NADA Data Sharing Agreement Guidelines

Automotive retail requires sharing data among dealer systems, OEMs, and third parties. The continuous flow of data ensures an integrated customer experience and promotes the safe and efficient operation, repair, and maintenance of vehicles. The guidelines below and related data sharing principles have been developed to promote legal and regulatory compliance, protect consumers, and build trust among all parties sharing data.

When receiving an agreement that involves data sharing, the following are six minimum key considerations.

What Data is Being Shared?

- Does the agreement require you to share customer data?
- Does the agreement specify what data will be shared? For example, name, phone number, email address, financing details, etc.
- Is the data being shared personal information or Non-Public Information (NPI)? The FTC has released guidance for businesses to determine if information is NPI here.
- If the agreement includes sharing NPI, does the contract comply with the FTC Privacy and Safeguards Rules and applicable state law? Information related to the FTC Privacy and Safeguards Rule that should be included is here.

Who Has Access to the Data?

- Does the agreement state that only the parties to the agreement will receive the data?
- Does the agreement specify with whom the data can be shared now or in the future (i.e. specific third party vendors)?
- Is there specific language in the agreement that the data can or cannot be shared?
- If the data can be shared, is that subject to approval by the dealer?

What Purposes Will the Data be Used For?

- The agreement should avoid violating Section 5 of the FTC Act for Unfair and Deceptive Practices, which can extend to sensitive personal information that is not considered NPI.
- Does the agreement specifically state what purposes the data will be used for?
- Are those purposes in compliance with the law?
- Can the sharing party use the data without informing the dealer?

How is the Data Being Protected?

- Are all parties held to the same standard to protect data—legally and technically?
- Is data being shared equipped with the same technical safeguards (i.e. encrypted) for all parties?
- Are all parties required to hold the same certifications or requirements (STAR, ISO, NIST, etc.)?

Who Has Responsibilities Under the Agreement?

- What are the rights and responsibilities of each party if a data breach occurs?
- If privacy notices and/or consent are required to obtain information from customers, does the agreement state who is responsible for providing the notice and receiving consent?
- What laws need to be followed and by whom?
- Does an updated agreement need to be executed if there are changes in the law?

What Rights Do Parties Have to Terminate the Agreement?

- What are the conditions for terminating the agreement?
- How much notice does the terminating party need to provide?
- If a party terminates an agreement, is the other party obligated to provide operational support to transfer data back to the owner?

This document is offered for informational purposes only and is not intended as legal advice. Consult an attorney who is familiar with federal and state law addressing these topics.

NATIONAL AUTOMOBILE DEALERS ASSOCIATION
8484 WESTPARK DRIVE, SUITE 500, TYSONS, VA 22102 | 800.557.6232 | nada.org