bizcommunity

TikTok, Meta fined hundreds of millions by EU regulators for data privacy breaches

In a landmark ruling, Ireland's Data Protection Commission (DPC) has fined TikTok €530m ($571m) for illegally transferring European users' data to China, marking one of the largest penalties under the EU's General Data Protection Regulation (GDPR). The decision reflects Europe's intensified focus on data protection.

By Ryszard Lisinski and Brett Weinberg 13 May 2025

Image source: raw pixel from Freepik

The violation

TikTok admitted in April 2025 that European user data was stored on Chinese servers, contradicting earlie statements to Irish regulators. This breach eroded trust and fuelled the DPC's decision.

Stated DPC Deputy Commissioner Graham Doyle:

> *"TikTok's personal data transfers to China infringed the GDPR because TikTok failed to verify, guarantee and demonstrate that the personal data of EEA users, remotely accessed by staff in China, was afforded a level of protection essentially equivalent to that guaranteed within the EU."*

The company neglected to assess risks posed by Chinese national security laws, which grant Chinese authorities broad data access.

Beyond the fine

The DPC has ordered TikTok to comply with GDPR within six months or face a potential suspension of da transfers to China, which could disrupt operations.

This case underscores tensions between global tech operations and regional privacy laws, particularly wh those operations span jurisdictions with fundamentally different approaches to privacy and governmental access to data.

China's legal framework

The ruling hinges on conflicts between EU data protection standards and Chinese legislation on anti-terrorism, counter-espionage, cybersecurity and national intelligence.

The aforementioned legislation mandates data access for state purposes, clashing with GDPR's requirement for "essentially equivalent" protection for EU data abroad. The DPC determined that TikTok failed to implement sufficient safeguards to ensure this equivalence when data was accessible from Chin

LEGISLATION & REGULATION

PoPIA, GDPR - or both?

Karl Blom and Ekene Nkado 30 Nov 2020

TikTok's track record

TikTok, owned by Beijing-based ByteDance, has faced ongoing scrutiny over their data practices. In 2022 admitted that Chinese employees could access European user data to conduct various platform checks.

Several governments have banned TikTok on government devices and some countries have threatened broader bans over security risks. However, the company has spent billions on the "Project Clover" initiative designed to safeguard European user data and operations.

TikTok's response

TikTok expressed disagreement and plans to appeal the ruling.

"This ruling risks setting a precedent with far-reaching consequences for companies and entire industries across Europe that operate on a global scale," stated a TikTok spokesperson.

The company emphasised that it has never provided European user data to the Chinese government and would refuse to do so if asked.

What's next?

The full decision will be published by the DPC in the coming weeks, providing additional insight into the specific violations and required remediation steps.

TikTok now faces crucial decisions about how to restructure its data flows while continuing to operate its global platform effectively.

For the millions of TikTok users across Europe, the decision represents a significant regulatory effort to protect their personal information, although the immediate impact on the user experience remains unclear.

As digital platforms increasingly operate across jurisdictional boundaries with conflicting legal requirement

the TikTok case may establish an important precedent for how data-driven companies navigate the compl global landscape of privacy regulations and national security interests.

CYBER LAW

Is ChatGPT yet another hurdle for data privacy?

Ahmore Burger-Smidt 1 Mar 2023

Meta fined €200m over "consent or pay" model

In another significant regulatory action, the European Commission fined Meta €200m for violating the Digit Markets Act (DMA) with its "consent or pay" advertising model.

The controversial model

Introduced in November 2023, Meta's "consent or pay" model required Facebook and Instagram users to either consent to their personal data being used for targeted advertising or, alternatively, pay for an ad-free experience.

The model was designed to comply with EU data protection regulations - amid mounting pressure from EU privacy authorities - while preserving Meta's ad-driven revenue, but was deemed non-compliant with DMA standards.

Commission's findings

The Commission found that Meta's model failed to offer users a service equivalent to personalised ads bu with less data usage. The DMA mandates explicit user consent for combining their data across services.

The European Commission held that Meta's model embodied a binary choice which did not allow for genuine user consent.

Meta's defense

Meta contested the ruling, arguing that it unfairly targets American tech companies.

"The European Commission is attempting to handicap successful American businesses while allowing Chinese and European companies to operate under different standards. This isn't just about a fine; the Commission forcing us to change our business model effectively imposes a multi-billion-dollar tariff on Me while requiring us to offer an inferior service," stated Joel Kaplan, Meta's chief global affairs officer.

The company further claimed that restrictions on personalised advertising would negatively impact Europe businesses and economies, suggesting broader economic consequences beyond just Meta's operations

PUBLISHING

Navigating PoPIA compliance: Lessons from the regulator's enforcement notices

Juta and Company 8 Oct 2024

Next steps

Meta now has 60 days to comply with the Commission's decision. Failure to make the required changes could result in additional penalties.

The company must develop an alternative approach that allows users more granular control over their data while still maintaining compliance with both the DMA and other EU privacy regulations.

Broader DMA enforcement

The action against Meta was not the only significant DMA enforcement announced recently. The Commission also imposed a €500m fine on Apple over app store-related issues, signalling the EU's commitment to enforcing the new digital regulations across major technology platforms.

Industry-wide implications

The TikTok and Meta rulings highlight the EU's resolve to enforce GDPR and DMA compliance, particularly on cross-border data transfers and user consent respectively.

In addition, following the invalidation of both the Safe Harbor and Privacy Shield frameworks for EU-US data transfers in recent years, companies have struggled to find legally sound mechanisms for cross-border data flows.

For TikTok, restructuring data flows is critical to avoid operational disruptions. Meta must develop a DMA-compliant model offering users granular data control. Both cases may influence how tech firms navigate privacy regulations worldwide.

Implications for South Africa: A warning under PoPIA

South African businesses and consumers should take particular note of these European developments, as the Protection of Personal Information Act (PoPIA) in South Africa is closely modelled on the EU's GDPR framework.

As European regulators escalate both the frequency and severity of penalties against tech companies, South Africa's Information Regulator may well follow suit.

PoPIA, which came into full effect in July 2021, grants the Information Regulator similar powers to impose substantial administrative fines of up to R10m for serious violations. While enforcement has been relatively measured during the initial implementation period, the regulatory landscape appears to be shifting toward stricter enforcement globally.

South African companies processing personal information should view these European cases as a clear warning sign. As the Information Regulator builds capacity and experience, businesses can expect increased scrutiny of their data handling practices, particularly regarding cross-border data transfers and obtaining proper user consent.

Organisations operating across multiple jurisdictions face particular challenges in navigating the complex international privacy landscape. Companies with connections to both European and South African markets must ensure compliance with both regulatory frameworks, as non-compliance in one jurisdiction may trigger investigations in others.

The time for South African businesses to review and strengthen their data protection practices is now, before local enforcement actions begin to mirror the substantial penalties being imposed in Europe.

ABOUT THE AUTHOR

Ryszard Lisinski - Director: Business Rescue & Insolvency, Litigation; Brett Weinberg - Senior Associate: Business Rescue & Insolvency, Litigation at Fluxmans