Data Protection Commission Reference: IN-18-08-3

In the matter of TikTok Technology Limited

Summary of Draft Decision of the Data Protection Commission

The Decision concerns an Inquiry by the Data Protection Commission (the '**DPC'**) into TikTok Technology Limited ('**TikTok'**), a data controller with its main establishment in Ireland. The DPC made the Decision on 30 April 2025 and it relates to an own volition statutory inquiry ('the **Inquiry'**) that the DPC commenced on 14 September 2021. The Inquiry examined TikTok's compliance with Articles 13(1)(f) and 46(1) GDPR regarding its transfers of EEA User Data to China.

The Transfers to China considered in the Inquiry

TikTok informed the Inquiry that it did not store EEA User Data on servers located in China. Rather, TikTok's position, until after the DPC submitted its draft decision to the GDPR cooperation mechanism, was that its transfers of EEA User Data to China consisted of remote access to that personal data by personnel of the ByteDance group of companies in China. Accordingly, the Decision considers whether those transfers by way of remote access complied with Chapter V of the GDPR. The temporal scope of the Inquiry related to the Data Transfers taking place from 29 July 2020 and ongoing until 17 May 2023, when the DPC set out its provisional findings to TikTok enabling it to exercise its right to be heard on those findings.

In April 2025, TikTok informed the DPC of an issue that it discovered that resulted in EEA User Data being stored on servers in China. TikTok informed the DPC that this had resulted in TikTok providing inaccurate information to the Inquiry. While the Decision relates to TikTok's transfers by way of remote access only, the Decision expressed the DPC's deep concern that TikTok had submitted inaccurate information to that inquiry. On 4 July 2025, the DPC commenced a separate own volition inquiry to consider the lawfulness of TikTok's transfers that resulted in EEA User Data being stored on servers in China.

Findings in the Decision

The Decision made the following findings, which are outlined below in further detail:

1. TikTok Ireland infringed Article 46(1) GDPR by carrying out the Data Transfers during the temporal scope while failing to verify, guarantee and demonstrate that that the personal data of EEA Users subject to the Data Transfers was afforded a level of protection essentially equivalent to that guaranteed within the European Union.

2. TikTok Ireland infringed Article 13(1)(f) GDPR from 29 July 2020 to 1 December 2022 by failing to provide data subjects with required information on the Data Transfers and information on how

the processing concerned remote access to personal data stored in Singapore and the United States by personnel based in China.

Finding 1: TikTok infringed Article 46(1) GDPR

The GDPR provides a high level of protection of personal data throughout the EEA and provides data protection rights to individuals. When personal data is transferred outside of the EEA this can impede the ability of individuals to exercise rights and can circumvent that high level of protection. Therefore, it is crucial that the level of protection ensured by the GDPR should not be undermined in the case of such transfers. Accordingly, transfers of personal data can take place only if the conditions laid down in Chapter V of the GDPR are complied with. This ensures that the high level of protection provided within the European Union continues where personal data is transferred to a third country.

Article 45(1) GDPR provides that a transfer of personal data to a third country may be authorised by a decision of the European Commission to the effect that the third country, a territory or one or more specified sectors within that third country, ensures an adequate level of protection (an **'Adequacy Decision'**). China has not been subject of an Adequacy Decision. TikTok's own assessment of Chinese law set out that there are aspects of the Chinese legal framework that preclude a finding of essential equivalence to EU law. In this regard, TikTok's assessment considered, amongst other things, Chinese laws such as the Anti-Terrorism Law, the Counter-Espionage Law, the Cybersecurity Law and the National Intelligence Law.

In the absence of an Adequacy Decision, Article 46 GDPR enables transfers of personal data to third countries if the data controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. On this basis, TikTok relied on Standard Contractual Clauses ("SCCs") and supplementary measures for its transfers of EEA User Data to China.

The CJEU's Schrems II judgment clarified that transfers made in reliance on SCCs must ensure a level of protection essentially equivalent to that which is guaranteed in the European Union. This judgment also held that the data controller or processor must verify that level of protection in light of the appropriate safeguards and supplementary measures, and that the data controller or processor must suspend or end the transfers if it cannot guarantee that level of protection.

Where data controllers or processors rely on Article 46 GDPR for transfers, such transfers are not subject to prior approval by data protection authorities, nor do they have the benefit of an adequacy decision adopted by the European Commission concluding that the third country ensures an adequate level of protection. Therefore, there is a responsibility on the data controller or processor to verify and guarantee that the personal data transferred is subject to a level of protection essentially equivalent to that which

is guaranteed in the European Union. A failure to comply with this obligation renders any subsequent transfers unlawful.

While TikTok acknowledged that aspects of the Chinese legal framework preclude a finding of essential equivalence to EU law, it contended that, by implementing supplementary measures to provide for the transfers to be implemented by way of secure remote authorised access, it ensured the effectiveness of the SCCs, and afforded EEA User Data a level of protection essentially equivalent to that guaranteed within the European Union. TikTok emphasised its assessment of the territoriality principle in Chinese law and its conclusion that Chinese authorities are not lawfully entitled to compel organisations and individuals in China to provide data that are not domestically stored within the territory of China. However, the remote access by employees of the China Group Entities resulted in processing of EEA User Data on computer information systems in China.

The Decision finds that TikTok's transfers to China infringed Article 46(1) GDPR because it failed to verify, guarantee and demonstrate that the supplementary measures and the SCCs were effective to ensure that the personal data of EEA users was afforded a level of protection essentially equivalent to that guaranteed within the EU. In particular, the DPC found that TikTok's failure to adequately assess the level of protection provided by Chinese law and practices to the personal data of EEA users the subject of transfers, which said personal data is processed in China, not only directly impacted TikTok's ability to select appropriate safeguards and supplementary measures, but also prevented TikTok from verifying and guaranteeing an essentially equivalent level of protection.

Finding 2: TikTok infringed Article 13(1)(f) GDPR

Article 13(1)(f) GDPR requires data controllers to provide data subjects with information on that controller's transfers of personal data to a third country. The DPC considered TikTok's October 2021 EEA Privacy Policy and found that this policy was inadequate in two key respects for the purposes of Article 13(1)(f) GDPR.

First, the 2021 Privacy Policy did not name the third countries, including China, to which personal data was transferred. Second, the 2021 Privacy Policy did not explain the nature of the processing operations that constitute the transfer. Specifically, the 2021 Privacy Policy failed to specify that the processing included remote access to personal data stored in Singapore and the United States by personnel based in China.

TikTok updated its Privacy Policy during the course of the Inquiry and provided its December 2022 EEA Privacy Policy to the DPC. That Privacy Policy did identify the third countries to which EEA user data was transferred. That Privacy Policy also informed EEA Users that personal data was stored on servers in the United States and Singapore, and was the subject of remote access by entities in TikTok's corporate group located in Brazil, China, Malaysia, Philippines, Singapore, and the United States.

The DPC assessed TikTok's December 2022 EEA Privacy Policy as compliant with the requirements of Article 13(1)(f) GDPR in terms of the Data Transfers subject to the material scope of the Decision. Therefore, the duration of the infringement of Article 13(1)(f) GDPR in the Decision relates to the period from 29 July 2020 to 1 December 2022.

Summary of Findings

No	Article of the GDPR	Findings
1	46(1)	The DPC found that TikTok infringed Article 46(1) GDPR during the temporal scope of the Inquiry by carrying out the Data Transfers while failing to verify, guarantee and demonstrate that that the personal data of EEA users subject to the Data Transfers was afforded a level of protection essentially equivalent to that guaranteed within the European Union.
2	13(1)(f)	The DPC found that TikTok infringed Article 13(1)(f) GDPR from 29 July 2020 to 1 December 2022 by failing to provide data subjects with required information on the Data Transfers and information on how the processing concerned remote access to personal data stored in Singapore and the United States by personnel based in China.

Corrective Measures

Where the DPC makes a decision under Section 111(1)(a) of the Act, it must also make a decision under Section 111(2) as to whether a corrective power should be exercised in respect of the controller or processor concerned, and if so, the corrective power to be exercised.

Having considered the infringements of the GDPR as set out above, the DPC decided to exercise the following corrective powers, in accordance with Article 58(2) GDPR:

- An order pursuant to Article 58(2)(j) GDPR requiring TikTok Ireland to suspend the Data Transfers.

- An order pursuant to Article 58(2)(d) GDPR requiring TikTok Ireland to bring the processing into compliance. This requires TikTok to ensure that any EEA User Data located in China, as a result of the Remote Access Solution, when the order takes effect must cease being processed in China immediately at that point in time.

- Two administrative fines pursuant to Article 58(2)(i) GDPR as follows:
    i. In respect of TikTok's infringement of Article 46(1) GDPR, a fine of €485million.
    ii. In respect of TikTok's infringement of Article 13(1)(f) GDPR, a fine of €45million.

In deciding to impose two administrative fines totalling €530 million, the DPC gave due regard to the factors set out in Article 83(2) GDPR. The DPC also considered that administrative fines totalling €530 million met the requirements set out in Article 83(1) GDPR of being effective, proportionate and dissuasive.

Prior to its adoption, the DPC submitted a draft of its decision to the Concerned Supervisory Authorities in February 2025, as required under Article 60(3) of the GDPR. The Concerned Supervisory Authorities did not raise any objections (for the purpose of Article 60(4) GDPR) to the draft decision.