Fujian FTZ Data-Export Negative List (2025)

DCC working English reference — measures and list scope. 中国（福建）自由贸易试验区数据出境管理清单（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	Fujian 福建 — Free Trade Zone
VERSION	2025 edition
ISSUED	December 18, 2025
ISSUERS	Fujian CAC · Provincial Commerce Dept · Provincial 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	4 sectors · 26 scenarios · 298 data fields
MODEL	Pre-export filing (3-year validity)

Part A — Administrative Measures (Trial)

Administrative Measures for the Data-Export Negative List of the China (Fujian) Pilot Free Trade Zone (Trial) — 中国（福建）自由贸易试验区数据出境负面清单管理办法（试行）. Six chapters, twenty-four articles.

Chapter 1 — General Provisions

Purpose and legal basis (Art. 1). The Measures are enacted to safeguard data security, protect personal-information rights and interests, raise the data-export management capacity and service level of the China (Fujian) Pilot Free Trade Zone (the "Fujian FTZ"), and promote efficient, convenient and secure cross-border data flows. They rest on the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, the Network Data Security Management Regulation, and the Cyberspace Administration of China's *Provisions on Promoting and Regulating Cross-Border Data Flows* (CBDF Provisions).

Scope (Art. 2). The Measures govern the formulation, execution and management of the data-export negative list within the Fujian FTZ.

Principles (Art. 3). Four principles guide the list: - **Hold the security baseline** — comply with law, build a data-security coordination mechanism and management system, strengthen technical safeguards, and promote lawful, orderly, free data flow only on the premise that data security is protected. - **Promote development** — give full weight to data handlers' reasonable and necessary export needs, scientifically scope what must go on the list, build a facilitated cross-border-flow model, cut enterprises' export-compliance costs, and release data value. - **Advance by category** — following the classification-and-grading requirements of the relevant national industry authorities and regulators, formulate the list in batches, industry by industry and sector by sector. - **Manage dynamically** — track and assess implementation and security risk, and adjust the list's content as the national data-security picture, handlers' actual needs, and the governing law and policy change.

Chapter 2 — Responsibilities and Division of Labour

Provincial-level administrative authorities (Art. 4). The Fujian Provincial Cyberspace Administration (Fujian CAC), the Provincial Data Administration, the Provincial Department of Commerce (FTZ Office), the Provincial Public Security Department and the Provincial State Security Department are together the "provincial-level administrative authorities." They build the FTZ's negative-list management system and coordinate related matters; guide and supervise cross-border data-flow activity; organise formulation of the list by industry, sector and batch; run the reporting-review and filing procedures; establish the dynamic-management mechanism; and, with the provincial-level industry regulators, strengthen supervision and inspection of implementation.

Provincial units for industry, telecommunications, transport, finance, natural resources, health, education, science and technology and the like are together the "provincial-level industry authorities and regulators." They draft classification-and-guidance rules for their industry or sector, guide identification of that sector's important data, assist in formulating the negative list, and carry the sector's data-security regulatory responsibility.

Area implementing agencies (Art. 5). The management committees of the Fuzhou, Xiamen and Pingtan areas of the Fujian FTZ and the relevant local functional departments are together the "area implementing agencies." They set up the area's negative-list working mechanism; help the provincial authorities formulate the list and issue its supporting implementation guide; define who may use the list and the application process; build and improve export supervision-and-service platforms; guide compliant use of the list by data handlers in the area; and run whole-chain pre-, during- and post-event supervision.

Data handler defined (Art. 6). A "data handler" (数据处理者) is an enterprise, public institution, organisation, association or other entity registered within the Fujian FTZ that carries out cross-border data-flow and related activity. Data handlers must identify and declare important data as required, conduct exports per each area's requirements, and cooperate with the authorities and area agencies in follow-up verification and inspection.

Chapter 3 — Formulation and Management of the Negative List

Formulation workflow (Art. 7). Five stages: (i) **needs research** — survey exportable data across the key industries by business scenario, category, volume and field; (ii) **important-data identification** — under the provincial data-security coordination mechanism, set identification criteria, classify and grade data, form the Fujian FTZ important-data catalogue, and file it with the Office of the National Data Security Work Coordination Mechanism (where an industry authority has published classification-and-grading standards, those govern; otherwise the *China (Fujian) FTZ Data Classification-and-Grading Reference Rule* applies — see Part B); (iii) **business-scenario analysis** — for scenarios with urgent, frequent export needs, analyse export scale, scope and frequency and set data items and volume tiers for risk-controllable scenarios; (iv) **demonstration and consultation** — expert review plus consultation of industry authorities, functional departments and key enterprises; (v) **approval and filing** — once the industry regulators unanimously agree, the list is approved by the Provincial Party Committee's Cybersecurity and Informatization Commission, jointly filed by Fujian CAC and the Provincial Data Administration with the national CAC and national Data Administration, then issued jointly in the name of Fujian CAC, the Provincial Data Administration and the Provincial Department of Commerce (FTZ Office).

What the list must contain — the two tiers (Art. 8). The list must cover at least: - **Tier 1 — data requiring a data-export security assessment:** (1) a critical information infrastructure operator (CIIO) providing personal information or important data abroad; and (2) a non-CIIO data handler providing important data abroad, or providing personal information abroad that reaches the list's threshold for declaring a security assessment. - **Tier 2 — data requiring a personal-information standard contract filing or personal-information-protection certification:** a non-CIIO data handler providing personal information abroad that reaches the list's threshold for concluding a personal-information standard contract or obtaining certification.

Dynamic management (Art. 9). The provincial administrative authorities and industry authorities track and assess each issued list's implementation and risk and coordinate revisions; for industries or sectors not yet covered, they assess actual export need and develop the corresponding list, continually completing the FTZ's cross-border-flow policy system.

Chapter 4 — Implementation of the Negative List

Self-assessment first; off-list is exempt (Art. 10). Before exporting, a data handler self-determines whether the FTZ negative list applies. In an industry or sector where a list has been published, exporting data that is **off** the list is exempt from a security assessment, a personal-information standard contract, and certification.

The filing process (Art. 11). To export data using the list, a handler must, before export: (i) **apply** to the relevant FTZ area per that area's implementation guide, stating place of registration, industry, business situation, and any administrative penalties or regulator investigations/rectifications in the past 2 years; (ii) **file**, after passing review, submitting the export business scenario, export-data catalogue, export-data scale, overseas recipient, the reason the data falls under the list, and the applicable list sub-categories; (iii) **export in compliance**, per the assessment opinion issued by the area, cooperating with supervision and verification.

Area review timelines (Art. 12). Each FTZ area (i) reviews the application per its implementation guide and notifies the handler in writing **within 5 working days**, then assists successful applicants in filing; (ii) **within 5 working days** of the filing, issues an opinion on whether the export data falls within the list, files that opinion with the provincial authorities, and reports back to the handler — where the data is **on** the list, guiding the handler to a security assessment, standard contract or certification; where **off** the list, confirming it may flow "safely and in an orderly manner" under the guide; where the list does not apply, current law governs; and (iii) provides consultation and keeps improving export-facilitation measures.

Validity, renewal and change (Art. 13). An approved list-application is valid for **3 years** from the date the review opinion issues. To keep using the list past expiry with no material change to the export data, the handler applies for renewal **within 60 working days before expiry**. A **material change** — in export purpose, method or scope; a large increase in export volume; a material change of overseas recipient; or a change in the legal documents between handler and recipient that could affect export-data security — requires a fresh application and filing under Article 11. A non-material change may be registered through a simplified change process.

Chapter 5 — Supervision and Management

Provincial oversight (Art. 14). The provincial authorities enforce national and industry data-security requirements, build mechanisms for information-sharing, risk assessment and security-incident notification, develop monitoring and early-warning capacity, and run whole-chain supervision of list use.

Incident duty (Art. 15). Handlers must cooperate with supervision and verification; on a data-export security incident or a rising export-security risk, they must take remedial measures and report immediately to the area implementing agency, which reports up to the provincial authorities.

Consistency spot-checks and penalties (Art. 16). The area implementing agency has professional technical bodies conduct **consistency spot-checks** between the actual export and the filing. A handler that breaks its commitments, or conceals, misreports or deliberately creates inconsistency between actual and filed data, may be ordered to **suspend** exports and rectify within a deadline, then re-run the application and filing; in serious cases exports are **terminated** and key-supervision measures imposed, with a report to the provincial authorities. Refusal to correct, or serious consequences, draws liability under law.

Reporting and tiered supervision (Art. 17). Area agencies report implementation and export activity to the provincial authorities **every six months**; the provincial authorities and industry regulators periodically inspect and assess area

agencies and handlers. Significant risk triggers immediate remediation, and export data affecting or potentially affecting national security is promptly added to the list. On suspected criminal leads, the Provincial Public Security and State Security Departments act within their remits.

Innovation encouraged (Arts. 18 – 19). Area agencies are encouraged to build credit-evaluation and self-conformity-declaration mechanisms, and to pilot new governance models around traceability, key-scenario security-governance standards, and key-scenario security-liability definition.

Chapter 6 — Supplementary Provisions

National core data excluded (Art. 20). Data bearing on national security, the lifelines of the national economy, major aspects of people's livelihood or major public interest is **national core data**, subject to a stricter regime and **not** managed through the negative list.

Reference rules for uncovered sectors (Art. 21). For industries or sectors the Measures do not address, national classification-and-grading provisions and standards apply.

Export-control carve-out and residual law (Art. 22). Where a covered industry or sector involves technical materials on controlled items under the *Export Control Law*, or technology-export matters under the *Foreign Trade Law*, those statutes govern. Export data in industries or sectors not covered by the list and guide follows national rules (the Network Data Security Management Regulation, the Security Assessment Measures, the Standard Contract Measures, the CBDF Provisions, etc.). International conventions, bilateral/multilateral treaties, and arrangements with Hong Kong, Macao and Taiwan govern where they provide otherwise. **The Fujian FTZ may also refer to and apply data-export negative lists officially issued by other pilot FTZs and free-trade ports** — i.e., other zones' lists are mutually referenceable within Fujian.

Interpretation and effect (Arts. 23 – 24). The Measures are interpreted by Fujian CAC together with the Provincial Data Administration, the Provincial Department of Commerce (FTZ Office), and the Provincial Public Security and State Security Departments. They take effect on issuance, for a **two-year trial period**. (Being the inaugural trial edition, the Measures contain no repeal of any prior version.)

Part B — Important-Data / Classification Annex

The Measures append the *China (Fujian) FTZ Data Classification-and-Grading Reference Rule* （中国（福建）自由贸易试验区数据分类分级参考规则）, used to identify important data where no sector-specific standard exists.

Unified important-data identification reference rule. The rule applies to non-classified data (state-secret data follows separate rules). Data is treated as **important data** where a Fujian FTZ enterprise holds any of: - personal information of 10,000,000+ persons (excluding sensitive personal information); - sensitive personal information of 1,000,000+ persons; - sensitive personal information of 100,000+ persons that includes personal bank accounts, personal insurance accounts, personal registered accounts, personal diagnosis-and-treatment data, and the like; - (for a CIIO) personal information of 100,000+ persons; - high-value sensitive data tied to industry competitiveness or production safety, collected or generated in R&D, manufacturing or operations, and enterprise supply-chain data bearing on national security; or - automatic-control-system parameters and control, operation-maintenance and testing data in fields bearing on the national economy and people's livelihood.

Catalogue — 13 categories, 40 sub-categories. Representative important data by category (summarised for scope):

Category (一级类别)	Sub-categories (二级类别)	Representative important data
Strategic materials & bulk commodities 战略物资和大宗商品类	1. Petroleum, petrochemicals & natural gas	Output and international-trade data from which the operating state, trend or growth of nationally strategic sectors could be inferred; undisclosed strategic-reserve, international-cooperation and trade data for staple farm goods;

Category (一级类别)	Sub-categories (二级类别)	Representative important data
	2. Agricultural products	germplasm (incl. genetic) resource data affecting biosafety; undisclosed agricultural statistics, inspection and quarantine data; geographic data at defined precision.
Natural resources & environment 自然资源和环境类	3. Geographic information 4. Meteorology 5. Ocean/marine 6. Environmental protection 7. Water conservancy	Basic, remote-sensing and thematic geographic data meeting national coverage/precision/currency/scale thresholds or depicting sensitive areas or targets; meteorological monitoring serving military, defence-research or high-tech uses; militarily valuable marine-environment and disaster-defence data unfit for release; flood/drought-defence business data, undisclosed water-resource and hydrological data, digital-twin water spatial data, key water-project physical-security data.
Industry 工业类	8. Steel & nonferrous metals 9. Rare earths 10. Other minerals 11. Chemical industry 12. Electric power 13. Electronic information 14. Civil nuclear facilities 15. Industrial equipment 16. Intelligent connected vehicles 17. Others	Largely identified per the 《工业领域重要数据识别指南》 (Industrial-Sector Important-Data Identification Guide, YD/T 4981-2024). Includes nonferrous-metal reserves/output and steel & nonferrous strategic reserves; China's uniquely held rare-earth mining/smelting technology; bulk-raw-material and pricing-power data; key hazardous-chemical monitoring, process and output data; civil-nuclear R&D and operation-monitoring data; advanced electronic-information, IC design/manufacturing and key-component localisation data; automotive key-component R&D and autonomous-driving model-training data; industrial-internet / control-system security-operation data.
National-defence science, technology & industry 国防科技工业类	18. National-defence sci-tech industry	Management, R&D-design, manufacturing, test-verification and maintenance data bearing on military, economic, technological and network security; data reflecting key defence-industry entities' R&D and production capacity, or — when aggregated — the sector as a whole.
Telecommunications 电信类	19. Telecommunications	Identified per the 《电信领域重要数据识别指南》 (Telecom-Sector Guide, YD/T 3867-2024): planning, performance-parameter, monitoring/analysis, operation-maintenance and statistical data of important network facilities and information systems.
Radio, TV & online audiovisual 广播电视和网络视听类	20. Radio and television 21. Online audiovisual	Undisclosed audiovisual content, or content whose misuse could endanger ideological or public security; transmission-coverage data of provincial-and-above broadcasters; broadcast monitoring/regulation data; sector CII and important-network planning, operation-maintenance and security data.
Finance 金融类	22. Banking 23. Insurance 24. Securities & futures 25. Financial leasing	Institutional security data of banks, insurers, securities/futures firms and leasing companies; business data they process for key entities, including defence-industry and national-security-related enterprises.
Transport 交通运输类	26. Transport	Across rail, road, road-transport, urban, waterway, civil-aviation and postal: control-class data affecting production safety; natural-resource data obtained during construction; undisclosed route maps and key-node data; data whose leak or tampering could cause a major transport accident.

Category (一级类别)	Sub-categories (二级类别)	Representative important data
Health & food/drug 卫生健康和食品药品类	27. Genetic resources 28. Health & medical 29. Food 30. Drugs 31. Biosafety 32. Disease control	Genetic-resource data reflecting a race as a whole or bearing on biosafety; food, drug, biosafety and disease-control data bearing on national, life and human safety; medical diagnosis-and-treatment data on public life, health and safety for specific fields, groups or regions at defined precision and scale.
Public security 公共安全类	33. Physical security 34. Cybersecurity	Important-target base data, security-equipment data and sensitive-site security-deployment data whose unlawful use could seriously harm social stability; CII or important-network planning and secure-operation data.
Internet services & e-commerce 互联网服务和电子商务类	35. Internet platform services 36. AI services	Data usable for social mobilisation; digital-portrait data of sensitive groups (e.g., veterans); records or tracking of military-industrial or government clients; AI training data, algorithm source code, key-component data and control programs that could affect national security or public interest.
Science & technology 科学技术类	37. Intellectual property & major discoveries 38. Prohibited/restricted export technologies	IP relating to national defence or security; research papers, observation data and industrialisation results that markedly enhance national-security capability; data relating to technologies in the 《中国禁止出口限制出口技术目录》 (Catalogue of Technologies Prohibited or Restricted from Export in China).
Other data 其他数据类	39. Data controlled under the Export Control Law 40. Other national-security-affecting data	Data on items on the national export-control list; other data meeting the important-data definition that may affect national political, territorial, military, economic, cultural, social, technological, network, ecological, resource, nuclear, overseas-interest, space, polar, deep-sea or biological security.

Part C — The Negative List: Scope

China (Fujian) FTZ Data-Export Management List (Negative List) (2025 edition) — 中国（福建）自由贸易试验区数据出境管理清单（负面清单）（2025版）. It binds data handlers registered in, and exporting from, the Fujian FTZ. Data in a covered sector that is **off** the list may be exported without a security assessment, standard contract or certification; data in sectors the list does not reach follows the ordinary national regime.

Structure. The list is organised **by industry/sector → by business scenario → by data category** (important data vs. personal information), with items grouped into export-pathway tiers:

- **Tier 1 — data requiring a data-export security assessment.** Captures CIIO exports of personal information or important data, and non-CIIO exports of important data or of personal information at/above the stated (higher) thresholds.
- **Tier 2 — data requiring a personal-information standard contract filing or personal-information-protection certification.** Captures non-CIIO exports of personal information within the stated (lower) bands.
- The pharmaceutical sector adds a third bucket — **data requiring other lawful/compliant paths** — for genetic information.

Counting rule. Personal-information volumes are counted as a **de-duplicated statistic per natural person**, cumulative **from January 1 of the current year**. Volumes falling under the CBDF Provisions Arts. 3, 4, 5(1)(i) – (iii) and 6 are **excluded** from the cumulative count.

Sector	Tier 1 — Security assessment (important-data focus + PI thresholds at/above which assessment is required)	Tier 2 — Standard contract / certification (PI bands)
Pharmaceuticals & medicine 医药行业 (chemical APIs & formulations, biologics, medical-device makers; excludes non-drug lines)	**Important data:** group diagnosis/treatment, health-physiology, medical-rescue and specific-drug trial/special-disease data on 100,000+ persons; medical-resource and biometric data on 10,000+ in specific fields/groups/regions; undisclosed frontier-biotech drug-production and other specific-drug trial/production data; drug safety/efficacy/quality research data; undisclosed medical-device manufacturing/operation data; export-controlled data. **Personal information (per scenario):** trial subjects 10,000+ (clinical trials/DCT/R&D); patients 50,000+ (pharmacovigilance/complaints/inquiry); healthcare-professional-type PI 200,000+ (non-sensitive) or 100,000+ (sensitive); patient physiology / under-14 minors 100,000+ (device after-sales); medical-business contacts 100,000+ (sensitive); catch-all 1,000,000+ (non-sensitive) or 10,000+ (sensitive).	Trial subjects 5,000 – <10,000; patients 10,000 – <50,000; healthcare-professional-type PI 10,000 – <200,000 (non-sensitive) or 10,000 – <100,000 (sensitive); patient physiology / under-14 minors <100,000; medical-business contacts <100,000 (sensitive); catch-all 100,000 – <1,000,000 (non-sensitive) or <10,000 (sensitive).
Internet of Vehicles (connected vehicles) 车联网行业 (automakers, parts/software suppliers, dealers, repairers, mobility firms; excludes autonomous driving)	**Important data (12 categories):** geo/people-flow/vehicle-flow data of sensitive areas (military zones, defence-industry units, county-level+ Party/government organs) and important civil facilities; undisclosed data from serving government/military/sensitive institutions; traffic/logistics data reflecting economic operation; regional EV-charging-network data; off-vehicle video/images bearing faces, plates or road signs; key IoV service data incl. remote vehicle control; map data at defined precision/scale/coverage (10,000+ vehicles or provincial road mileage); scenario-library data; supply-chain-attack (APT) data; transport/IoV CII cyber-protection data; core-tech / export-control / strategic-reserve / military-strike-relevant data; and IoV important data recognised by industry authorities. **Personal information:** 1,000,000+ (non-sensitive); 10,000+ sensitive PI — all scenarios.	100,000 – <1,000,000 (non-sensitive); <10,000 sensitive PI — all scenarios.
Retail 零售行业 (consumer retail, lodging, catering, software/IT & internet-information services; membership scenarios only)	**No important data listed — personal information only.** Consumer-member PI 3,000,000+ (non-sensitive) or 500,000+ (sensitive), membership-management scenario; catch-all 1,000,000+ (non-sensitive) or 10,000+ (sensitive), other scenarios.	Consumer-member PI 500,000 – <3,000,000 (non-sensitive) or 100,000 – <500,000 (sensitive), membership; catch-all 100,000 – <1,000,000 (non-sensitive) or <10,000 (sensitive), other scenarios.

Sector	Tier 1 — Security assessment (important-data focus + PI thresholds at/above which assessment is required)	Tier 2 — Standard contract / certification (PI bands)
Aircraft maintenance 航空维修行业 (civil-aircraft & equipment maintenance/repair; excludes aircraft manufacturing and non-civil maintenance)	**Important data (6 categories):** flight-data-recorder (FDR) data from civil-aircraft accidents; cockpit-voice-recorder (CVR) data from accidents; aircraft health-monitoring data; core design principles, processes, methods, schemes, key parameters, experimental data and test reports bearing on tech strength/competitiveness; aggregated/mined multi-dimensional supply-chain data reaching greater scale/depth; export-controlled data. **Personal information:** supplier/customer/dealer/partner PI 1,000,000+ (non-sensitive) or 50,000+ (sensitive), business-cooperation scenario; catch-all 1,000,000+ (non-sensitive) or 10,000+ (sensitive), all scenarios.	Supplier/customer/dealer/partner PI 100,000 – <1,000,000 (non-sensitive) or 10,000 – <50,000 (sensitive), business-cooperation; catch-all 100,000 – <1,000,000 (non-sensitive) or <10,000 (sensitive), all scenarios.

Pharmaceutical third bucket — other lawful paths. Genetic information, and gene data reaching the scale or precision set by the relevant national authorities, apply in **all scenarios**: human gene and genome data derived from human genetic-resource material (excluding clinical, imaging, protein and metabolic data). Exports that have already discharged the "administrative licensing and filing" duties of Chapter IV of the *Implementing Rules for the Regulation on the Administration of Human Genetic Resources* are exempt.

Sector notes. *Pharma:* "trial subjects" include patients and healthy volunteers in a clinical trial; "patients" here are those experiencing an adverse drug reaction in pharmacovigilance; race coding follows the E2B(R3) regional guide. *IoV:* covers connected-vehicle information-service handlers, not autonomous driving; sensitive-area collection needs prior approval; PI excludes anonymised data. *Retail:* only the personal information collected/used in membership-management scenarios is in scope. *Aircraft maintenance:* covers civil-aircraft maintenance/repair only.

Source: 中国（福建）自由贸易试验区数据出境管理清单（负面清单）（2025版） and its administrative measures, issued by Fujian CAC · Provincial Commerce Dept · Provincial Data Administration, December 18, 2025. Chinese originals downloadable at datacompliancechina.com/resources/negative-lists.

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