the platform. Based on a user's past interaction, TikTok creates and shows a personalised feed of videos and allows users to like, comment or share the videos, and follow other users on the platform.

In light of the fact that TikTok collects, stores, and uses users' information it must ensure that its users have control over how their data is processed. This can be achieved by adding features or functionalities which allows users to choose the types of data they are willing to share or how long they want their data to be stored on TikTok, especially where the information is not strictly required for the functionality of the application. An example of this is introducing options for data retention or control over user's locations. It is also important that TikTok provides clear and user-friendly consent

notifications, for example for information that is used for the purposes of marketing. POPIA requires that consent must be a “voluntary, specific and informed expression of will”. It is important that users are well-informed and aware of the risks and implications of sharing their personal information online.

Ultimately, social media applications, like TikTok must ensure that they comply with POPIA. This should include implementing measures to protect personal information, granting users access and control over their data and being transparent on how it utilises data. This will not only ensure compliance with data privacy laws like POPIA but will also show TikTok’s commitment to protecting its users’ data and privacy.

[Contact us](#) for more good, clear, precise advice.