China's Proposed Auto Data Rules Could Change How EVs Reach Market

China's draft mandatory standard could make data architecture part of vehicle readiness. Manufacturers should understand the control model before product, supplier and infrastructure choices become difficult to change.

Regulatory updates

China's proposed automotive data-security standard carries a practical warning for EV manufacturers and connected-vehicle companies:

Data compliance may need to be resolved before a vehicle is ready for market, not after the technology platform has been built.

The proposal isn't law yet, but is under public consultation, and the suggested commencement date of July 1st, 2028, has not been finalized. But if the standard is substantially adopted as drafted, electric vehicle manufacturers may have to demonstrate that their vehicles, supporting systems and suppliers meet detailed data-security requirements as part of the product-approval process. MIIT

That could change the sequence of work, bringing data-compliance decisions earlier in vehicle development. Decisions about cloud services, software architecture, vehicle functions and engineering partners may appear merely technical when they are first made. Under the proposed framework, they could later determine whether the manufacturer can actually produce the controls and evidence needed for approval.

From voluntary benchmark to product readiness

MIIT opened consultation on the proposed *Requirements for Vehicle Data Security* on October 20, 2026. The project would fully replace **GB/T 44464-2024**, the current recommended national standard, with a mandatory **GB** standard. Consultation remains open until December 19. MIIT

But why does this matter? Well, the current standard provides a technical benchmark. A mandatory replacement would convey a different regulatory consequence.

The drafting explanation links compliance with mandatory standards to China's vehicle product-admission system. It states that products failing to meet compulsory standards would not be permitted into the relevant catalog for production. New vehicle-type applications would be covered from the proposed commencement date, with a later transition for models already approved. Again, these are proposals, not current deadlines. But they do provide an early indication of how data security may be integrated into the approval regime. MIIT

The draft applies to M- and N-category vehicles, not EVs alone. Nevertheless, the implications are particularly relevant to EV and connected-vehicle businesses, where software, sensors, mobile applications, cloud platforms and over-the-air services are inherent to the product rather than just peripheral support systems. MIIT

The draft asks manufacturers to prove how the system works

The proposal extends far beyond a general policy requiring data to be handled securely.

Manufacturers would need function-level records of automotive data-processing activities. The proposed draft also calls for oversight of development and data-processing partners, internal assessment before data export, continuing export supervision, risk assessment and testing. Measures for monitoring and record keeping showing that the controls operate in practice would need to be in place under the proposed new rules. MIIT

The operating chain begins to look like this:



That chain is difficult to reconstruct once a vehicle program and its supporting platforms are already established.

Consider the connected cabin feature. The vehicle manufacturer may own the customer relationship, while a local supplier develops part of the function. A cloud platform processes some of the data and a global engineering team supports the software. Each participant may have a legitimate role.

The compliance problem is knowing precisely where one role ends, and another begins.

The manufacturer would need to show what the feature collects, where all copies and replicas sit, and what the supplier can do. All to answer the question: Does the operation match the approved control model?

Local hosting does not resolve the cross-border issue

Very significantly, the draft states that vehicles should not transmit data directly overseas, subject to exclusions for independent user activity, such as visiting foreign websites or using communications applications. MIIT

That should not be interpreted as a general ban on automotive data exports.

China's 2026 automotive outbound-data guidance continues to describe lawful cross-border data transfer routes involving security assessment, standard contracts, certification and specified exemptions. There are also export procedures for scenarios including research and development, manufacturing, automated driving, software upgrades and connected operation. The framework regulates automotive data exports; it's important to remember it does not prohibit them outright. MIIT

The architectural implication is narrower but no less important. Vehicle behavior, processing inside China and any later transfer abroad are separate control questions.

Putting a domestic server between the vehicle and an overseas destination does not, by itself, authorize the onward transfer. Equally, the presence of a global engineering team does not automatically make the operating model noncompliant.

The critical factor is whether or not the manufacturer can explain and evidence the route by which data moves. They must also show the legal basis for that movement and the controls applied at each boundary.

The risk lies in making these decisions too late

China already has binding automotive data rules. Since 2021, automotive data processors have faced obligations concerning personal information, Important Data, domestic storage and security assessment for certain exports. The new proposed standard should not be presented as though automotive data protection were previously optional—it was never optional. Cyberspace Administration of China

What the new proposal adds is a more detailed connection between those obligations and the vehicle's operating design.

It asks manufacturers to think in terms of functions, lifecycle controls, supplier relationships, monitoring, testing and inspection records. Documentation submitted for inspection would need to be versioned, made tamper-proof, and retained for at least three years. That three-year period applies to the inspection documentation, not to every item of automotive data. MIIT

This is where the danger of an unresolved compliance issue can become a product-development problem.

A manufacturer that discovers late in the program that it cannot identify every cloud copy, or restrict a provider's authority, or produce the required evidence may have to change more than its documentation. It may need to alter the application, its interfaces or the relationship between the China and global environments. That's far from trivial.

What EV players should do before the standard is finalized

The immediate response should not be a wholesale infrastructure replacement. Existing China deployments may actually already satisfy much of the eventual standard, and the final text may of course change through the consultation process.

A more practical next step is to test one real vehicle function against the proposed control model.

Choose a connected service, driver-assistance feature or OTA process and establish:

- what personal information or Important Data it creates;
- where each operational copy is held;
- what suppliers and internal teams can do;
- where the China environment interacts with global systems;
- what evidence would be available during inspection.

The exercise should bring together product, engineering, legal, security and China operations. Its purpose is not to create another compliance spreadsheet. It is to identify where the intended control model and the actual operating environment diverge.

That is also where Carolync's pre-deployment approach becomes relevant. The work begins with the application and its data behavior, then establishes control ownership, provider boundaries, evidence requirements and the permitted China/global interfaces. Infrastructure and vendor choices can then be tested against that model rather than defining it accidentally.

So, this isn't about whether every EV company needs a new data center or cloud provider. It's about ascertaining if an implementation gap exists—and whether it can be corrected before vehicle approval, supplier contracts and platform decisions become seriously expensive to unwind.

Related Carolync Insight: Architecture Has Become Strategy

China's proposed standard remains in draft form. But the direction is already clear enough to act on. For EV players, data architecture is moving closer to product architecture. The manufacturers best prepared will be those that can show not only where the data sits, but how the entire operating chain remains under demonstrable control.

Sources

1. **MIIT:** *Public consultation on the proposed Requirements for Vehicle Data Security, October 20, 2026.* MIIT
2. **National Standards Information Public Service Platform:** *Project 20261957-Q-339, current consultation status and proposed implementation date.* Standard Information Service Platform
3. **SAMR:** *Current GB/T 44464-2024 standard record.* Open Standard
4. **MIIT:** *Full consultation draft of the proposed mandatory standard.* MIIT
5. **MIIT:** *Official drafting explanation, including the proposed transition and product-admission implications.* MIIT
6. **MIIT:** *Explanation of the 2026 automotive outbound-data guidance.* MIIT
7. **Cyberspace Administration of China:** *2021 automotive data-security rules.*