What does the recent TikTok Ireland penalty tell us about Europe-World data transfers?

The business world is shaken by the Irish Data Protection Commission's (**DPC**) €530m penalty decision (published in October 2025) imposed on TikTok for unlawful data transfers, following an inquiry initiated by the DPC in 2021.[1] The logic behind the strict rules is that "*When personal data is transferred outside of the EEA this can impede the ability of natural persons to exercise data protection rights and can circumvent that high level of protection.*" Under Article 46 of the General Data Protection Regulation (**GDPR**),[2] if EEA personal data travels, the GDPR must travel with it.

Background

Prior to the TikTok decision, the legal position about European data transfers had been clarified in the 2023 €1.2bn penalty decision against Meta Platforms Ireland Limited[3] and the "Schrems II"[4] and "Schrems I"[5] decisions. Each Schrems decision invalidated a US-EU "adequacy decision". The third successor US adequacy decision is now also subject to legal challenge.[6]

Data transfers are lawful if the country of the recipient benefits from an "adequacy decision" from the European Commission. This only applies to 15 countries and the remaining 180 countries of the world including China must rely on alternative data transfer mechanisms under the GDPR, such as the Commission's standard contractual clauses (**SCCs**). The SCCs must be agreed between the EEA data exporter and the overseas data importer. However, even the new SCCs released in 2021 will not by themselves be enough to render a data transfer lawful.

In Schrems II, the Court of Justice of the European Union (**CJEU**) clarified that cross-border transfers of personal data outside the European Union will be lawful only if data subjects are afforded a level of protection essentially equivalent to that guaranteed by the GDPR and EU Charter of Fundamental Rights of the European Union, even if the parties enter into the SCCs. However, this is often hard to guarantee if the overseas data importer is subject to "problematic" local laws that enable unrestricted

[1] DPC Case Reference: IN-21-9-2 In the matter of TikTok Technology Limited (link).
[2] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (link).
[3] DPC Inquiry Reference: IN-20-8-1 In the matter of Meta Platforms Ireland Limited (previously known as Facebook Ireland Limited).
[4] *Case C-311/18 Facebook Ireland v Schrems* EU:C:2020:559 (link).
[5] *Case C-362/14 Schrems v DPC* EU:C:2015:650 (link).
[6] *Case C-703/25 P Latombe v Commission*.

government data access powers. If because of such powers the data importer cannot substantially comply with the SCCs, the data transfer will not be lawful under the GDPR.

Where does this leave international trade in digital services? Is all such trade in Europe subject to the European Commission's binary decision that a certain country's legal system is adequate or not?

Facts of the TikTok Ireland decision

During a previous inquiry the DPC learned that TikTok allowed ByteDance companies in China including Beijing Zitiao Network Technology Co. remote access to EEA data stored on servers in the United States, Singapore and Malaysia. Such remote access constitutes a "data transfer" under the GDPR.

The ByteDance companies required access to the EEA data for a wide range of essential activities, such as trust-and-safety, operations, monetisation, payments and information security. ByteDance staff had access to user account information, device information, behaviour logs, transaction information, etc. The DPC considered these transfers were systematic, repetitive and continuous, which meant that TikTok could not rely on any of the exemptions for incidental transfers under the GDPR.

TikTok asserted that no EEA data was actually stored on Chinese servers. However, TikTok failed to appreciate that remote access often creates temporary copies of data on local machines in China. The decision suggests that TikTok was ill-prepared, did not understand its own facts, misconstrued the law, caused delays and provided inaccurate information to the DPC.

Unfortunately for TikTok, this penalty is not the end of the story. In 2025 it transpired that, contrary to TikTok's narrative, some EEA data had been stored on Chinese servers. This may attract another penalty in future.

Decision

The DPC found that TikTok breached:

- Article 46(1) GDPR which requires that personal data remains subject to a level of protection essentially equivalent to that guaranteed within the European Union.
- Article 13(1)(f) GDPR by failing to tell users about remote access by personnel based in China.

Essentially, despite its substantial submissions about Chinese law and essential equivalence, TikTok relied on hypothetical interpretation of the law without firm conclusions about how Chinese law could affect the EEA data in practice. TikTok's

submissions focused on how Chinese law applied to EEA data located outside China and "*TikTok Ireland chose not to address the issue of EEA User Data in China*". Because of this, TikTok could not guarantee that law and practice in China did not undermine the effectiveness of the SCCs and TikTok's supplementary measures.

Essential equivalence

The GDPR required TikTok to comprehensively assess the law and practices of China and verify whether appropriate safeguards and supplementary measures are capable of providing an essentially equivalent level of protection.

The DPC introduced the Milieu report[7] of the legal system in China but it gave preference to the evidence presented by TikTok including two reports from Professor Ke Xu, advice from law firm Fangda Partners, a report from Professor Prateek Mittal and an anonymous statement produced by Clifford Chance in China. Unfortunately, all this evidence wrongly focused on how Chinese law applied to EEA data located outside China, thereby entirely missing the point.

TikTok acknowledged that Chinese authorities had broad undefined investigative and surveillance powers. However, it argued that Chinese authorities are not lawfully entitled to compel organisations in China to provide access to data stored outside China, as doing so would breach the "principle of sovereignty". TikTok submitted evidence that Chinese entities are unaware of cases of disclosure of data held abroad compelled by Chinese authorities. However, TikTok failed to address how Chinese law applied to EEA data temporarily stored on local devices in China. Further, the DPC questioned whether the "territoriality principle" under Chinese law would be interpreted in such a restrictive way in practice, and TikTok continually failed to present relevant and authoritative evidence.

Chinese law seems to lack clarity about limitations of power. By contrast, the 2023 Meta decision highlighted the (at the time) "very clear inadequacies in US law" consisting of explicit broad powers of US agencies under section 702 of the Foreign Intelligence Surveillance Act (FISA),[8] EO 12333[9] and PPD-28[10] to gather "*foreign intelligence*".

The DPC was not satisfied that controls on surveillance powers under Chinese law were prescriptive and clear enough. There was no approval by a judge or other independent

[7] Government access to data in third countries, EDPS/2019/02-13 (link).
[8] According to the Meta decision, the US Foreign Intelligence Surveillance Act, 1978 allowed the Attorney General and the Director of National Intelligence to authorise jointly, following FISC approval, the surveillance of individuals who are not US citizens located outside the US in order to obtain *"foreign intelligence information",* and provides, inter alia, the basis for the PRISM and UPSTREAM surveillance programmes.
[9] According to the Meta decision, the US Executive Order 12333 allowed the NSA to access data "*in transit*" to the US, by accessing underwater cables on the floor of the Atlantic, and to collect and retain such data before arriving in the United States and being subject there to the FISA. Activities conducted pursuant to EO 12333 are not governed by statute.
[10] According to the Meta decision, the US Presidential Policy Direction-28 allows for bulk' collection … of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target … to focus the collection".

body whose decision is binding on the Chinese government. The practices around the Personal Information Protection Law enforced by the Cyberspace Administration of China are not yet fully established. The DPC questioned whether any Chinese regulator was independent from the government.

All these shortcomings suggested a failure to meet the Essential Guarantees Recommendations formulated by the EDPB,[11] including the "rule of law" (Guarantee A), necessity and proportionality and privacy as a "human right" (Guarantee B), independent regulator with effective powers (Guarantee C) and effective remedies for the individual (Guarantee D).

Supplementary measures

Under the GDPR, supplementary measures may be adopted to compensate for divergencies in local laws, particularly where SCCs fail to provide the required level of protection.

TikTok argued that it was permitted to adopt a risk-based approach and that given the low risk to individuals assessed objectively, its data transfers were lawful. However, the DPC disagreed. Had TikTok assessed specific risks in the first place, it would have been able to select appropriate supplementary measures based on the level and likelihood of risk. However, this was not possible without first identifying the relevant divergencies in Chinese law and practice and assessing the relevant risks, which TikTok failed to do. This rendered its supplementary measures ineffective.

Much of the detail about TikTok's technical contractual and organisational measures is redacted in the decision. TikTok did implement strict access controls, encryption, an intra-group data transfer agreement, contracts with external cloud providers, as well as EEA Data Transfer Policy and Law Enforcement Guidelines and Frequently Asked Questions. However, as these measures were not directed at addressing specific risks, they were considered ineffective. Adducing evidence such as TikTok's and LinkedIn's transparency reports about limited law enforcement requests by Chinese authorities did not assist.

Further, many of the supplementary measures were reflective of general security measures required under Article 32 GDPR, which the DPC found could not assist. For example, encryption, physical data separation and access controls are ineffective if Chinese authorities could compel access to plain text data. Contractual measures are not binding or effective on public authorities in China. TikTok asserted that Chinese authorities could impose confidentiality of data and protect privacy that way. However, TikTok failed to outline how this would work in practice.

[11] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (link).

Derogation

The GDPR allows for derogations where data transfers may be lawful, for example, if based on contractual necessity, compelling legitimate interests or consent.

TikTok submitted an example where a highly skilled TikTok engineer in China needed remote access to EEA data to deal with an emergency, such as significant risk of harm. However, TikTok did not produce any underlying compliance documentation such as a balancing test assessment. The DPC held that wrongful reliance on derogations could undermine the essence of people's right to data protection and the principle of proportionality.

Transparency

The DPC investigated TikTok's compliance with its transparency obligation under Article 13(1)(f) GDPR in relation to transfers of personal data to China by way of remote access.

The DPC recalled that transparency must be as meaningful, specific and as precise as possible to empower data subjects to hold organisations accountable and to exercise their data rights, such as the right to object and otherwise control their personal data.

The DPC held that, essentially, Article 13(1)(f) requires a controller to provide the following information in clear, plain, easily accessible written form at the time of data collection:

- intention to transfer personal data to a third country;
- name of third country;
- details of the transfer mechanism, such as SCCs; and
- appropriate or suitable safeguards and data subjects' ability to obtain a copy.

Whilst TikTok's 2021 EEA Privacy Policy failed to provide these details, its 2022 EEA Privacy Policy informed individuals that personal data was stored on servers in the United States and Singapore, and was the subject of limited remote access by entities in TikTok's corporate group located in Brazil, China, Malaysia, Philippines, Singapore, and the United States. The DPC assessed that this policy was compliant for the purposes of this investigation.

Conclusion

It is clear that Chinese law may not be considered to provide essential equivalence in many (but not all) circumstances. Unfortunately, the DPC's decision leaves us wondering how it might have played out had TikTok been more prepared. TikTok failed to present the correct facts in its submissions and assessments, failed to submit

relevant evidence, failed to identify specific risks and failed to address those risks with relevant supplementary measures. It tells us little about how compliance may be achieved by other Chinese companies, not engaged in the high privacy risks of social media. On the other hand, if sophisticated organisations like ByteDance and TikTok with privacy experts at their disposal get it wrong, how do other Chinese organisations stand a chance?

The decision does not mean that Europe-China data transfers, or in fact, data transfers to any other country in the world, are entirely banned. Each case will turn on its own facts. Rather, data transfers require particular attention, planning and maintenance, to stay on the right side of the law. Organisations should take advantage of privacy-preserving technologies including pseudonymisation. The CJEU's recent SRB decision[12] suggests that pseudonymised data will not always constitute personal data, particularly, if the recipient is effectively unable to identify the individuals.

If a transfer impact assessment (**TIA**) discloses unresolved high risk, it might be appropriate for Chinese organisations to initiate a prior consultation with the relevant data protection authority in Europe under Article 36 GDPR. This is another safeguard, even if much less practical, that organisations could take advantage of when designing their international operations.

Some of the lessons from the TikTok decision include:

- Every cross-border data transfer **must be underpinned by a factually correct, supported and well-reasoned TIA**, a valid transfer mechanism, targeted supplementary measures, updated privacy policy and a data privacy training programme and other measures to demonstrate compliance with the GDPR.

- **A TIA must be realistic** and take account of actual likely practice, precedents, case law, practical examples and risks. It must disclose practical examples supported by evidence of how the law will apply to data in the context of the matter, rather than relying on favourable hypothetical interpretation of the law which might be applied differently in practice. Where divergencies are identified, their effect on compliance must be practically examined and substantiated.

- There is **no duty to identify all divergences** between EU and local law but a duty to identify and explain the effect of those laws that are relevant in the context of the specific data transfer.

- Inadequate assessment of local law will likely result in the **adoption of inadequate and ineffective supplementary measures**.

[12] *Case C-413/23 P EDPS v Single Resolution Board (SRB)* EU:C:2025:645 (link).

- **Each TIA will turn on its facts** including technical details of electronic copies of data in networks and on devices. Organisations must carry out a data map with the help of privacy experts to discover all facts and avoid errors.

- A **risk-based approach is not recognised** to negate the duty to identify essential equivalence and resulting risks. However, assessing that certain risk is "*hypothetical or very unlikely to materialise*" may be relevant in choosing appropriate supplementary measures.

Alexander Dittel, Principal in Data Privacy Cyber and Digital at KHQ Lawyers (Melbourne)