Identification of Important Data and Compliance Obligations

By Xun Yang | Echo Li

The Data Security Law establishes a data classification and grading protection regime. As the pivotal category bridging the strict controls on core data and the routine management of general data, important data is the centrepiece of most enterprises' data compliance work. Since the Regulations on Network Data Security Management (State Council Order No. 790, the 'Network Data Regulations') took effect on 1 January 2025, the rules governing the identification, protection obligations and export of important data have gradually become clear; the Measures for Network Data Security Risk Assessment (the 'Risk Assessment Measures'), effective 20 August 2026, further specify how risk assessment obligations will be implemented. This article addresses three questions: how important data is identified, what compliance obligations enterprises assume once important data is identified, and how important data may be exported in compliance with the law.

I. Identification of Important Data

1.1 Self-Identification by Enterprises and Final Confirmation by the Government

Article 21 of the Data Security Law provides that the State establishes a data classification and grading protection regime, under which the competent authorities of each region and each department determine the specific catalogues of important data for their respective regions, departments, industries and sectors. In other words, the final authority to identify important data rests with the government. Article 29 of the Network Data Regulations further provides that network data processors must identify and declare important data in accordance with relevant State rules, and that the competent region or department will confirm the identification and notify the

For more Llinks publications, please contact:

Publication@llinkslaw.com

processor or publish it publicly. This creates the basic structure of 'self-identification and declaration by enterprises, followed by government confirmation and notification.'

This structure has two implications. First, as far as day-to-day security measures are concerned, an enterprise cannot exempt itself from liability on the ground that it has 'not been notified.' Identifying and declaring important data is itself a statutory obligation: before receiving confirmation from the competent authority, an enterprise must proactively carry out identification and take protective measures for any data suspected of being important data; an enterprise shall remain liable where it fails to identify important data due to negligence in identification or declaration. Second, for the specific scenario of data export, the rules provide an express exemption: Article 2 of the Provisions on Promoting and Regulating Cross-Border Data Flows provides that a data processor that has not been notified by the competent department or region, and whose data has not been publicly released, as important data, is not required to apply for a data export security assessment in respect of such data as important data. In other words, the export assessment obligation is triggered only by official notification or public release; data that an enterprise itself suspects of being important data does not automatically become subject to export assessment before official confirmation. This arrangement strikes a balance between strengthening day-to-day protection and facilitating data flows, but enterprises should still keep written records of the identification process to demonstrate that they have duly discharged their identification and declaration obligations.

1.2 Self-Identification by Enterprises

The principal technical basis for self-identification is the national standard GB/T 43697-2024, Data Security Technology — Rules for Data Classification and Grading (the 'Classification and Grading Standard'). Published and implemented in 2024, the standard provides general rules for industry regulators and data processors alike, and its Annex G, Guidelines for Identifying Important Data, is a normative annex with direct guiding effect.

The standard divides data, from highest to lowest, into three levels: core data, important data and general data. Important data refers to data that relates to a specific field, a specific group or a specific region, or that reaches a certain level of precision or scale, and that, once leaked, tampered with or destroyed, could directly endanger national security, economic operations, social stability, or public health and safety. Data that affects only an organisation itself or individual citizens is generally not treated as important data.

As to the identification rules, Article 6.5 of the Classification and Grading Standard sets out seven conditions for identifying important data, the core logic of which is 'object of impact + degree of impact': data whose compromise would directly cause ordinary harm to national security, or serious harm to economic operations, social order or public interests, should be identified as important data; likewise, data in specific fields, or relating to specific groups or specific regions, that directly bears on national security, economic operations, social stability, or public health and safety, as well as data

reaching a certain precision, scale, depth or degree of importance, also constitutes important data. Building on these rules, Annex G lists eighteen specific identification factors, covering, among others, non-public geographic and natural-resource data, data on strategic-material stockpiles and production capacity, data on the operation of and supply chains for critical information infrastructure, technical data relating to export-controlled items, important biological resources and population health data, and non-public statistical data. Enterprises may screen their data against these factors item by item.

Operationally, enterprises may follow the five-step process in Article 7.2 of the Classification and Grading Standard: first, take stock of data assets to establish a complete inventory; second, adopt internal rules — where the industry regulator has issued classification and grading rules, apply them with priority and refine them as appropriate, and where no industry rules exist or certain data is not covered, apply the national standard directly; third, carry out classification and grading to determine the scope of core data, important data and general data; fourth, review the results, compile the classification and grading inventory and the important data catalogue, and submit them through the prescribed procedures; fifth, update dynamically as the importance of the data and the degree of potential harm evolve. Throughout the process, enterprises should observe three principles: grading at the highest level (where several factors affect the grading, classify at the highest degree of impact); combining individual items with aggregated effects (assess not only individual data items but also the security impact of converging and fusing data from multiple sources); and dynamic updating (reassess the grading whenever the scale, timeliness or use scenario of the data changes significantly).

1.3 Identification by the Competent Authorities

The first mode of identification by the competent authorities is direct confirmation by legislation, exemplified by the automotive industry. Article 3 of the Several Provisions on the Management of Automobile Data Security (Trial), jointly issued by the Cyberspace Administration of China (CAC) and four other departments, directly enumerates six categories of important data: geographic information, personnel flows and vehicle flows relating to important sensitive areas such as military administration zones, defence science and industry entities, and Party and government organs at or above the county level; data reflecting economic performance, such as vehicle flows and logistics data; operational data of vehicle charging networks; exterior video and image data containing facial or licence-plate information; personal information involving more than 100,000 data subjects; and other data designated by the relevant authorities. The Provisions also require important data to be stored within China. Under this 'legislative enumeration' model, enterprises can directly match their data against the statutory list, making the identification criteria the clearest of all.

The second mode is 'survey and mapping — institutional declaration — confirmation and notification,' typified by the financial sector. The National Financial Regulatory Administration (NFRA) issued the Measures for Data Security Management of Banking and Insurance Institutions, requiring banking and insurance institutions to establish data classification and grading protection systems, to prepare and promptly update catalogues of important data, and to submit them to the regulator. In practice, the

regulator first conducts surveys to establish a baseline understanding of the industry's data and the applicable identification criteria; institutions then complete self-identification and declare their catalogues, which the regulator reviews and confirms before notifying the institutions, thereby forming each institution's list of important data. Under this model, enterprise identification is the starting point and regulatory confirmation the endpoint, with continuous interaction between the two.

In addition, the industry and information-technology sector applies catalogue filing for important data and core data under the Measures for Data Security Management in the Field of Industry and Information Technology (Trial), while surveying and mapping geographic information data in the natural-resources sector is subject to separate controls. The general trend is that regions and departments are successively publishing important data catalogues for their respective industries and sectors; enterprises should closely track these developments and promptly recalibrate their own identification results.

II. Compliance Obligations for Important Data

Once data is identified as important data, the processor assumes a series of enhanced obligations under the Data Security Law and the Network Data Regulations, which can be grouped into six areas.

2.1 Organisational Structure

Paragraph 2 of Article 27 of the Data Security Law requires processors of important data to designate a data security officer and establish a data security management body to implement data security protection responsibilities. Article 30 of the Network Data Regulations further refines the qualification requirements: the data security officer must be a member of the management team, possess professional knowledge of data security and relevant management experience, and have the right to report data security issues directly to the competent authorities, such as the cyberspace administration and the public security bureau. The data security management body is responsible for developing and implementing management systems and operating procedures, organising education and training, monitoring and addressing security risks, and handling complaints and reports. Notably, under Article 28 of the Network Data Regulations, a processor that processes the personal information of more than 10 million individuals must comply with the foregoing requirements even if it does not process important data. In implementation, enterprises should ensure that the data security officer participates substantively in business decisions and holds resource-allocation authority commensurate with the responsibility, so as to avoid a mere 'nominal appointment.'

2.2 Institutional Systems

Article 27 of the Data Security Law establishes the basic requirements of 'establishing a sound full-lifecycle data security management system and organising data security education and training'; Article 9 of the Network Data Regulations further requires a sound network data security management system

to be built on the foundation of the multi-level cybersecurity protection scheme. For processors of important data, the institutional framework should include at least: (i) a data classification and grading system that sets out the procedures for identifying, declaring, cataloguing and dynamically updating important data; (ii) full-lifecycle management rules covering the operating procedures and approval requirements for each stage of collection, storage, use, processing, transmission, provision, disclosure and deletion; (iii) rules on external provision and entrusted processing, bringing the provision, entrusted processing and joint processing of important data within the scope of ex ante ad hoc assessment and contractual constraints; (iv) an emergency response system with mechanisms for incident grading, response, reporting and drills; and (v) personnel management rules binding employees with access to important data through training and confidentiality obligations. In addition, Article 32 of the Network Data Regulations imposes a reporting obligation in special circumstances: where a processor of important data undergoes merger, division, dissolution or bankruptcy in a way that may affect the security of important data, it must take measures to safeguard the data and report the data disposal plan and information on the recipient to the competent authorities at or above the provincial level.

2.3 Technical Measures

Article 27 of the Data Security Law requires data processors to adopt corresponding technical measures and other necessary measures; Article 9 of the Network Data Regulations lists representative measures such as encryption, backup, access control and security authentication. In general, technical measures should be commensurate with the importance of the data: encrypted storage and backup at the storage stage; access control, identity authentication and transmission encryption to prevent unauthorised access at the use and transmission stages; and de-identification, watermarking and interface authentication at the sharing and provision stages. Log retention and security auditing underpin the effectiveness of all such measures, and operations on important data must be fully traceable. It is also worth noting that Article 23 of the Risk Assessment Measures requires that, where technical measures such as encryption of important data are involved, a commercial cryptography application security evaluation must be carried out in accordance with State cryptography laws and administrative regulations.

2.4 Risk Monitoring and Incident Response

Article 29 of the Data Security Law imposes two tiers of obligations: a processor must strengthen risk monitoring in the course of its data processing activities and, upon discovering risks such as data security defects or vulnerabilities, must immediately take remedial measures; when a data security incident occurs, it must immediately take response measures and, as required, promptly notify users and report to the competent authorities. Processors of important data should institutionalise risk monitoring, using vulnerability scanning, intrusion detection and anomalous-behaviour analysis to stay apprised of the security status of important data; establish an emergency response mechanism with clear incident grading standards and reporting timelines so that 'response, notification and reporting'

proceed in tandem; and conduct post-incident root-cause analysis and remediation reviews, incorporating incidents and their handling into the annual risk assessment report, thereby closing the loop of 'monitoring — response — review — improvement.'

2.5 Risk Assessment

Article 30 of the Data Security Law requires processors of important data to conduct risk assessments of their data processing activities on a regular basis and to submit assessment reports to the competent authorities, covering the categories and volumes of important data processed, the data processing activities carried out, the risks faced and the corresponding countermeasures. The Network Data Regulations and the Risk Assessment Measures (effective 20 August 2026) elaborate this obligation into a two-tier structure of 'annual assessments + ad hoc assessments.'

The routine assessment is the annual assessment. Article 33 of the Network Data Regulations requires processors of important data to assess their network data processing activities once a year and to submit the assessment report to the competent authorities at or above the provincial level. The Risk Assessment Measures further provide that the assessment may be conducted in-house (with a designated person in charge) or entrusted to a third-party assessment institution; that assessments should follow national standards such as GB/T 45577-2025, Data Security Technology — Methodology for Data Security Risk Assessment; and that the report must be submitted within 20 working days after completion of the annual assessment and retained for at least three years.

Ad hoc assessments correspond to special circumstances. First, Article 31 of the Network Data Regulations requires a risk assessment before important data is provided to others or entrusted or jointly processed, focusing on the legality, propriety and necessity of the processing purpose, data security risks, the recipient's integrity and compliance record, the binding force of the contract, and the effectiveness of technical and management measures (except where processing is in performance of statutory duties or obligations). Second, Article 5 of the Risk Assessment Measures requires that, where a material change in the security status of important data may adversely affect data security, a timely assessment of the changed part and its impact be conducted. Ad hoc and annual assessments have independent triggers and should in principle be conducted separately; in practice, new matters may be covered by a supplementary assessment within the annual framework to avoid duplicated effort.

2.6 Security Assessment for Data Export

The export of important data is not governed by the ordinary risk assessment regime but must pass a dedicated national security review. Article 31 of the Data Security Law establishes the regulatory framework for important data exports, and Article 37 of the Network Data Regulations provides that important data collected and generated in the course of domestic operations may be provided abroad only where genuinely necessary and after passing the data export security assessment organised by

the national cyberspace authority. Under Article 7 of the Provisions on Promoting and Regulating Cross-Border Data Flows, a critical information infrastructure operator (CIIO) that provides personal information or important data abroad, and any other data processor that provides important data abroad, must apply for an export security assessment, with no quantitative threshold — any involvement of important data triggers the filing obligation. The security assessment is organised by the national cyberspace authority and functions as a form of ex ante admission: important data that has not passed the assessment may not be exported. An assessment result is valid for three years and may be extended if the relevant conditions are met.

III. Cross-Border Export Compliance for Important Data

Export compliance for important data can be divided into two layers: 'foundational arrangements before export' and 'compliant use of the export channel.' The former addresses where the data and access to it are located; the latter addresses how data may lawfully flow across borders.

3.1 Foundations of Export Compliance

3.1.1 Localised Deployment

The underlying policy for important data is 'domestic storage as the rule, export as the exception.' Local storage is the cornerstone of supervision over important data: if an enterprise operates in a thin-terminal mode with no local servers, important data leaves the country as soon as it is generated, leaving regulators with nothing to oversee. Article 11 of the Several Provisions on the Management of Automobile Data Security (Trial) likewise requires important data to be stored within China, and provides that data may be provided abroad only where genuinely necessary and after passing a security assessment. The words 'genuinely necessary' indicate that localisation is the default and that export is subject to case-by-case review premised on business necessity.

For multinational enterprises, localised deployment is the physical foundation of export compliance. Many foreign-invested enterprises have established data centres in China, storing their China business data domestically and transmitting abroad only those data items approved for export through assessment. Local deployment also directly affects the feasibility of an export assessment: the Self-Assessment Report on Data Export Risks requires the applicant to describe the systems, platforms and data centres in which the data to be exported is stored within China, as well as the export pathway; without a clear domestic storage and linkage architecture, there would be no basis for an application. When planning their IT architecture, enterprises should segregate and tier domestic and overseas data storage at an early stage, avoiding a pattern of 'architecture first, compliance later.'

3.1.2 Local Access Control

Local storage of important data must be accompanied by local access control. If the highest administrative privileges over domestically stored important data sit abroad, the domestic entity cannot in practice control how the data is accessed and processed from overseas, and Chinese regulators would find it difficult to exercise jurisdiction over the processing of the important data.

The Guidelines for Applications for Data Export Security Assessment (Third Edition) make clear that where data is stored in China but overseas institutions, organisations or individuals are able to query, retrieve, download or export it, this constitutes a data export. Remote access to domestic systems by an overseas parent company, global R&D teams or overseas IT operations personnel is itself a 'logical export' channel and is not exempt merely because the data is physically stored in China.

Access control is therefore the second cornerstone of export compliance. Enterprises should establish dedicated controls over overseas access: (i) ultimate administrative privileges must reside in China, ensuring control over important data stored domestically; (ii) overseas personnel may access important data in China only under least-privilege authorisation; (iii) access must be logged end to end, with auditable access records generated through log auditing and bastion-host screen recording; and (iv) technical isolation should be adopted — where overseas query access is genuinely required, de-identified queries or controlled API calls should be preferred over direct database access. Robust access control is both a firewall against 'export without filing' and the factual basis for demonstrating the necessity of any export.

3.2 Export Pathways

3.2.1 Overview of the Security Assessment Process

The lawful channel for exporting important data is the data export security assessment. Under the Guidelines for Applications for Data Export Security Assessment (Third Edition): the data processor first conducts a self-assessment of export risks and prepares a self-assessment report; it then submits the application materials online through the data export filing system (sjcj.cac.gov.cn), while special categories of applicants such as CIIOs file offline through the provincial cyberspace administration; the provincial cyberspace administration completes a completeness check within five working days and, if the materials are complete, refers the application to the national cyberspace authority, which decides whether to accept it within seven working days; upon acceptance, the assessment will be under review, and supplementary or corrected materials may be required; when the assessment is completed, a notice of the assessment result is issued, and any objection may be submitted for re-assessment within 15 working days. The assessment result is valid for three years; within 60 working days before expiry, the processor may apply for an extension provided that, among other conditions, the purpose

and scope of the export and the parties involved remain unchanged and the increase in the volume of data to be exported does not exceed 20 per cent.

3.2.2 Non-overall Data Export

The security assessment reviews data items item by item within each business scenario, and the outcome is 'clearance item by item' rather than 'one-package approval.' An enterprise cannot export its important data in one package; it must conduct a necessity assessment for each scenario, and only data that must be exported may be exported. Official figures released by the CAC confirm this: as of March 2025, of the 44 assessment projects involving the export of important data, only 325 of the 509 important data items declared were approved for export, representing 63.9 per cent of the total, and seven projects were rejected outright. Enterprises should adopt the expectation of 'export nothing that need not be exported, and export as little as possible,' screening and narrowing the data items to be exported before filing.

3.2.3 Necessity Assessment

Necessity is at the heart of the assessment review. The self-assessment report must list, in tabular form, each data item's name, a description of its content and the necessity of its export, explaining item by item why the data must be exported and why the overseas recipient must use it. The purpose, scope and method of the export must be lawful, proper and necessary, and must correspond to the purposes and means by which the overseas recipient processes the data. Vague necessity arguments and a lack of correspondence between data items and business scenarios are common reasons why the CAC rejects an application or requires the export scope to be narrowed.

3.2.4 Internal Controls

Passing the security assessment is not the end of the matter. Enterprises must also: (i) maintain a ledger of exported data, carry out export activities strictly in accordance with the purposes, scope, methods, and categories and volumes of data specified in the notice of the assessment result, and retain records for inspection; and (ii) manage changes dynamically — reapply where the purpose, scope or recipient of the export changes, and apply in good time for an extension where exports are to continue beyond the validity period.

If you would like to know more information about the subjects covered in this publication, please contact:

Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

SHANGHAI

19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING

30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli, Chaoyang District
Beijing 100020 P.R.China
T: +86 10 5081 3888
F: +86 10 5081 3866

SHENZHEN

18F, China Resources Tower
2666 Keyuan South Road, Nanshan District
Shenzhen 518063 P.R.China
T: +86 755 3391 7666
F: +86 755 3391 7668

HONG KONG

Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON

1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD