Guangdong FTZ Data-Export Negative List (2025)

DCC working English reference — measures and list scope. 中国（广东）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	Guangdong 广东 — Free Trade Zone
VERSION	2025 edition
ISSUED	May 2026
ISSUERS	Guangdong CAC · Provincial Commerce Dept · Government Services and 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	2 sectors · 7 scenarios · 67 data fields
MODEL	Post-export reporting (先用后报 / use-first, report-after)

Part A — Administrative Measures (Trial)

Full title: 中国（广东）自由贸易试验区数据出境负面清单管理办法（试行） — Administrative Measures for the Data-Export Negative List of the China (Guangdong) Free Trade Zone (Trial). Six chapters, 26 articles, plus one annex (translated as Part B below).

Chapter 1 — General Provisions (总则)

Article 1 (Purpose and basis). These Measures are formulated to safeguard national data security, protect personal-information rights and interests, enhance the data-export (数据出境, outbound-transfer) management capacity and facilitation level of the China (Guangdong) Free Trade Zone ("Guangdong FTZ") and the Shenzhen Park of the Hetao Shenzhen – Hong Kong Science and Technology Innovation Cooperation Zone ("Hetao Shenzhen Park"), and to promote efficient, convenient and secure cross-border data flows — 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 (CBDF Provisions), the Guangdong Digital Economy Promotion Regulation, and other applicable laws, regulations and rules.

Article 2 (Scope). These Measures apply to activities of formulating, approving, and use-managing the data-export negative list (负面清单) within the Guangdong FTZ and the Hetao Shenzhen Park.

Article 3 (Principles). Negative-list management adheres to three principles:

1. **Hold the security bottom line (坚持安全底线).** Comply with laws and regulations, build sound security-management mechanisms and technical safeguards, and promote lawful, orderly data flows on the premise of data security.
2. **Support industrial development (助力产业发展).** Give full weight to data handlers' real data-export needs, define the scope of data placed on the negative list scientifically and reasonably, maximise convenience for data-export

activities, and promote cross-border business.

3. **Batch-and-category management (分批分类管理).** The negative list is formulated in batches by industry and sector. Its data items are managed by category and, by degree of sensitivity, divided into: data subject to the **data-export security assessment (数据出境安全评估)**, and data subject to **personal information export standard-contract filing (备案)** or **personal information protection certification (个人信息保护认证)**.

Chapter 2 — Responsibilities and Division of Labour (职责及分工)

Article 4 (Provincial-level administrative authorities). In accordance with the national cross-border data-transfer security-management system, the Guangdong Cyberspace Administration (广东省互联网信息办公室, Guangdong CAC), the Guangdong Provincial Commerce Department, the Guangdong Provincial Government Services and Data Administration, the Guangdong Provincial Public Security Department, and the Guangdong Provincial State Security Department (collectively, the "provincial-level administrative authorities" / 省级管理部门) are responsible for: establishing and coordinating the negative-list management system for the Guangdong FTZ and Hetao Shenzhen Park; guiding and supervising cross-border data-flow activities in those zones; organising negative-list formulation by industry, sector and batch; carrying out the reporting-for-approval and filing procedures; and establishing a dynamic-management mechanism for the negative list.

Article 5 (Regional administrative agencies). The management committees of the Nansha and Qianhai-Shekou areas of the Guangdong FTZ, the Guangdong Provincial Government's Office for the Guangdong-Macao In-Depth Cooperation Zone in Hengqin and the Executive Committee of that Cooperation Zone, and the Hetao Shenzhen Park Development Bureau (collectively, the "regional administrative agencies" / 区域管理机构) are responsible for: organising compliant use of the negative list by data handlers in their respective zones; formulating and issuing supporting implementation guidelines and management rules; guiding data handlers in the lawful use of the negative list; strengthening tracking and supervision of data-export activities; and building in-process evidence-retention and post-hoc supervisory capacity. The relevant implementation guidelines and management rules are issued and implemented **after filing (备案) with the provincial-level administrative authorities**.

Article 6 (Definition of data handler). For these Measures, a **data handler (数据处理者)** is an enterprise, public institution, organisation, group, other organisation or individual registered within the Guangdong FTZ and Hetao Shenzhen Park that conducts cross-border data-flow and related activities. A data handler must identify and declare important data (重要数据) in accordance with the relevant provisions; **where data has not been notified, or publicly released, as important data by the relevant authority or region, the data handler need not declare it as important data for the data-export security assessment.** Data handlers must conduct data-export activities in accordance with the regional administrative agencies' requirements and cooperate with the provincial-level authorities and the regional agencies in tracking-verification and supervision-inspection.

Chapter 3 — Formulation and Management of the Negative List (负面清单制定及管理)

Article 7 (Formulation workflow). Formulating the negative list mainly comprises five steps:

1. **Needs research (需求调研).** Focusing on the industrial development and real data-handler needs of the two zones, select priority industries and sectors for research, and survey the actual outbound-data situation across business scenarios, categories, volumes and fields, as the basis for the list.
2. **Important-data identification (重要数据识别).** Under the coordination of the provincial data-security work coordination mechanism, the provincial-level authorities set important-data identification standards pursuant to the Data Security Law and related law, classify and grade data, form the **Important-Data Catalogue of the Guangdong FTZ and Hetao Shenzhen Park**, and file it, per procedure, with the office of the national data-security work coordination mechanism. Where an industry regulator has published — or issued within its industry — data classification-and-grading standards, important data is identified under those first; where a regulator has set no

clear standard, important data is identified under the **China (Guangdong) FTZ Data Classification and Grading Reference Rule** (translated in Part B).

3. **Business-scenario analysis (业务场景分析).** Combining the research and important-data-identification results, select business scenarios with urgent export demand and frequent flows, analyse the scale, scope and frequency of export, and reasonably set data items and volume thresholds for risk-controllable export scenarios.
4. **Demonstration and consultation (论证与征求意见).** Invite experts in the relevant industry, law and data security to review and validate the draft, seek the views of provincial industry regulators and relevant functional departments, and revise accordingly.
5. **Approval and filing procedures (履行审批报备流程).** The negative list, after review and clearance by the Guangdong data-security work coordination mechanism, is submitted for approval to the Cybersecurity and Informatization Commission of the CPC Guangdong Provincial Committee, and is then jointly filed by the Guangdong CAC and the Guangdong Provincial Government Services and Data Administration with the national cyberspace administration (国家网信部门) and the national data administration (国家数据管理部门).

Article 8 (Required contents — the two tiers). The negative list must contain at least the following two parts:

1. **Data requiring the data-export security assessment (Tier 1)**, chiefly:
   - a critical information infrastructure operator (CIIO / 关键信息基础设施运营者) providing personal information or important data abroad; and
   - a data handler other than a CIIO providing important data abroad, or providing personal information abroad that reaches the negative-list threshold for declaring a data-export security assessment.
2. **Data requiring personal information export standard-contract filing or personal information protection certification (Tier 2)**, chiefly:
   - a data handler other than a CIIO providing personal information abroad that reaches the negative-list threshold for concluding a personal information export standard contract or obtaining personal information protection certification.

Article 9 (Dynamic management). The negative list is managed dynamically. For lists already issued, the provincial-level authorities track and evaluate implementation and security risk and coordinate revisions. For industries and sectors not yet covered by a list, they promptly assess actual export demand and research and formulate the corresponding list, continually improving the two zones' cross-border data-flow policy framework.

Chapter 4 — Implementation of the Negative List (负面清单实施)

Article 10 (Self-identification and the on-list / off-list test). Before conducting a data-export activity, a data handler must, on its own, identify and determine the type and quantity of the outbound data and assess whether it falls within the negative list.

- Where the outbound data falls within an industry or sector listed on the negative list **and, on assessment, is within the list**, the handler must — as the list requires — declare a data-export security assessment, conclude a personal information export standard contract, or obtain personal information protection certification.
- Where the outbound data falls within a listed industry or sector but is **not within the list**, it may be exempted from those three mechanisms.
- Where the outbound data does **not** fall within any industry or sector listed on the negative list, it is handled under the applicable national rules — the Network Data Security Management Regulation, the Data Export Security Assessment Measures, the Measures on the Standard Contract for Personal Information Export, the CBDF Provisions, and the like.

Article 11 (Reporting to the regional agency). A data handler that uses the negative list to conduct data-export activities must promptly report the export to its regional administrative agency, including but not limited to the export business scenario, the outbound-data catalogue, the export scale, and the overseas recipient. Where the export situation changes, the change must be reported promptly.

Article 12 (Security-safeguard obligations). In transferring important data and personal information abroad, a data handler must comply with laws and regulations, perform its data-security-protection duties, and take technical and other necessary measures to secure the export. On the occurrence of a data-export security incident, or on finding that data-export security risk has increased, it must take remedial measures and promptly report to the provincial-level authorities and the regional administrative agency.

Article 13 (Guidance and liaison service). Each regional administrative agency strengthens guidance and supervision of data handlers' export activities, establishes a liaison-service mechanism with data handlers using the negative list, dynamically gathers their export needs, hears their views on using the list, and — in light of the overall cross-border-flow situation — continually optimises the zone's data-export facilitation measures.

Chapter 5 — Supervision and Administration (监督管理)

Article 14 (Whole-chain provincial supervision). The provincial-level authorities strictly implement national and industry data-security requirements, strengthen guidance and supervision of export activities in the two zones, build risk-assessment and incident-discovery/notification mechanisms, coordinate the build-out of security-risk monitoring and early-warning capacity, and reinforce comprehensive before-, during- and after-the-fact supervision across the whole chain and all sectors of negative-list use.

Article 15 (Consistency spot-checks and penalties). Each regional administrative agency must formulate specific management rules and engage professional technical bodies to conduct **consistency spot-checks (一致性抽验)** between actual data exports and the situation the handler reported. Where a data handler fails strictly to honour its commitments in export activities, or engages in concealment, false reporting, or deliberately causing actual exports to diverge from what was reported, the regional agency may order it to suspend export activities and rectify within a set period; in serious cases, it terminates the handler's export activities, subjects it to **key-supervision measures (重点监管)**, and promptly reports to the provincial-level authorities. Regional agencies are supported in building one-stop cross-border data-service platforms with declaration-service, compliance-coaching and security-supervision functions, so as to build a "controllable yet open" (管得住、放得开) supervisory-service system.

Article 16 (Inspection, evaluation and referral). The provincial-level authorities, together with industry regulators, periodically inspect and evaluate how regional agencies and data handlers implement these Measures. On finding that data-processing activities carry significant security risk, they must immediately take remedial measures and eliminate hazards; for outbound data that affects or may affect national security, they promptly update the negative list to include it. On finding leads suggesting an offence or crime, they promptly notify the Guangdong Provincial Public Security Department and the Guangdong Provincial State Security Department, which — under the applicable laws and administrative regulations and within their respective remits — prevent and combat unlawful and criminal activities that endanger data-export security.

Article 17 (Legal liability). Where a data handler violates these Measures and the national data-export security-management rules by exporting data in breach, the competent authority pursues its legal liability under the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, the Network Data Security Management Regulation, and other applicable law.

Chapter 6 — Supplementary Provisions (附则)

Article 18 (Interpretation). These Measures are interpreted by the Guangdong CAC together with the Guangdong Provincial Commerce Department, the Government Services and Data Administration, the Public Security

Department, and the State Security Department.

Article 19 (Uncovered sectors). For industries and sectors not addressed by these Measures, data classification-and-grading reference rules follow the relevant provisions and standards.

Article 20 (Export-control carve-out). Where an industry or sector on the negative list involves the export of technical materials for controlled items under the Export Control Law, or technology-export matters under the Foreign Trade Law, such export is handled under the Export Control Law, the Foreign Trade Law, and other applicable laws, regulations and rules.

Article 21 (International treaties). Where an international treaty or agreement that China has concluded or acceded to provides differently from domestic law, that treaty or agreement applies, except for clauses on which China has declared a reservation. The province supports aligning with high-standard international economic and trade rules to advance export facilitation, conducting stress tests of the data-export clauses of such rules, and exploring a data-export security-risk-prevention system suited to a higher level of openness.

Article 22 (Personal-information counting rule). On the negative list, the scale of personal information is counted by **natural person (de-duplicated / 去重)**. Situations falling under Article 3, Article 4, or Article 5, paragraph 1, items (1) – (3) of the CBDF Provisions are **not counted toward the cumulative total**.

Article 23 (Sensitive personal information). Sensitive personal information (敏感个人信息) referenced on the negative list may be identified with reference to the relevant technical specifications issued by the national standardisation authority or industry regulators, in light of the specific business scenario.

Article 24 ("And above" is inclusive). In the personal-information-scale descriptions on the negative list, "and above" (以上) is inclusive of the stated figure.

Article 25 (Other FTZs' lists). Data-export negative lists officially released by other free trade zones may be referred to and applied (参照执行) in the Guangdong FTZ and the Hetao Shenzhen Park.

Article 26 (Effective date). These Measures take effect on the date of issuance, for a **two-year trial period**.

Annex: China (Guangdong) Free Trade Zone Data Classification and Grading Reference Rule — translated as Part B.

> **Translator's note.** These Measures contain no national-core-data (国家核心数据) carve-out and no repeal-of-prior-version clause; none appears in the Chinese source, and none has been supplied. National core data remains governed by the general national regime and is, by definition, outside any export mechanism. No separate filing/implementation guide (with application → filing-result-notice → validity-period, or district/municipal review timelines) accompanies this source; under Article 5, such guides are issued separately by each regional administrative agency after filing with the provincial authorities.

Part B — Important-Data / Classification Annex

Annex to the Measures: **China (Guangdong) Free Trade Zone Data Classification and Grading Reference Rule** (中国（广东）自由贸易试验区数据分类分级参考规则). It comprises a set of unified important-data identification reference rules and a 13-category / 40-subcategory important-data catalogue.

Unified important-data identification reference rules (重要数据统一识别参考规则):

1. This reference rule applies to **non-classified data**; classified (state-secret) data is handled under the relevant provisions.

2. Held by Guangdong FTZ enterprises: personal information (excluding sensitive) of **10 million+ persons**; sensitive personal information of **1 million+ 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.
3. Personal information of **100,000+ persons** held by an operator nationally recognised as critical information infrastructure.
4. High-value sensitive data related to industry competitiveness or industry production safety, collected and generated by Guangdong FTZ enterprises during R&D design, manufacturing, and operation-management; and enterprise supply-chain data bearing on national security.
5. Automatic-control-system parameters and control, operation-maintenance and testing data, in fields bearing on the national economy and people's livelihood, held by Guangdong FTZ enterprises.

The catalogue below pairs each Level-1 category (一级类别) and Level-2 sub-category (二级类别) with representative important-data. Several sub-categories are identified by reference to national industry guidelines — the **Guidelines for Identifying Important Data in the Industrial Sector (YD/T 4981-2024)**, the **Guidelines for Identifying Important Data in the Telecommunications Sector (YD/T 3867-2024)**, and, for connected vehicles, the **Automotive Data Export Security Guidelines (2026 edition)**.

Category (一级类别)	Sub-category (二级类别)	Representative important-data
Strategic materials & bulk commodities （一）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 international-trade data of the petroleum/petrochemical/natural-gas sector from which the operating status, development trend and growth rate of important fields bearing on major national strategy could be inferred.
	2. Agricultural products 农产品	Strategic-reserve data for bulk agricultural products (grain, cotton, edible vegetable oil, sugar, meat, dairy, etc.); non-public international-cooperation and trade data; data on categories/quantities of rare and endangered germplasm resources (incl. genes) of crops, livestock and aquatic species that may affect biosecurity; non-public agricultural/rural statistical, inspection-monitoring and epidemic-prevention/quarantine data; geographic-information data of a certain precision or not publicly released.
Natural resources & environment （二）自然资源和环境类	3. Geographic information 地理信息	Fundamental geographic-information data (positioning-base, place-name/address, terrain/landform, geographic-entity) and remote-sensing imagery reaching state-prescribed coverage, precision and scale, or depicting sensitive areas and targets; thematic geographic-information data.
	4. Meteorology 气象	Meteorological-monitoring data serving military, national-defence-research and high-tech fields (among monitoring, atmospheric-monitoring, support, regional, radar-base and station-metadata categories).
	5. Ocean / marine 海洋	Marine eco-environment monitoring data and disaster-defence data unsuitable for public release or of military value.
	6. Environmental protection 环保	Self-monitoring data reflecting pollutant-emission levels, data from administrative penalties, and other pollutant-emission data.

Category (一级类别)	Sub-category (二级类别)	Representative important-data
	7. Water conservancy 水利	Flood/drought-defence business data reflecting flood/drought and engineering hazards; basic data on dangerous works/sections; non-public national water-resource and water-environment base data, water-regime and hydrological-observation data; remote-sensing imagery and digital-twin water data of a certain precision; physical-security-protection status of key water projects.
Industry （三）工业类	8. Steel & non-ferrous metals 钢铁、有色金属	Per YD/T 4981-2024. National steel/non-ferrous-metal strategic-reserve data or important geological data of strategic non-ferrous-metal deposits; reserves/output/procurement data of non-ferrous metals of significant military or civilian value; mining-area data rich in important associated-mineral resources.
	9. Rare earths 稀土	Per YD/T 4981-2024. Rare-earth mining and smelting production-technology data uniquely mastered by China.
	10. Other minerals 其他矿产	Reserve, international-cooperation and international-trade-negotiation data and mineral-related industrial-layout data; bulk raw-material information and data capable of swaying raw-material procurement pricing power.
	11. Chemical industry 化学工业	Per YD/T 4981-2024. Detection/monitoring of key hazardous chemicals, key-process, equipment-operation and output/reserve data held by Guangdong FTZ enterprises.
	12. Electric power 电力	Power-plant production data, transmission/distribution data, construction and O&M data.
	13. Electronic information 电子信息	Per YD/T 4981-2024. Advanced electronic-information technologies; advanced IC design/manufacturing technology; major computing-equipment design data; algorithms and hardware/software architecture; localisation rate of important electronic components and equipment.
	14. Civil nuclear facilities 民用核设施	Experiment/test data in civil-nuclear-facility research, facility design and manufacturing-process information, and facility operation-monitoring data.
	15. Industrial equipment 工业装备	Per YD/T 4981-2024. R&D and production data of key automotive components bearing on China's S&T strength and international competitiveness (e.g., body-stability-control and active-damper systems).
	16. Intelligent connected vehicles 智能网联汽车	Per YD/T 4981-2024 and the Automotive Data Export Security Guidelines (2026 ed.). Autonomous-driving model-training data used in ICV R&D/production; spatio-temporal data of a certain precision/scale covering specific areas, collected/generated during networked operation of vehicles and roadside equipment.
	17. Other (industrial) 其他	Per YD/T 4981-2024. Industrial-internet or industrial-control-system secure-operation safeguard data used by above-scale industrial enterprises.
National defence S&T industry （四）国防科技工业类	18. National defence S&T industry 国防科技工业	Management, R&D-design, manufacturing, test-verification and maintenance-support data related to national military, economic, S&T and cybersecurity; data reflecting the R&D and production capacity of important defence-S&T-industry entities; data that, aggregated, reflects the overall state of the defence S&T industry; and sector-specific characteristic important data.

Category (一级类别)	Sub-category (二级类别)	Representative important-data
Telecommunications （五）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.
Radio, television & online audiovisual （六）广播电视和网络视听类	20. Radio & television 广播电视	Non-public audiovisual creative content; audiovisual content whose misuse could jeopardise ideological or public security; transmission-coverage data of provincial-and-above broadcasting bodies; broadcasting/audiovisual monitoring-regulation data.
	21. Online audiovisual 网络视听	As above, plus the sector's critical-information-infrastructure and important-network/information-system planning-construction, O&M, key-resource and security-safeguard data.
Finance （七）金融类	22. Banking 银行	Institutional security-guard information across banking, insurance, securities/futures, financial leasing and payment-clearing; and business data these institutions process for important entities, including defence/military enterprises and enterprises bearing on national security. (Bank customer, business, management, system-operation and security-management data.)
	23. Insurance 保险	Insurer customer, business, management, system-operation and security-management data (see the shared finance rule above).
	24. Securities & futures 证券期货	Investor-class, technical-class and business-class data (see the shared finance rule above).
	25. Financial leasing 融资租赁	Customer, enterprise-transaction and management data (see the shared finance rule above).
Transportation （八）交通运输类	26. Transportation 交通	Data affecting production safety and supply-chain safety in railway, highway, road, urban, waterway, civil-aviation and postal fields; natural-resource data obtained during construction; non-public route maps and key-station data; and data whose leakage or tampering could cause a major traffic accident.
Health, food & drugs （九）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 related to ethnicity and group health that reflect an ethnic group's overall condition or bear on biosecurity.
	28. Health & medical 健康医疗	Medical-service, EMR/EHR and medical-research data; diagnosis-and-treatment data involving people's life, health and safety in specific fields, groups or areas, or reaching a certain precision and scale; results of developing/utilising patient health-medical data.
	29. Food 食品	Food-safety traceability-identifier data; automatic-control-system parameters and control-type data in food production.
	30. Drugs 药品	Experimental data submitted in drug supply and drug approval; trial data related to drug-production processes and facilities.
	31. Biosecurity 生物安全	Virus-research or biological-laboratory-related data.
	32. Disease-control data 疾控数据	Data on public-health emergencies and infectious diseases — epidemic, treatment, vaccine and cause-of-death data. (Food/drug/biosecurity/disease-control data bearing on national, life and human safety.)

Category (一级类别)	Sub-category (二级类别)	Representative important-data
Public security （十）公共安全类	33. Physical security 物理安全	Base data of important targets, security-equipment data and security-deployment data of sensitive premises whose illegal use could seriously harm social stability.
	34. Cybersecurity 网络安全	FTZ-enterprise information-system design/operation data, network-facility topology-architecture data and security-safeguard data; critical-information-infrastructure or important-network planning and secure-operation data.
Internet services & e-commerce （十一）互联网服务和电子商务类	35. Internet platform services 互联网平台服务	Data generated in providing internet services that could be used for social mobilisation; digital-portrait data of sensitive groups such as veterans; and records/tracking data of military-industrial 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 may affect national security and public interest.
Science & technology （十二）科学技术类	37. Intellectual property & major discoveries 知识产权和重大发现	IP data involving national defence and security; research papers, observation data and industrialisation results that could significantly enhance, or directly affect, national-security capacity.
	38. Prohibited/restricted export technology 禁止出口限制出口技术	Data related to technologies listed in the Catalogue of Technologies Prohibited or Restricted from Export by China.
Other data （十三）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 the national export-control list; data controlled under the Export Control Law that relates to national security and interests and to non-proliferation and other international obligations.
	40. Other national-security-affecting data 其他可能影响国家…安全的数据	Other data meeting the definition of important data that may affect national politics, territory, military, economy, culture, society, S&T, cyberspace, ecology, resources, nuclear, overseas interests, space, polar, deep-sea, low-altitude or biological security.

Part C — The Negative List: Scope

The 2025 list (中国（广东）自由贸易试验区数据出境管理清单（负面清单）（2025版）) covers **two sectors**. Each sector is split into the **two tiers** of Article 8:

- **Tier 1 — security-assessment list** (需要通过数据出境安全评估的数据清单): important data, plus personal information above the high thresholds. Export requires a **data-export security assessment**.
- **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): personal information in the middle/lower bands. Export requires a **personal information export standard contract (filing)** or **personal information protection certification**.

Within each sector, the personal-information rows are further split between **named business scenarios** (where the higher bands apply) and **"other scenarios"** (all scenarios beyond the named ones). The seven scenarios across the two sectors are: for personal credit reporting — *credit-status inquiry; loan / credit-card application review; guarantee review; post-loan risk management*; for intelligent equipment manufacturing — *R&D and manufacturing; supplier management; recruitment*. Field-level detail (67 fields in total) is summarised here for scope, not reproduced.

Counting rule (Measures Arts. 22, 24). Personal-information volume is counted **by natural person (de-duplicated)** and accumulated **from 1 January of the current year**. Situations under **CBDF Provisions Art. 3, Art. 4, and Art. 5(1)(i) – (iii)** are **excluded** from the cumulative total. "And above" (以上) is inclusive of the stated figure. *(The Chinese source states these three provisions only; it does not reference Art. 6.)*

Sector	Tier 1 — security assessment (important-data focus & high PI bands)	Tier 2 — standard contract / certification (PI bands)
Personal credit reporting services 个人征信服务业 Applies to personal-credit-reporting institutions qualified to operate personal-credit-reporting business; covers the personal information and important data involved in providing credit-status-inquiry and similar services.	**Important data:** important data assessed and determined by the industry regulator — all scenarios — including important data the regulator has notified or publicly released. **Personal information (per year, cumulative):** • In the named scenarios (credit-status inquiry; loan / credit-card application review; guarantee review; post-loan risk management): PI excl. sensitive ⩾ **1,000,000 persons**; or sensitive PI ⩾ **10,000 persons**. • In other scenarios: PI excl. sensitive ⩾ **1,000,000 persons**, or sensitive PI ⩾ **10,000 persons** (excluding CBDF Provisions Art. 3/4/5(1)(i) – (iii) situations).	**Personal information (per year, cumulative):** • In the named scenarios: PI excl. sensitive **100,000 to < 1,000,000 persons**; or sensitive PI < **10,000 persons**. • In other scenarios: PI excl. sensitive **100,000 to < 1,000,000 persons**, or sensitive PI < **10,000 persons**.
Intelligent equipment manufacturing 智能装备制造业 Applies to enterprises, universities and research institutes in intelligent equipment manufacturing. "Intelligent equipment" = devices with self-sensing, self-decision, self-execution, self-adaptation and self-learning functions built on deep integration of advanced manufacturing and next-generation IT. Note: personal information of high-level S&T talent (with academic standing, mastery of key technology, and outstanding contribution to enterprises' digital/intelligent transformation) is *excluded* from this list.	**Important data (four categories):** (1) data — generated in planning/implementing national S&T-program projects (incl. national major projects and key R&D programs) in intelligent equipment manufacturing — that is directly related to national security and involves national-security and social-development interests; (2) data related to industry competitiveness or the sector's core competitiveness / industrial-ecosystem development; (3) data related to national AI security involving national-security and social-development interests; (4) important data assessed and determined by the industry regulator (all scenarios). **Personal information (per year, cumulative):** • In the named scenarios (R&D and manufacturing; supplier management; recruitment): PI excl. sensitive ⩾ **1,000,000 persons**; or sensitive PI ⩾ **10,000 persons**. • In other scenarios: PI excl. sensitive ⩾ **1,000,000 persons**, or sensitive PI ⩾ **10,000 persons** (excluding CBDF Provisions Art. 3/4/5(1)(i) – (iii) situations).	**Personal information (per year, cumulative):** • In the named scenarios: PI excl. sensitive **100,000 to < 1,000,000 persons**; or sensitive PI < **10,000 persons**. • In other scenarios: PI excl. sensitive **100,000 to < 1,000,000 persons**, or sensitive PI < **10,000 persons**.

How to read the bands. For a given sector and scenario, personal information at or above the Tier-1 threshold requires a data-export security assessment; the middle band (100,000 up to but not reaching 1,000,000 non-sensitive persons, or fewer than 10,000 sensitive persons) drops to Tier 2 (standard contract or certification); and volumes below Tier 2 — together with any export not falling within a listed sector/field, or within a listed sector but off the list — fall outside these three mechanisms under Article 10, subject to the national baseline rules and the export-control

carve-out. Both sectors carry the same export-control note: where the data involves controlled-item technical materials under the Export Control Law or technology-export matters under the Foreign Trade Law, those laws govern.

Source: 中国（广东）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 Guangdong CAC · Provincial Commerce Dept · Government Services and Data Administration, May 2026. Chinese originals downloadable at datacompliancechina.com/resources/negative-lists.