China Digital Governance — Analytical Report

Generated: 2026-04-08 | Scope: China Digital Governance (demo set) | Template: Academic Style

Period: 2026-03-01 — 2026-03-31 | Claims: 2 | Evidence records: 2

1. Context

Two captured Chinese first-party sources describe a coordinated digital-governance posture: a State Council normative notice and a CAC enforcement announcement, both captured on 2026-03-30.

2. Findings

2.1 State Council establishes graded data security regime. The State Council notice requires all regions and departments to build a graded and classified data security management system[1]. The notice is binding on all administrative levels.

2.2 CAC opens a one-month cross-border enforcement window. The Cyberspace Administration of China announced a one-month special enforcement campaign focused on entities that have not completed the required cross-border data transfer security assessment[2].

2.3 Cross-source pattern. The two captures, taken together, show the State Council's normative posture being given an operational expression by a regulator within the same week[1][2].

3. Evidence

Two evidence records were assembled, both from L1 normative / L4 regulator sources. Each footnote in this report resolves to a captured `source_version_id` preserved in the platform store.

4. Implications

Downstream sectoral and data-class rules can now attach to the State Council notice as a normative anchor[1]. The enforcement campaign anchors a concrete observation point regardless of whether activity persists past the one-month window[2].

5. Constraints and caveats

- This report is bounded to the demo source set (8 sources). It makes no claim about sources outside that set. - Findings describe published policy, not measured implementation. - Translations in the body are derivative; the Chinese spans in the footnotes are canonical. - No generative synthesis was used. Body text is assembled deterministically from accepted claims.

6. Methodology

Assembled via XINAPI's deterministic-extractive report path. Evidence is drawn from human-accepted claims only. Footnote ordinals are stable across markdown, PDF, and DOCX renderers.

Notes

[1] 国务院, "国务院关于网络安全和数据保护的通知", 2026-03-30, https://www.gov.cn/policy/v-demo-2026-03-30, accessed 2026-03-30. '第一条 各地区各部门应当按照本通知的要求，全面落实网络安全和数据保护责任，建立分级分类的数据安全管理制度。"

[2] 国家网信办, "国家网信办数据出境专项行动公告", 2026-03-30, https://www.cac.gov.cn/notice/v-demo-2026-03-30, accessed 2026-03-30. '国家网信办决定开展为期一个月的数据出境专项行动，重点检查未按规定开展数据出境安全评估的行为。"

Methodology

This report was assembled using XINAPI extractive report generation. All analytical claims are drawn from accepted (reviewer-approved) items only. Each claim listed in Key Findings is footnoted to its source evidence. Sections marked [Analytical Inference] represent synthesis across multiple sources rather than direct quotation. Sections marked [Uncertainty Note] or [Coverage Limitation] flag known gaps in the evidence base.

Source evidence derives from the XINAPI automated priority source set. Manual-only channels (e.g. WeChat Official Accounts without automated acquisition) are excluded from the automated claim set and are not represented in this report unless explicitly noted.

Report ID: rpt-report-dg | Generated by XINAPI