

Shanghai City-wide Data-Export Negative List (2025)

DCC working English reference — measures and list scope. 中国（上海）自由贸易试验区及临港新片区、国家服务业扩大开放综合试点地区（上海）数据出境管理清单（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 list's field-level detail is summarised for scope rather than reproduced in full — consult the Chinese original (downloadable alongside this file) for the authoritative text.

REGION	Shanghai 上海 — City-wide
VERSION	2025 edition
ISSUED	April 29, 2026
ISSUERS	Shanghai CAC · Shanghai Municipal Data Administration
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 scenarios · 29 data sub-classes · 109 data items
MODEL	Post-export reporting (materials filed within 15 working days)

Part A — Administrative Measures (Trial)

Full title: 中国（上海）自由贸易试验区及临港新片区、国家服务业扩大开放综合试点地区（上海）数据出境负面清单管理办法（试行） — *Measures for the Administration of the Data-Export Negative List for the China (Shanghai) Pilot Free Trade Zone and the Lin-gang Special Area, and the National Comprehensive Pilot Zone for Expanding Opening-up of the Service Sector (Shanghai) (Trial)*. Five chapters, twenty-one articles.

Chapter I — General Provisions (总则)

Article 1 — Purpose and basis. The Measures are enacted to safeguard national data security, protect personal-information rights and interests, replicate and extend the mature data-export management experience of the China (Shanghai) Pilot Free Trade Zone and the Lin-gang Special Area, further promote and regulate the lawful and orderly export of data, comprehensively align with high-standard international economic and trade rules, and build a national demonstration zone for institutional opening-up. They rest on the **Cybersecurity Law**, the **Data Security Law**, the **Personal Information Protection Law**, the **Network Data Security Management Regulation** and the **Provisions on Promoting and Regulating Cross-Border Data Flows** (CBDF Provisions), together with the Ministry of Commerce's *Overall Plan for the Comprehensive Pilot on Expanding Opening-up of the Service Sector in Shanghai* and its *Notice on Replicating and Extending a New Batch of Demonstration Experiences from the Comprehensive Service-Sector Opening-up Pilot*.

Article 2 — Scope. The Measures apply to **data handlers registered in Shanghai and carrying out data-export activities in Shanghai**, and to the related promotion, safeguarding and supervision work. Pursuant to the *Measures for the Administration of Personal Information Protection Compliance Audits*, providing personal information to organisations and individuals placed on the list of those **restricted or prohibited from receiving personal information** does not fall under these Measures. Where laws, administrative regulations, or the national cyberspace authority or an industry regulator provide otherwise, those provisions govern.

Article 3 — Compliance model. Persisting in coordinating development and security, a data-security-compliant export model that **combines a negative list with operational guidelines** is established; data handlers are encouraged to carry out data-export business in accordance with law and the convenience of data export is to be improved.

Article 4 — Principles. Following the principles of inclusiveness and prudence, tolerance for innovation and error, promotion of development, and protection of rights and interests, Shanghai advances the facilitation of data export.

Chapter II — Working Mechanism and Responsibilities (工作机制与职责)

Article 5 — Classification, grading and important-data catalogues. Under the overall coordination of the Shanghai data security work coordination mechanism, the **Shanghai Cyberspace Administration (Shanghai CAC)**, the **Shanghai Municipal Data Administration** and the relevant municipal-level industry regulators — acting under the Data Security Law and related law and applying the relevant important-data identification standards — organise industry data handlers to conduct **data classification and grading**, form **important-data catalogues**, and file them by procedure with the office of the national data security work coordination mechanism. Where an industry regulator has already published, or issued within the industry, data classification-and-grading standards for its sector, important data are identified under those first; where no determination criteria have been specified, important data are identified under the *Data Classification and Grading Reference Rules for the China (Shanghai) Pilot Free Trade Zone and Lin-gang Special Area* and the *National Comprehensive Service-Sector Opening-up Pilot Zone (Shanghai)* (translated in Part B).

Article 6 — Division of labour. In line with the national data-export transmission security management system and focused on building the “Five Centres” (五个中心), the Shanghai CAC, the Shanghai Municipal Data Administration and the **Shanghai Municipal Public Security Bureau** are responsible for coordinating matters relating to the Shanghai data-export negative list, establishing a **data-security risk-assessment mechanism** for the list, regularly conducting effectiveness assessments and risk prevention and control, and using assessment results as an important basis for optimising list management; together with the municipal industry regulators they guide and supervise data-export activities. The **Shanghai Municipal State Security Bureau**, within its remit and under the relevant laws, administrative regulations and these Measures, undertakes data-export security supervision. **Each district** is responsible for organising and guiding data handlers within its area to use the negative list for data export, and for continuous before-, during- and after-the-event management. The Shanghai Pilot FTZ Administrative Committee and the Lin-gang Special Area Administrative Committee, each within its remit, actively explore new cross-border data-management models, drive innovation and facilitation in cross-border data-flow mechanisms, and enhance the effectiveness of the **cross-border data service centres**.

Article 7 — List drafting and information-sharing. The Shanghai CAC and the Shanghai Municipal Data Administration, together with the municipal industry regulators and in accordance with the data classification-and-grading protection system, are principally responsible for **compiling and updating** the Shanghai data-export negative list and the operational guidelines, resolving the problems data handlers encounter in data export, and maintaining information-sharing across Shanghai — notifying the implementation status of the list and guidelines and specific problem-solutions so that information is mutually exchanged.

Chapter III — Implementation and Management of the Negative List (负面清单实施与管理)

Article 8 — Approval and national filing. Once approved by the Municipal Cybersecurity and Informatization Commission (市委网络安全和信息化委员会), the data-export negative list is jointly filed by the Shanghai CAC and the Shanghai Municipal Data Administration with the national CAC and the national Data Administration.

Article 9 — The core benefit. A data handler registered in Shanghai that belongs to an industry or field for which a negative list has been published, and that provides data **falling outside the negative list** to overseas recipients, may be

exempt from applying for a data-export security assessment, from concluding a personal information standard contract, and from obtaining personal information protection certification.

Article 10 — Relationship with operational guidelines. Where operational guidelines have been issued for a given industry or field, data handlers with export needs may proceed under those guidelines. **Where the guidelines and the negative list are inconsistent, the negative list controls.** Where national law provides otherwise on data export, those provisions govern.

Article 11 — The two-step process. A data handler using the negative list follows this workflow:

1. **Submit a filing application** — in accordance with the negative list's supporting *Implementation Guide*, the data handler submits a filing (备案) application to the district in which it is located.
2. **Carry out compliant export** — once filed, the data handler conducts data export as required by its district, and **promptly updates its filing** with the district whenever the export circumstances change.

A data handler transmitting important data and personal information overseas must, under the relevant national law and supporting policy and standards, discharge its data-security protection obligations, adopt technical and other necessary measures, strengthen its data-security safeguards, ensure export security, and **retain data-export logs**. On a data-export security incident or the discovery of a risk, it must take remedial measures and promptly report to the Shanghai CAC, the Shanghai Municipal Data Administration, the Shanghai Municipal Public Security Bureau, the Shanghai Municipal State Security Bureau, and its district.

Article 12 — District intake and municipal review. Each district publicly announces its intake channel; on receiving a data handler's filing materials it issues a **preliminary opinion** on whether the export data falls within the negative list, reports it to the Shanghai CAC and the Shanghai Municipal Data Administration for review, and then returns the filing-review result to the data handler:

- **Within the list** → the district guides the handler to apply for a data-export security assessment, conclude a personal information standard contract, or obtain personal information protection certification;
- **Outside the list** → the handler is told it may transfer the data freely and in an orderly manner in accordance with law;
- **Not covered by the list** → current law and regulations apply.

Districts are encouraged to establish **cross-border data service centres** offering advisory services on applying the negative list.

Article 13 — Municipal applicability and risk review. The Shanghai CAC and the Shanghai Municipal Data Administration review the districts' preliminary opinions and the handlers' application materials for **negative-list applicability and risk**. Complex matters may be reviewed jointly with the relevant industry regulators, and where necessary a special consultation or expert-appraisal meeting may be convened to form a review opinion.

Implementation Guide — filing procedure (folded in from the *Implementation Guide (Trial)*). The Guide governs data handlers registered and operating in Shanghai and details the mechanics of Article 11:

- **Application materials** (submitted to the district): (1) a copy of the unified social credit code certificate; (2) a copy of the legal representative's ID; (3) a copy of the handling agent's ID; (4) the agent's letter of authorisation (template); (5) the data-export negative-list filing application form (template); (6) a letter of commitment (template). Copies are stamped with the corporate seal, and forms (4) – (6) are completed in Chinese; offline filers also submit an electronic copy on disc.
- **District review — 10 working days.** Within 10 working days of receiving the materials the district organises a review, issues its preliminary opinion, obtains confirmation from the Shanghai CAC and the Shanghai Municipal Data Administration, and returns the result.

- **Supplementation / correction — 10 working days.** If materials must be supplemented or corrected, the handler submits them within **10 working days** of being notified; failing that without good cause, the district may terminate the filing.
- **Filing-result notice.** Outside the list → free, orderly transfer; within the list → apply for assessment / standard contract / certification, **submitting the filing-review result as supporting material**; not covered → current law applies.
- **Filing changes — 15 working days.** Where export circumstances change such that re-filing is needed, the handler submits an update application and re-submits materials within **15 working days**; where a list update affects a filing result, the district notifies the handler to re-file.
- **Filing termination.** Where a handler is penalised by the authorities, moves its registration out of Shanghai, or otherwise ceases to meet the list's requirements, the district — after confirmation by the Shanghai CAC and the Shanghai Municipal Data Administration — notifies it that the filing is terminated; to continue exporting, it must then follow the national regime (Data-Export Security Assessment Measures, Personal Information Standard Contract Measures, Personal Information Export Certification Measures, CBDF Provisions).
- **Compliance report — 3 months.** A handler that still must undergo assessment / standard contract / certification reports its export-compliance status to the district within **3 months** of receiving the filing-result notice (extension on justified notice and approval).
- **Annual report.** Every handler using the list reports its overall annual export activity to the district before year-end; the district consolidates and reports to the Shanghai CAC and the Shanghai Municipal Data Administration.

There is no fixed expiry term: a filing remains valid until circumstances change (re-file) or a termination trigger arises. The Guide also publishes the contact details of the district and special-area **cross-border data service centres** (updated to May 2026) across all sixteen districts, the Pilot FTZ zones (bonded, Lujiazui, Jinqiao, Zhangjiang, Expo), the Lingang Special Area, and the Hongqiao International Central Business District.

Chapter IV — Supervision and Administration (监督管理)

Article 14 — Inspection. The Shanghai CAC, the Shanghai Municipal Data Administration and the Shanghai Municipal Public Security Bureau, together with the municipal industry regulators and relevant functional departments, supervise implementation of the list and handlers' export activities through **regular inspections and “double-random” spot checks** (随机 inspectors on randomly selected targets).

Article 15 — Consistency, remediation and dynamic updating. The same authorities regularly inspect and assess handlers' compliance with these Measures. Where a processing activity presents a relatively high security risk, remedial measures are taken at once to remove the hazard, and **export data that affects or may affect national security is promptly added to the negative list**. Suspected offences are referred to the Shanghai Municipal Public Security Bureau and State Security Bureau, which prevent and combat crimes endangering data-export security within their respective remits.

Article 16 — District tracking and annual reporting. Each district tracks and supervises implementation and export activity in its area, strengthening before-, during- and after-the-event oversight and its risk-detection and early-warning capacity. Before year-end each district reports the overall annual export situation of handlers using the list in its area to the Shanghai CAC, the Shanghai Municipal Data Administration and the Shanghai Municipal Public Security Bureau (material matters reported promptly); the consolidated report goes to the office of the Shanghai data security work coordination mechanism and to the national CAC and national Data Administration.

Article 17 — Liability. A data handler that breaches these Measures and the national data-export security rules by exporting data non-compliantly is held liable by the competent authorities under the Cybersecurity Law, Data Security Law, Personal Information Protection Law, Network Data Security Management Regulation and related law.

Article 18 — Confidentiality of officials. Personnel involved in negative-list management must keep confidential the state secrets, personal privacy, personal information, trade secrets and confidential business information they learn in the course of duty, and must not disclose, unlawfully provide to others, or unlawfully use them; violators are punished under the relevant law.

Chapter V — Supplementary Provisions (附则)

Article 19 — Uncovered fields. For the classification-and-grading reference rules of industries and fields not covered by the negative list or the operational guidelines, the relevant provisions and standards apply.

Article 20 — Carve-outs and residual regime. Within the industries and fields covered by the list and guidelines, where the export involves technical materials for controlled items under the **Export Control Law** or technology-export matters under the **Foreign Trade Law**, those statutes and their implementing rules govern. Data of industries and fields **not covered** by the list or guidelines follow the Network Data Security Management Regulation, the Data-Export Security Assessment Measures, the Personal Information Standard Contract Measures, the Personal Information Export Certification Measures and the CBDF Provisions. Data-export negative lists formally released by FTZs, free-trade ports, reform-and-opening-up pioneer zones and national service-sector opening-up pilot demonstration areas in other provinces and cities **may be applied by Shanghai by reference**. On matters not expressly addressed here, any newer provisions issued by the national CAC or industry regulators prevail.

Article 21 — Interpretation, effect and repeal. These Measures are interpreted by the Shanghai CAC and the Shanghai Municipal Data Administration and take **effect on the date of issuance**. The former *Measures for the Administration of the Data-Export Negative List for the China (Shanghai) Pilot FTZ and Lin-gang Special Area (Trial)* and the *China (Shanghai) Pilot FTZ and Lin-gang Special Area Data-Export Management List (Negative List) (2024 Edition)* are **repealed simultaneously**. Data-export activities already lawfully carried out under the former Measures before these took effect **remain valid**.

Part B — Important-Data / Classification Annex

Appended to the Measures is the *Data Classification and Grading Reference Rules for the China (Shanghai) Pilot Free Trade Zone and Lin-gang Special Area and the National Comprehensive Service-Sector Opening-up Pilot Zone (Shanghai)* (数据分类分级参考规则). It is the fallback identification standard invoked by Article 5 where an industry regulator has set no criteria of its own.

Unified Important-Data Identification Reference Rules (重要数据统一识别参考规则) — the quantitative and qualitative triggers:

1. The rules apply to **non-classified data**; classified (state-secret) data follows the applicable secrecy rules.
2. Personal information held by Shanghai enterprises at: **≥ 10 million persons'** personal information (excluding sensitive personal information); **≥ 1 million persons'** sensitive personal information; or **≥ 100,000 persons'** sensitive personal information that includes personal bank accounts, personal insurance accounts, personal registered accounts, personal diagnosis-and-treatment data, and the like.
3. **≥ 100,000 persons'** personal information held by an operator designated by the State as **critical information infrastructure**.
4. High-value sensitive data bearing on industry competitiveness or industry production safety, collected or generated by Shanghai enterprises in R&D and design, production and manufacturing, or operation and management; and enterprise supply-chain data implicating national security.
5. Parameters, and control, operation-and-maintenance and test data, of **automatic control systems** in fields bearing on the national economy and people's livelihood, held by Shanghai enterprises.

Catalogue of reference categories (重要数据识别参考规则) — 13 first-level categories and 40 second-level categories, with representative important data. Several industrial and telecom rows defer to national identification guides (YD/T 4981-2024 for the industrial sector; YD/T 3867-2024 for telecommunications; and, for connected vehicles, the *Guidelines for the Security of Automotive Data Export (2026 ed.)*).

Category (一级类别)	Sub-category (二级类别)	Representative important data
I. Strategic materials & bulk commodities 战略物资和大宗商品类	1. Petroleum, petrochemicals & natural gas 石油、石化和天然气	Storage/trading and international-trade data; product-output and trade data from which the operating status, trends or growth of nationally strategic sectors could be inferred.
	2. Agricultural products 农产品	Strategic-reserve data for bulk farm goods (grain, cotton, edible vegetable oil, sugar, meat, dairy); undisclosed international-cooperation/trade data; biosafety-relevant data on rare/endangered crop, livestock and aquatic germplasm (incl. genes); undisclosed agricultural statistics, inspection/monitoring and quarantine data; geographic data at or above a set precision.
II. Natural resources & environment 自然资源和环境类	3. Geographic information 地理信息	Basic geographic data (positioning base, place-name/address, terrain/landform, geo-entities), remote-sensing imagery and thematic geo-info that reach state-set coverage/precision/scale or depict sensitive areas and targets.
	4. Meteorology 气象	Monitoring, upper-atmosphere, support, regional, radar-base and station-metadata; meteorological monitoring data serving the military, defence research and high-tech fields.
	5. Marine 海洋	Marine eco-environment and resource data; monitoring and disaster-defence data unsuitable for release or of military value.
	6. Environmental protection 环保	Self-monitoring, administrative-penalty and other pollutant-discharge data reflecting discharge levels.
	7. Water conservancy 水利	Flood/drought-defence and engineering-hazard data; undisclosed national water-resource/environment baselines, hydrological observations; precision remote-sensing and digital-twin water data; physical-security status of key water projects.
III. Industry 工业类	8. Steel & non-ferrous metals 钢铁、有色金属	Per YD/T 4981-2024. Non-ferrous reserves/output/procurement of military-civil value; national strategic-reserve data; key geological data of strategic deposits and associated-resource-rich mines.
	9. Rare earths 稀土	Per YD/T 4981-2024. China’s uniquely held rare-earth mining and smelting production-technology data.
	10. Other minerals 其他矿产	Reserves, international-cooperation and trade-negotiation data, mineral-related industrial layout; bulk raw-material information and data able to sway procurement pricing power.
	11. Chemical industry 化学工业	Per YD/T 4981-2024. Key hazardous-chemical monitoring and key-process data held by Shanghai enterprises.
	12. Electric power 电力	Power-plant production, transmission/distribution, construction/O&M, equipment-operation and output/reserve data; civil nuclear R&D test and operation-monitoring data.

Category (一级类别)	Sub-category (二级类别)	Representative important data
	13. Electronic information 电子信息	Per YD/T 4981-2024. Advanced tech, advanced IC design/manufacturing, major computing-equipment design, algorithms and hardware/software architectures, and localisation rates of key electronic components.
	14. Civil nuclear facilities 民用核设施	Experimental/test data from civil nuclear R&D, related design and manufacturing-process information, and operation-monitoring data.
	15. Industrial equipment 工业装备	Per YD/T 4981-2024. R&D and production data for key automotive components bearing on national technological strength (e.g., body-stability control, active-damper systems).
	16. Intelligent connected vehicles 智能网联汽车	Per YD/T 4981-2024 and the Guidelines for the Security of Automotive Data Export (2026 ed.). Autonomous-driving model-training data; set-precision/scale spatiotemporal data covering specific areas from networked vehicle/roadside-device operation.
	17. Other 其他	Per YD/T 4981-2024. Industrial-internet / industrial-control-system security-assurance data used by designated-size industrial enterprises.
IV. National defence science, technology & industry 国防科技工业类	18. National defence S&T industry 国防科技工业	Operation-management, R&D-design, production, test-verification and maintenance data; data reflecting the R&D/production capacity of key defence-industry entities, aggregate data reflecting the sector's overall situation, and sector-specific important data.
V. Telecommunications 电信类	19. Telecommunications 电信	Per YD/T 3867-2024. Construction-planning, performance-parameter, monitoring-analysis, O&M and statistical-analysis data of important network facilities and information systems.
VI. Radio, television & online audiovisual 广播电视和网络视听类	20. Radio and television 广播电视	Undisclosed audiovisual creations; content whose misuse could harm ideological or public security; transmission-coverage data of provincial-and-above broadcasters.
	21. Online audiovisual 网络视听	Monitoring/regulation data; the sector's CII and key-network/system planning, O&M, key-resource and security-assurance data.
VII. Finance 金融类	22. Banking 银行	Bank customer, business, operation-management and system-operation/security data.
	23. Insurance 保险	Insurer customer, business, operation-management and system-operation/security data.
	24. Securities and futures 证券期货	Investor, technical and business data.
	25. Financial leasing 融资租赁	Customer, enterprise-transaction and operation-management data. (Finance-wide: institutional-security information across banking, insurance, securities/futures, leasing and payment/clearing, and business data processed for key entities including defence-industry and national-security-related enterprises.)

Category (一级类别)	Sub-category (二级类别)	Representative important data
VIII. Transportation 交通运输类	26. Transportation 交通运输	Rail, road, road-transport, urban, waterway, civil-aviation and postal data affecting production or supply-chain safety; construction-obtained natural-resource data; 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类	27. Genetic resources 遗传资源	Natural-person gene data and human genetic-resource information reflecting an ethnic group's overall situation or bearing on biosafety.
	28. Health and medical 健康医疗	Medical-service, EMR, e-health-record and research data; diagnosis/treatment data for specific fields/groups/areas or at set precision/scale involving public life, health and safety.
	29. Food 食品	Food-safety traceability-label data; automatic-control-system parameter/control data in food production.
	30. Drugs 药品	Trial data submitted in drug supply and approval; test data on drug-production processes and facilities.
	31. Biosafety 生物安全	Virus-research and bio-laboratory-related data.
	32. Disease control 疾控数据	Data on public-health emergencies and infectious-disease outbreaks, treatment, vaccines and causes of death.
	33. Physical security 物理安全	Building-basic and security-equipment data. (Food/drug/biosafety/disease-control data bearing on national, life and human safety are treated as important.)
X. Public security 公共安全类	34. Cybersecurity 网络安全	Base data on important targets, security equipment and sensitive-site security deployment whose illegal use could seriously harm social stability; CII / important-network planning and secure-operation data.
XI. Internet services & e-commerce 互联网服务和电子商务类	35. Internet platform services 互联网平台服务	Service-generated data usable for social mobilisation; digital-profile data of sensitive groups (e.g., veterans); data recording/tracking military-industry and government clients.
	36. AI services 人工智能服务	AI training data, algorithm source code, key-component data and control programs that could affect national security and the public interest.
XII. Science & technology 科学技术类	37. Intellectual property & major discoveries 知识产权和重大发现	IP involving national defence/security or otherwise undisclosed; research papers, observation data and industrialisation results that markedly enhance or directly affect national security.
	38. Prohibited/restricted export technology 禁止出口限制出口技术	Data on technologies listed in the Catalogue of Technologies Prohibited or Restricted from Export by China.
XIII. Other data 其他数据类	39. Data controlled under the Export Control Law 属于出口管制法管制的相关数据	Data on items on national export-control lists; data controlled under the Export Control Law relating to national security/interest and non-proliferation obligations.
	40. Other national-security-relevant data 其他可能影响国家安全的数据	Other data that could affect security in politics, territory, military, economy, culture, society, S&T, cyber, ecology, resources, nuclear, overseas interests, space, polar, deep-sea, low-altitude or biological domains, and that meets the definition of important data.

Part C — The Negative List: Scope

What the list is. The negative list enumerates the data that — under the Network Data Security Management Regulation, the Data-Export Security Assessment Measures, the Personal Information Standard Contract Measures, the Personal Information Export Certification Measures and the CBDF Provisions — **must still go through** a data-export security assessment, a personal information standard contract, or personal information protection certification. Everything a covered handler exports that is *not* on the list is freed from those three formalities (Article 9). Following the *Overall Plan* and *Accelerating Work Plan* for the service-sector opening-up pilot, the applicable area is now **Shanghai city-wide (全域)**, superseding the Lin-gang 2024 list. **Critical information infrastructure operators (CIIOs) are excluded** from the list and remain under the national regime.

Structure. The list is organised **sector by sector (领域)**, and within each sector into **two tiers**:

- **Tier 1 — security-assessment list (需要通过数据出境安全评估的数据清单):** the higher-volume personal-information bands plus the sector's **important data**.
- **Tier 2 — standard-contract / certification list (需要通过个人信息出境标准合同备案、个人信息保护认证出境的数据清单):** the mid-volume personal-information bands.

Data below the Tier-2 floors is outside the list and flows freely. The sectors set out in the source text are the four below (the published list is broader — the meta figures above reflect the full edition; consult the Chinese original for the complete set).

Sector	Tier 1 — security assessment (重要数据 focus + PI bands)	Tier 2 — standard contract / certification (PI bands)
1. Reinsurance 再保险领域 Scenarios: life-reinsurance & property-reinsurance	Important data: (i) underwriting/claims data that may affect national security; (ii) data on certain sensitive/special units and their individuals; (iii) data whose disclosure could seriously affect economic operation or social stability; (iv) important data determined by the industry regulator. PI (reinsurance scenarios): ≥ 10 million persons' PI (excl. sensitive); or ≥ 1 million persons' sensitive PI. Other PI: ≥ 1 million persons' PI (excl. sensitive); or ≥ 10,000 persons' sensitive PI.	PI (reinsurance scenarios): ≥ 1 million and < 10 million persons' PI (excl. sensitive); or ≥ 10,000 and < 1 million persons' sensitive PI. Other PI: ≥ 100,000 and < 1 million persons' PI (excl. sensitive); or < 10,000 persons' sensitive PI.
2. International shipping 国际航运领域 Scenarios: water-transport services & port operations; crew management	Important data (water-transport & port operations): basic geographic information; port facility/equipment data; port system-operation & security data; port operation data; port business-management data; water-transport service data. PI (crew management): ≥ 150,000 persons' crew sensitive PI. Other PI: ≥ 1 million persons' PI (excl. sensitive); or ≥ 10,000 persons' sensitive PI.	PI (crew management): ≥ 150,000 and < 1 million persons' crew PI (excl. sensitive); or ≥ 10,000 and < 150,000 persons' crew sensitive PI. Other PI: ≥ 100,000 and < 1 million persons' PI (excl. sensitive); or < 10,000 persons' sensitive PI.
3. Commerce — retail & catering, accommodation 商贸领域 (零售与餐饮业、住宿业) Scenario: membership management	No important data — this sector is personal-information only. PI (membership management): ≥ 10 million persons' PI (excl. sensitive); or ≥ 1 million persons' sensitive PI. Other PI: ≥ 1 million persons' PI (excl. sensitive); or ≥ 10,000 persons' sensitive PI.	PI (membership management): ≥ 1 million and < 10 million persons' PI (excl. sensitive); or ≥ 100,000 and < 1 million persons' sensitive PI. Other PI: ≥ 100,000 and < 1 million persons' PI (excl.

Sector	Tier 1 — security assessment (重要数据 focus + PI bands)	Tier 2 — standard contract / certification (PI bands)
		sensitive); or < 10,000 persons' sensitive PI.
4. Meteorology 气象领域 Scenario: sharing / exchange / service of meteorological data	Important data: (i) meteorological data reaching state-set scale or precision, or usable to cause an environmental-security incident, or serving the military, defence research, high-tech or disaster-prevention fields; (ii) AI datasets formed from category-(i) data — excluding datasets that do not depict meteorological conditions within PRC territory or jurisdiction, and meteorological models and model-inferred datasets. No PI bands.	None — meteorology has a Tier-1 (security-assessment) list only.

Counting rule for personal information. Volumes are counted on a **de-duplicated, per-natural-person** basis. Transfers falling within CBDF Provisions Article 3, Article 4, and Article 5(1)(i) – (iii) are **excluded** from the cumulative count; for the residual “other PI” bands, Article 6 transfers are excluded as well. All cumulative counts run **from 1 January of the current year** (自当年 1 月 1 日起).

Sector carve-outs. In international shipping, **national core data** — such as national natural-resource and basic geographic-information data affecting national security — is **not** within the scope of permitted cross-border flow, notwithstanding the sector list. Across all sectors, export-controlled technical materials remain governed by the Export Control Law and Foreign Trade Law (Measures, Article 20).

Source: 中国（上海）自由贸易试验区及临港新片区、国家服务业扩大开放综合试点地区（上海）数据出境管理清单（负面清单）（2025版） and its administrative measures, issued by Shanghai CAC · Shanghai Municipal Data Administration, April 29, 2026. Chinese originals downloadable at datacompliancechina.com/resources/negative-lists.

Prepared by Data Compliance China — *the careful translator*. **Not legal advice.** The Chinese original controls.