Disclaimer: This two-pager has been prepared by the CKN Secretariat and should not be considered the work of the individuals listed as authors of the report.

#22 The Legal Protection of International Organisations' Data

Authors: Aude Géry and Anne-Thida Norodom

January, 2023

Key Takeaways

- Data of Europeans transferred to the United Nations may be stored in China or handled by Chinese cloud providers, raising questions about compliance with Dutch/EU privacy and cybersecurity requirements.
- Due to the privileges and immunities of the UN, neither European nor Chinese law applies directly to UN data; such data qualifies as "property and assets" enjoying immunity and inviolability, regardless of location.
- While the UN has its own internal data protection rules inspired by GDPR and similar frameworks, the level of protection does not appear equivalent to the European standard, and remains relatively vague in interpretation.
- Increasing conflicts of law between EU, China, and the UN are likely as data protection regimes evolve, especially given the growth of big data use and cloud computing within the UN system.

Policy Recommendations

- Encourage the conclusion or strengthening of agreements between China and the UN to explicitly recognize the immunity and inviolability of UN data and premises (e.g. the Regional Centre in China).
- Promote the development of a more precise and robust UN data protection framework to ensure a level of protection equivalent to European standards and facilitate international data transfers.
- Support continued EU–UN dialogue on data transfers to anticipate regulatory developments under the European Data Strategy (including the Data Governance Act and Data Act).
- Strengthen technical and contractual safeguards, including adapting contracts with cloud providers to include clear security obligations for the physical and IT protection of UN data.

Executive Summary

This study examines the legal protection of data belonging to international organisations, specifically the United Nations (UN), that may be stored in China. It forms part of a broader research project assessing the impact of China-based data storage on Dutch and European data security, with a focus on compliance with EU requirements on privacy and cybersecurity. The issue

has gained importance following the establishment in 2019 of a UN regional hub for big data in China, developed in cooperation with the Chinese National Bureau of Statistics as part of the United Nations Global Platform. As a result, data originating from European actors and transferred to the UN may be processed or stored in China.

A central finding of the study is that the legal framework governing such data differs fundamentally from standard EU or Chinese data protection regimes. Due to the privileges and immunities of the United Nations under international law, including those enshrined in the UN Charter and the Convention on the Privileges and Immunities, UN data is not subject to national legal systems. Instead, it qualifies as the "property and assets" of the organisation and benefits from immunity from legal process and absolute inviolability, irrespective of where the data is physically stored. This means that host states, including China, cannot access UN data without authorization, and may incur international responsibility in case of unauthorized interference. Infrastructure such as data centres and regional hubs may also qualify as "premises of the organisation", further reinforcing their protected status.

However, the non-applicability of EU and Chinese law does not imply the absence of regulation. The UN has developed a set of internal policies and principles on data protection, forming part of a broader emerging "common law" of personal data protection. While these principles are similar in structure to frameworks like the GDPR or China's Personal Information Protection Law (PIPL), they remain broad, flexible, and open to interpretation. Current interpretations tend to prioritise the functional needs of the organisation, resulting in a more permissive approach to data protection than that found in European law. Consequently, the level of protection for personal data within the UN system does not yet appear equivalent to EU standards. The study also emphasizes the growing complexity of overlapping legal regimes. As both the EU and China continue to expand their regulatory frameworks, moving beyond personal data to broader data governance issues, conflicts of law involving international organisations are likely to intensify.

To address these challenges, the study highlights the importance of strengthening both legal and practical safeguards. On the legal side, it calls for more explicit agreements between host states and the UN to secure recognition of immunities, as well as the development of a more detailed and stringent UN data protection regime aligned with international best practices. On the policy level, continued engagement between the EU and the UN is needed to manage data transfers and anticipate regulatory developments under the European Data Strategy. On the operational side, technical and contractual measures, especially in cloud computing arrangements, are essential to ensure robust data security.

Overall, the study concludes that while UN data benefits from strong protections under international law, gaps remain in terms of substantive data protection standards and practical safeguards, necessitating further institutional, legal, and technical efforts to ensure adequate protection for European data stored in China.