Beijing “Two Zones” Data-Export Negative List (2025)

DCC working English reference — Administrative Measures, important-data annex, and list scope. 中国（北京）自由贸易试验区、国家服务业扩大开放综合示范区数据出境负面清单（2025版）

DCC working translation — not official; not legal advice. This English rendering is prepared by Data Compliance China for the convenience of overseas counsel. Where it diverges from the published Chinese text, **the Chinese original controls**. The full list contains hundreds of field-level entries; the “list scope” section below summarises structure and thresholds rather than reproducing every data item — consult the Chinese original (downloadable alongside this file) for the authoritative text.

REGION	Beijing 北京 — province-wide (the “Two Zones”: the China (Beijing) Pilot Free Trade Zone + the National Comprehensive Demonstration Zone for the Expanded Opening of the Service Sector)
VERSION	2025 edition (supersedes the 2024 FTZ-only list)
ISSUED	May 11, 2026
ISSUERS	Beijing CAC · Municipal Government Services & Data Administration · Municipal Commerce Bureau · Municipal Public Security Bureau · Municipal State Security Bureau
LEGAL BASIS	Cybersecurity Law · Data Security Law · Personal Information Protection Law · Network Data Security Management Regulation · Provisions on Promoting and Regulating Cross-Border Data Flows (2024)
SCALE	9 industries · 67 scenarios · 612 data fields
MODEL	Pre-export filing (application to the district authority; 3-year validity)

Part A — Administrative Measures for the Data-Export Negative List (Trial)

Chapter I — General Provisions

Purpose and basis. These Measures are formulated to safeguard national data security, protect the rights and interests in personal information, replicate and extend the mature data-export management experience of the China (Beijing) Pilot Free Trade Zone, enhance the data-export management capability and level of facilitation of the Beijing “Two Zones,” and promote the efficient, convenient and secure cross-border flow of data — pursuant to the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, the Network Data Security Management Regulation, the Provisions on Promoting and Regulating Cross-Border Data Flows, and the relevant national rules on data-export security management.

Scope. These Measures apply to the formulation, approval and use-management of the data-export negative list within the Beijing “Two Zones.” Providing personal information to organisations or individuals placed on a restricted/prohibited personal-information-provision list (per the Personal Information Protection Compliance Audit Measures) is **excluded**. Where laws, regulations or rules provide otherwise, those provisions govern.

Principles. (1) **Hold the security bottom line** — comply with law, build sound security-management and technical-safeguard capacity, and promote orderly data flow only on the premise of data security. (2) **Support industrial development** — scope the data placed on the list scientifically and reasonably so as to maximise the facilitation of data-export activity. (3) **Batch-and-category management** — the list is formulated by industry and sector in batches; its data items are managed by category and, by sensitivity, divided into data subject to the **data-export security**

assessment and data subject to **personal-information standard-contract filing or personal-information protection certification**.

Chapter II — Responsibilities and Division of Labour

- **Municipal-level authorities** (Beijing CAC; Government Services & Data Administration; Commerce Bureau; Public Security Bureau; State Security Bureau) build and coordinate the "Two Zones" negative-list system, guide and supervise cross-border data activity, organise list formulation by industry/sector in batches, run the review-and-approval/filing process, and operate the dynamic-management mechanism. Public Security and State Security bureaus carry data-export security-supervision duties within their remits.
- **District-level authorities** (the lead departments of each district and the Economic-Technological Development Area) organise and guide handlers' **filing** work in their territory, strengthen tracking and supervision, and build mid-process evidence-retention and post-hoc oversight capacity. The FTZ-cluster districts (Chaoyang, Haidian, Changping, Tongzhou, Shunyi, Daxing, Yizhuang) act as the innovation/stress-test bed for new cross-border-flow management models.
- **Cross-border data service centres** provide advisory service on data-export policy and list application, connect to the security-assessment "green channel," and assist the municipal/district authorities with use consultation, filing-material review, and data-export risk assessment.
- **"Data handler"** means an enterprise, public institution, organisation, group or other organisation registered in the Beijing "Two Zones" that carries out cross-border data-flow and related activity. Handlers must identify and declare important data as required, conduct exports per district-authority requirements, and cooperate with consistency spot-checks and supervision.

Chapter III — Formulating and Administering the Negative List

Formulation workflow. (1) *Demand research* — survey key industries/sectors to map outbound data by scenario, category, volume and field. (2) *Important-data identification* — under the municipal data-security coordination mechanism, relevant industry regulators set identification standards, classify and grade the data, form an important-data catalogue and file it with the national mechanism; where an industry regulator has published a classification/grading standard, identify important data by that standard first, otherwise refer to the *Beijing "Two Zones" Data Classification & Grading Reference Rules* (Part B below). (3) *Scenario analysis* — select urgent, high-frequency export scenarios and set data items and volume tiers for controllable-risk scenarios. (4) *Review and consultation* — expert review plus consultation with municipal regulators. (5) *Approval and filing* — after review by the municipal data-security coordination mechanism, approval by the municipal cyberspace-affairs commission, then joint filing by Beijing CAC and the Data Administration with the national CAC and national data authority.

What the list must contain. (1) A **security-assessment list** — (i) CIIOs providing personal information or important data abroad; (ii) non-CIIO handlers providing important data abroad, or providing personal information abroad that reaches the assessment threshold. (2) A **standard-contract / certification list** — non-CIIO handlers providing personal information abroad that reaches the standard-contract or certification threshold.

Dynamic management. The municipal authorities track implementation and risk and revise the list; sectors not yet listed are studied and added over time. Beijing may **reference another province's FTZ / free-trade-port / reform-pilot negative list** for specific sectors — subject, in each case, to demand analysis and risk assessment by the municipal authorities, review by the data-security coordination mechanism, approval by the cyberspace-affairs commission, and filing with the national CAC and data authority.

Chapter IV — Implementing the Negative List

Handler process. (1) **File an application** with the district authority per the list's implementation guide (application form + letter of commitment). (2) **Export in compliance** — conduct exports per the **Negative-List Filing Result Notice** issued by the district authority, and cooperate with supervision and verification; **the filing result is valid for three years**; update the filing promptly when the export situation changes.

District review. Each district builds a special working mechanism and publishes an intake channel; within **10 working days** of receiving filing materials it reviews and issues a preliminary opinion on whether the outbound data falls on the list, and — after municipal confirmation — returns the result to the handler: **on-list** → guide the handler to a security assessment / standard contract / certification; **off-list** → notify the handler it may flow freely and securely; **not covered by the list** → apply current law.

Municipal review. The municipal mechanism runs a joint applicability-and-risk review of district opinions and applicant materials; participating units respond to Beijing CAC within **10 working days**; complex cases may involve the relevant industry regulator or an expert/consultation session.

Chapter V — Supervision and Administration

- Municipal and district cyberspace/data departments strengthen guidance and supervision of export activity across the full pre-/mid-/post-process chain, and build risk-assessment, incident-notification and monitoring-and-early-warning capacity.
- Within the filing validity period, district authorities run **consistency spot-checks** between actual exports and the filed materials. For handlers that breach commitments, or conceal / misreport / deliberately create inconsistency, the district authority may order suspension of exports and time-bound rectification (re-filing required afterward); in serious cases, terminate exports, impose priority supervision and report up to the municipal level.
- Municipal authorities and industry regulators periodically assess effectiveness and risk-control. A "**credit + risk" tiered-and-categorised supervision** approach may reduce inspection frequency for handlers with strong security capacity, good credit and low-risk exports.
- Handlers that export data in breach of these Measures and national rules bear legal liability under the Cybersecurity Law, Data Security Law, Personal Information Protection Law, Network Data Security Management Regulation and related law.

Chapter VI — Supplementary Provisions

- **National core data** — data bearing on national security, the lifelines of the national economy, important aspects of people's livelihood, or major public interests — is subject to stricter management and is **not** placed on the negative list.
- These Measures are interpreted by Beijing CAC together with the Data Administration, Commerce Bureau, Public Security Bureau and State Security Bureau.
- For unlisted industries/sectors, the classification/grading reference rules follow the applicable rules and standards; off-list exports follow the Data-Export Security Assessment Measures, the Personal Information Standard-Contract Measures, the CBDF Provisions and other national rules.
- Where export involves controlled items' technical materials under the **Export Control Law** or technology-export matters under the **Foreign Trade Law**, those laws govern.
- These Measures take effect on issuance; the original *China (Beijing) Pilot FTZ Data-Export Negative List Administrative Measures (Trial)* is repealed simultaneously. Filing result notices already obtained under the prior measures remain valid.

Part B — Annex: Data Classification & Grading Reference Rules

Unified important-data identification (reference thresholds)

Applies to non-classified data (classified data follows separate rules). Data held by Beijing "Two Zones" enterprises is treated as important data where it involves, for example:

- Personal information of 10,000,000+ individuals (excluding sensitive PI); sensitive PI of 1,000,000+; or PI of 100,000+ that includes personal bank / insurance / registered accounts or personal diagnosis-and-treatment data (sensitive).
- PI of 100,000+ held by an operator designated as critical information infrastructure (CIIO).
- High-value sensitive data related to industry competitiveness or production safety, collected/generated in R&D-design, manufacturing or operations; enterprise supply-chain data bearing on national security.
- Parameters, control, O&M and test data of automated-control systems in lifeline (economy-and-livelihood) sectors.

Important-data reference catalogue (13 categories · 40 sub-categories)

Top category	Sub-category	Illustrative important-data (representative)
I. Strategic materials & bulk commodities 战略物资和大宗商品	1. Oil, petrochemicals & gas; 2. Agricultural products	Product-output / international-trade data from which national strategic conditions could be inferred; strategic reserves of grain, cotton, edible oil, sugar, meat, dairy; undisclosed germplasm-resource category/quantity data affecting biosafety.
II. Natural resources & environment 自然资源和环境	3. Geographic information; 4. Meteorology; 5. Ocean; 6. Environmental protection; 7. Water resources	Geo-information at regulated coverage/precision/scale or showing sensitive areas; meteorological monitoring serving military/defence/high-tech; ocean-environment/disaster data unfit for release; flood/drought-defence and key-water-project data.
III. Industrial 工业	8. Steel & non-ferrous metals; 9. Rare earths; 10. Other minerals; 11. Chemicals; 12. Power; 13. Electronic information; 14. Civil nuclear; 15. Industrial equipment; 16. ICV; 17. Other	Reserves/output/procurement of militarily-and-civilly valuable metals; China-unique rare-earth mining/smelting technology; key hazardous-chemical process/equipment data; civil-nuclear R&D and monitoring; advanced IC design/manufacturing; automotive key-component R&D; ICV autonomous-driving training data. (Ref. YD/T 4981-2024.)
IV. Defence science-and-technology industry 国防科技工业	18. Defence S&T industry	Data on operations, R&D-design, manufacturing, testing and maintenance-support that reflects defence-industry capability or, aggregated, the sector as a whole.

V. Telecommunications 电信	19. Telecom	Build-out plans, performance parameters, monitoring/analysis and O&M data of important network facilities and systems. (Ref. YD/T 3867-2024.)
VI. Broadcasting & online audiovisual 广播电视和网络视听	20. Broadcasting & TV; 21. Online audiovisual	Undisclosed audiovisual content; content whose misuse could endanger ideological or public security; provincial-and-above transmission-coverage and monitoring/regulatory data; CII planning/O&M data.
VII. Finance 金融	22. Banking; 23. Insurance; 24. Securities & futures; 25. Financial leasing	Institutional security data across banking / insurance / securities-futures / leasing / payment-clearing, and the business data they hold for major enterprises — including defence-industry and national-security-related entities.
VIII. Transportation 交通运输	26. Transport (rail, road, urban, water, civil aviation, postal, integrated)	Data affecting production/supply-chain safety; natural-resource data acquired in construction; undisclosed route maps and key-node data; data whose leak/tampering could cause major transport accidents.
IX. Health, food & drug 卫生健康和食品药品	27. Genetic resources; 28. Health & medical; 29. Food; 30. Drugs; 31. Biosafety; 32. Disease control	Genetic-resource data reflecting ethnic/population health or biosafety; diagnosis-and-treatment data at scale/precision involving public health and safety; special-drug trial data; epidemic / vaccine / cause-of-death data on infectious disease.
X. Public safety 公共安全	33. Physical security; 34. Cybersecurity	Baseline data on key targets and security-equipment/deployment whose misuse could seriously harm social stability; design/operation data of CII or important networks.
XI. Internet services & e-commerce 互联网服务和电子商务	35. Internet-platform services; 36. AI services	Service-generated data usable for social mobilisation; digital-persona data of sensitive groups (e.g. veterans); records tracking military/government clients; AI training data, algorithm source code, key-component data and control programs that could affect national security.
XII. Science & technology 科学技术	37. IP & major discoveries; 38.	IP bearing on defence/national security; non-public research

	Prohibited/restricted-export technology	papers, observation data and industrialisation results that materially raise national-security capability; data on technologies in the Catalogue of Technologies Prohibited/Restricted from Export.
XIII. Other 其他	39. Export-control-listed items; 40. Other national-security-affecting data	Data on items in national export-control lists; other data meeting the important-data definition that could affect political, territorial, military, economic, cultural, social, technological, cyber, ecological, resource, nuclear, overseas-interest, space, polar, deep-sea, low-altitude or biological security.

Part C — The Negative List (2025): Scope

How the list is structured

Each of the nine industries is presented in **two tiers**, each a table of *data category → data sub-class → basic features and description*:

- **Tier 1 — security-assessment list:** CIIOs providing any PI or important data abroad; non-CIIO handlers providing **important data**, or PI reaching the assessment volume band.
- **Tier 2 — standard-contract / certification list:** non-CIIO handlers providing PI reaching the standard-contract/certification band.

Baseline personal-information volume bands (cumulative from January 1 of the current year, unless an industry sets a scenario-specific band):

- Security assessment: 1,000,000+ individuals' PI (non-sensitive), **or** 10,000+ individuals' sensitive PI.
- Standard contract / certification: 100,000 **to under** 1,000,000 PI (non-sensitive), **or under** 10,000 sensitive PI.

Volumes are **de-duplicated by natural person**; flows within Articles 3, 4, 5(1)(i) – (iii) and 6 of the CBDF Provisions are **not counted**. Export-controlled technical materials follow the Export Control Law / Foreign Trade Law regardless of the list.

The nine industries

Industry	Important-data focus (Tier 1, representative)	Scope notes
1. Automotive 汽车	External imagery/geo-info that could locate military/defence/Party-and-government sensitive areas; traffic & logistics data reflecting economic activity; regional charging-network data; off-vehicle video containing faces / plates / road signs; key-tech and high-value R&D data; special-vehicle design; remote-control telematics; CII	Applies to makers, parts/software suppliers, dealers, repair shops, mobility firms; **autonomous-driving firms are excluded** (see industry 7). Baseline PI bands apply.

	supply-chain data; large-scale supply-chain data.	
2. Pharmaceutical 医药	100,000+ group diagnosis/health, medical-rescue, special-drug-trial data; 10,000+ biometric or medical-resource data; undisclosed frontier-biotech production data; drug safety/efficacy/quality research data.	Scenario-specific PI bands: e.g. 50,000+ trial-subject PI; 100,000+ pharmacovigilance patient PI; 200,000+ HCP/investigator PI; 100,000+ HCP sensitive PI (with residual scenarios on the baseline bands).
3. Civil aviation 民航	Aviation data from sector development, regulation/enforcement, government administration, production/operation and service-assurance whose exposure affects operational or supply-chain safety.	Aircraft-maintenance data cross-references the Fujian FTZ list (2025). Baseline PI bands apply.
4. Retail & modern services 零售与现代服务业	—	**Personal information only, limited to the member-management scenario.** (No important-data tier; the retail entry is a PI-band entry for membership/CRM data.)
5. AI training data 人工智能训练数据	High-value sensitive data related to industry competitiveness collected/generated in R&D-design; content whose tampering/leak could endanger national security, economic operation or social stability; PI and important data within training-sample sets for machine-learning models.	"Training data" = the input-sample sets used to train ML models. Baseline PI bands apply.
6. Medical devices 医疗器械	Device-industry supply-chain security data; 100,000+ group diagnosis / 10,000+ biometric data; key-tech / key-process / domestic-substitution R&D data; genetic information and gene data at regulated scale/precision.	"Medical device" per the Regulation on Supervision and Administration of Medical Devices. Baseline PI bands apply.
7. Autonomous driving (ICV) 自动驾驶（智能网联汽车）	Sensitive-area external imagery; high-precision location/trajectory, inertial-navigation, camera/lidar road-perception data; fusion-compute data; regional charging-network data; scene-library data; HD-map/mapping data; remote-control data affecting public/traffic/life safety; high-value R&D data; regulator-designated important data.	The autonomous-driving counterpart to the automotive list, scoped to ICV. Baseline PI bands apply.
8. Trade & logistics 贸易物流	Sensitive-area geo-info at precision; sea/land/air-port hub facility,	Covers transport, warehousing/sorting,

	operation and security data; customs-operation data; declaration/clearance data reflecting economic trends; key-enterprise customs data; platform-collected undisclosed statistics and trade secrets reflecting the broader economy.	declaration, clearance and delivery. Baseline PI bands apply.
9. Banking 银行业	Identity-authentication data of Party/government/military units; data usable to attack critical information infrastructure; banking important data designated by the central financial regulator.	Covers important data and PI in commercial-banking business activity. Baseline PI bands apply.

Source: 中国（北京）自由贸易试验区、国家服务业扩大开放综合示范区数据出境负面清单（2025版） and its Administrative Measures (Trial), issued by Beijing CAC and partner departments, May 11, 2026; filed with the national CAC and National Data Administration. Chinese originals downloadable at datacompliancechina.com/resources/negative-lists.