数据合规｜TikTok天价处罚背后

参考资料：

- 新闻稿 提示：处罚原文尚未公布。
- TikTok回应
- IAPP对副专员Cian O'Brien专访
  - 对专访的内容总结及评述：
    - 科技利维坦｜观察做了要点提炼，并对这一处罚的后续影响——企业向中国进行数据传输所面临的结构性难题进行了评述。
    - 智幻时刻FUNGIMIND撰写的分析报告对副专员发言中的要点进行了清晰的整理。
    - 数据何规｜文字实录提供了专访全程（目测）AI中文稿。

背景概述

2025年5月2日，爱尔兰数据保护委员会（Irish Data Protection Commission，DPC）对TikTok处以5.3亿欧元（约合人民币44亿元）的罚款，并要求其在6个月内整改数据跨境传输的合规问题，否则将暂停其向中国传输数据的活动。这是欧盟首次针对向中国的数据转移行为开出罚单，也是首次下达暂停向中国数据转移的命令。TikTok表示将上诉至爱尔兰法院。本篇笔记中，我将基于上述参考资料（主要是访谈内容），对本案件目前的重点问题进行梳理。

重点问题

1. 为什么远程访问被视为数据转移？调查有哪些发现？

💬 **问题**
数据保护委员会发现TikTok违反《通用数据保护条例》（GDPR）第46条第五章关于国际数据转移的规定，涉及中国境内人员远程访问欧盟/欧洲经济区（EEA）用户数据。请详细说明为何远程访问被视为数据转移，以及调查中的发现。

💬 **回答**

- **远程访问的本质**：
  此次数据转移与此前案例（如2023年5月对Meta处以12亿欧元罚款、荷兰2024年7月对Uber处以2.9亿欧元罚款）不同。Meta和Uber涉及将EEA用户数据存储在第三国（美国）服务器，而TikTok案例涉及中国员工基于业务需求远程访问存储在中国境外服务器的EEA用户数据。访问目的多样，导致大量类别的数据被转移，性质为系统性、重复性和持续性。
  根据2020年欧洲数据保护委员会（EDPB）的补充措施建议，第三国的远程访问构成GDPR意义上的数据转移，因为数据在中国本地设备上被处理，尽管未存储在中国服务器。
- **调查发现**：
  - 调查始于2021年9月，覆盖至2023年5月（决定初稿发布时）。TikTok的“三叶草项目”（Project Clover）调整了数据转移方式，但DPC仍认定需暂停数据转移并要求合规化。
  - 2025年2月，TikTok发现少量EEA用户数据存储在中国服务器，纠正了此前“无数据存储在中国”的陈述。DPC正与EEA其他监管机构关注此事，但本次决定仅针对远程访问，未涉及数据存储问题。

涉及法条与案例：

- **GDPR第46条**：规定数据向未获充分性认定的第三国转移需采取适当保障措施。
- **EDPB 2020年补充措施建议**：明确远程访问构成数据转移。
- **Meta案例（2023年5月）**：因向美国转移数据被罚12亿欧元。
- **Uber案例（2024年7月）**：荷兰监管机构因数据存储在美国被罚2.9亿欧元。

2. TikTok依赖哪些机制进行数据转移？DPC如何评估标准合同条款（SCCs）的使用？

💬 **问题**
TikTok依赖标准合同条款（SCCs）进行数据转移。DPC如何评估TikTok对SCCs的使用？涉及哪些法律依据？

💬 **回答**

- **TikTok的机制**：
  TikTok使用SCCs，并在欧盟委员会期限内完成版本转换。SCCs适用于向未获充分性认定的国家（如中国）转移数据。TikTok还实施了技术、组织和合同等补充措施，符合大型科技公司的标准做法。
- **DPC的评估**：
  - 根据“Schrems II案”判决，依赖SCCs的实体须核查并保证数据在第三国获得与欧盟基本等效的保护水平，否则须暂停或终止转移。TikTok的评估存在两方面缺陷：
    1. **宏观评估不足**：TikTok承认中国法律在数据隐私、公共机构数据获取、监管监督、救济权利及国际条约等方面与欧盟存在差异，但未针对具体数据转移场景深入分析这些差异，仅笼统认为数据存储在境外即可规避问题。
    2. **属地原则支持不足**：TikTok认为中国法律无域外效力，境外存储数据不受中国法律管辖，但未充分证明在远程访问（数据在中国本地设备处理）场景下，中国法律如何不适用。
  - DPC强调，评估需结合具体数据转移的性质、数据类型及处理方式，而非仅宏观比较法律框架。还需考虑第三国国家安全和执法相关法律的影响。

涉及法条与案例：

- **GDPR第46条**：规定SCCs作为数据转移工具的要求。
- **Schrems II案**：要求依赖SCCs的实体核查并保证基本等效保护水平，否则暂停转移。
- **Schrems I案**：首次明确基本等效性标准，要求数据转移提供与欧盟相当的保护。

3. 中国法律和实践在数据转移中的影响是什么？

💬 **问题**
从DPC的决定中，能否了解中国在EEA数据转移方面的法律和实践情况？TikTok的评估有哪些关键点？

💬 **回答**

- **TikTok的评估**：
  TikTok提交的数据转移评估报告指出，中国法律在以下方面与欧盟标准存在差异：
  - **数据隐私监管**：中国法律未提供与欧盟相当的保护。
  - **公共机构数据获取**：获取数据需批准，但批准机构不独立，规则不透明。
  - **监管监督**：缺乏欧盟要求的独立监督机制。

- **救济权利及国际条约**：与欧盟标准存在显著差距。
  TikTok认为，结合SCCs和补充措施，数据可获基本等效保护，且因数据存储在境外，不受中国监控法律管辖。
- **DPC的观点**：
  远程访问导致数据在中国本地设备处理，中国的法律和实践可能影响基本等效性认定。TikTok未充分分析这些法律在具体场景下的适用性，其结论缺乏依据。

涉及法条与案例：

- **GDPR第46条**：要求核查第三国法律以确保基本等效保护。
- **Schrems II案**：强调评估第三国法律和实践的重要性。

4. TikTok在透明度方面有哪些违规？为何重要？

💬 **问题**
DPC发现TikTok在2021年10月隐私政策透明度方面存在问题。请详细说明发现及重要性。

💬 **回答**

- **违规发现**：
  DPC依据GDPR第13条第1款（f）项评估TikTok的透明度义务，发现2021年10月隐私政策存在两方面违规：
  1. **未明确目的国**：政策未列明数据转移至中国等具体国家，仅泛指“转移出EEA”，不足以让数据主体了解数据处理地点及方式。
  2. **未说明处理操作性质**：政策未披露数据处理包括中国远程访问境外服务器数据的情况，导致数据主体无法知晓转移的真实性质。
- **后续改进**：
  2022年12月隐私政策更新，明确提及中国作为目的国，并说明数据存储在境外服务器，由字节跳动中国实体有限远程访问，符合GDPR要求。
- **重要性**：
  透明度是GDPR核心原则，数据主体需清楚数据转移的目的国及处理操作性质，以决定是否使用服务。明确目的国是普遍要求，除非基于充分性认定（GDPR第45条）。本案中，透明度违规导致罚款4500万欧元。

涉及法条与案例：

- **GDPR第13条第1款（f）项**：要求数据控制者告知数据主体数据转移至第三国的事实及适当保障措施。
- **WhatsApp案例**：DPC因透明度问题对其罚款2.25亿欧元。

5. DPC行使了哪些纠正权力？后果是什么？

💬 **问题**
DPC行使了三项纠正权力，包括暂停数据转移、要求合规化及罚款。请详细说明这些措施及不遵守的后果。

💬 **回答**

- **纠正权力**：
  1. **暂停数据转移命令**：要求停止向中国转移数据，基于“Schrems II案”判决，因TikTok未能保证基本等效保护。
  2. **数据处理合规化命令**：针对暂停令生效时已在中国的EEA用户数据，要求整改以符合GDPR。
  3. **行政罚款**：总计5.3亿欧元，分为：
     - 4.85亿欧元：针对违反GDPR第46条（非法数据转移）及第13条第1款（f）项（透明度）。
     - 4500万欧元：针对透明度违规。
- **罚款依据**：
  依据GDPR，考虑侵权严重性（系统性、持续性转移）、疏忽性质及数据未存储在中国的缓解因素，确保罚款有效、合理且具威慑性。
- **合规期限与后果**：
  TikTok有6个月整改期，DPC将与其沟通确保合规。若不遵守，可能面临进一步执法行动，如延长暂停令或追加处罚。

涉及法条与案例：

- **GDPR第46条、第13条第1款（f）项**：违规依据。
- **Schrems II案**：支持暂停数据转移的法律依据。

6. 决定对其他组织的意义是什么？

💬 **问题**
罚款是否旨在对其他组织传递信息？决定对向中国或其他第三国转移数据的组织有何影响？

💬 **回答**

- **威慑性目的**：
  罚款旨在防止TikTok再次违规，同时对所有组织起到警示作用，强调遵守GDPR的重要性。
- **更广泛信息**：
  无论转移至中国、美国或其他第三国，依赖SCCs的实体须核查并保证基本等效保护水平，否则不得转移数据。若第三国情况变化，需持续重新评估并暂停不合规转移。评估需基于具体转移场景，而非仅依赖宏观法律分析。

涉及法条与案例：

- **GDPR第46条**：核查基本等效性的要求。
- **Schrems II案**：强调持续评估和暂停不合规转移。

7. 监管机构会否提供更多指引？公司评估如何接受审查？

💬 **问题**
能否期待DPC或其他监管机构针对向中国、俄罗斯等国家的数据转移提供更多指引？公司评估是否足以证明合规？

💬 **回答**

- **监管机构的角色**：
  主要由数据控制者或处理者核查基本等效性。若公司表面证明合规，DPC可独立评估第三国法律以验证结论。例如，“Schrems案”中，爱尔兰高等法院通过听证美国法律专家确定事实。
- **指引前景**：
  监管机构会基于具体案例处理，未明确承诺针对中国等国发布通用指引。EDPB曾发布报告，研究中国、印度、俄罗斯等国政府数据获取情况，为评估提供参考。

- **公司评估的审查**：
  公司不能仅做表面评估，需提供实质证据证明基本等效性，否则可能被监管机构质疑或推翻。

涉及法条与案例：

- **Schrems案**：监管机构独立评估第三国法律的案例。
- **EDPB报告**：研究多国政府数据获取情况。

8. 决定发布流程及跨境执法趋势

💬 **问题**
最终决定何时发布？跨境执法中监管机构观点是否趋于一致？这对隐私专业人员有何意义？

💬 **回答**

- **决定发布**：
  TikTok已于上周收到最终决定，正确定机密信息以供删减。DPC将审查并尽快发布删减版决定，避免泄露技术措施等敏感信息。
- **跨境执法趋势**：
  这是DPC连续第五个未受其他EEA监管机构反对的决定，反映GDPR执法趋于一致。原因包括：
  - GDPR生效7年（2018-2025），法律确定性增强。
  - 欧盟法院判决（如“Schrems II案”、领英行为广告案(*编者注：不确定是哪一个案例*)）及EDPB约束性决定提供清晰指引。
  - 监管机构发布更多指南，合作加强。
    未来若有反对意见或需EDPB约束性决定，仍属正常，因涉及复杂法律和技术问题。
- **对隐私专业人员的意义**：
  监管机构观点趋同意味着违规后果严重（高额罚款、纠正命令）。隐私专业人员需准确预判监管立场 需加强数据映射、风险评估及合规措施。

涉及法条与案例：

- **GDPR第7章**：合作与一致性机制。
- **Schrems II案、领英行为广告案**：提供法律指引。

9. 对小公司的建议

💬 **问题**
TikTok投入“三叶草项目”仍未合规，小公司向中国等非充分性国家转移数据时，DPC有何建议？

💬 **回答**

- **建议**：
  小公司应聚焦具体数据转移场景，评估数据类型、处理方式、存储位置及访问权限。无需全面分析第三国法律，仅针对具体转移场景核查基本等效性。
  若无法保证保护水平，应考虑数据本地化或减损条款等替代方案，在合规前不得启动转移。
- **区别**：
  依赖SCCs的转移需逐案评估，区别于基于充分性认定的转移（GDPR第45条）。

涉及法条：

- **GDPR第46条**、**第45条**：SCCs与充分性认定的区别。

TikTok对DPC决定主要异议

TikTok对2025年5月2日DPC对其处以5.3亿欧元罚款并要求整改数据跨境传输的决定表示强烈反对，并计划全面上诉。其主要异议集中在以下三方面：

1. **未充分考虑“三叶草项目”的数据保护措施**
   TikTok认为DPC决定未能充分评估其耗资120亿欧元的“三叶草项目”（Project Clover），该项目于2023年实施，提供了行业领先的数据保护措施，包括：
   - 默认将欧洲用户数据存储在欧洲数据中心（如芬兰新建的数据中心）。
   - 通过NCC Group（欧洲权威网络安全公司）独立监控数据访问和传输。
   - 实施安全网关和隐私增强技术（如访问加密、差分隐私），确保中国员工仅能访问去标识化的非敏感数据，限制对敏感数据（如电话号码、邮箱、IP地址）的访问。
     TikTok强调，这些措施超越行业标准，且NCC Group已验证其有效性，但DPC未给予应有重视，质疑若如此严格的保护仍不足，何为合规标准。
2. **决定聚焦过往时期，忽视现行合规实践**
   DPC的调查聚焦2021年9月至2023年5月的数据转移行为，TikTok认为这忽略了“三叶草项目”实施后（2023年起）的重大改进。TikTok指出，其现行数据保护实践已显著提升，决定未反映当前合规状态，评估依据过时。
3. **对标准合同条款（SCCs）使用的评估不公**
   TikTok认为DPC错误认定其未进行必要的数据转移评估。TikTok强调：
   - 其依赖欧盟标准合同条款（SCCs）进行数据转移，与众多在欧洲运营的全球公司做法一致，符合欧盟法律框架。
   - 已在外部律师和专家指导下开展了详细的数据转移评估，透明披露相关机制（如隐私政策中明确数据转移至中国）。
     TikTok认为DPC将其单独挑出是不公平的，尤其是在其他公司同样使用SCCs的情况下，决定可能对依赖SCCs的全球企业造成广泛影响，损害欧盟竞争力。
4. **中国政府未请求或获取欧洲用户数据**
   TikTok重申，DPC报告确认其从未收到中国政府对欧洲用户数据的请求，也从未向其提供此类数据。TikTok认为，DPC对其数据转移风险的评估过于假设性，未基于实际证据，忽视了其通过“三叶草项目”有效管控风险的努力。