

## Arizona

### **Section 28-4651**

In this article, unless the context otherwise requires:

1. "Authorized Integrator" means a third party with whom a dealer enters into a contractual relationship to perform a specific function for a dealer that allows the third party to access protected dealer data or to write data to a dealer data system, or both, to carry out the specified function.
2. "Cyber ransom" means to encrypt, restrict or prohibit or threaten or attempt to encrypt, restrict or prohibit a dealer's or a dealer's authorized integrator's access to protected dealer data for monetary gain.
3. "Dealer data system":
  - (a) Means a software, hardware or firmware system that is owned, leased or licensed by a dealer, that includes a system of web-based applications, computer software or computer hardware, whether located at the motor vehicle dealership or hosted remotely, and that stores or provides access to protected dealer data.
  - (b) Includes dealership management systems and consumer relations management systems.
4. "Dealer data vendor" means a dealer management system provider, consumer relationship management system provider or other vendor providing similar services that permissibly stores protected dealer data pursuant to a contract with the dealer.
5. "Fee" means a charge for allowing access to protected dealer data beyond any direct costs incurred by the dealer data vendor in providing protected dealer data access to an authorized integrator or allowing an authorized integrator to write data to a dealer data system.
6. "Prior express written consent" means the dealer's express written consent that is contained in a document separate from any other consent, contract, franchise agreement or other writing and that contains:
  - (a) The dealer's consent to the data sharing and identification of all parties with whom the data may be shared.

(b) All details that the dealer requires relating to the scope and nature of the data to be shared, including the data fields and the duration for which the sharing is authorized.

(c) All provisions and restrictions that are required under federal law to allow the sharing.

7. "Protected dealer data" means any:

(a) Personal, financial or other data relating to a consumer that a consumer provides to a dealer or that a dealer otherwise obtains and that is stored in the dealer's dealer data system.

(b) Motor vehicle diagnostic data that is stored in a dealer data system. This subdivision does not give a dealer any ownership or rights to share or use the motor vehicle diagnostic data beyond what is necessary to fulfill a dealer's obligation to provide warranty, repair or service work to its consumers.

(c) Other data that relates to a dealer's business operations in the dealer's dealer data system.

8. "Required manufacturer data":

(a) Means data that is required to be obtained by the manufacturer under federal or state law or to complete or verify a transaction between the dealer and the manufacturer.

(b) Includes information that is reasonably necessary for any of the following:

(i) A safety, recall or other legal notice obligation.

(ii) The sale and delivery of a new motor vehicle or a certified used motor vehicle to a consumer.

(iii) The validation and payment of consumer or dealer incentives.

(iv) Claims for dealer supplied services relating to warranty parts or repairs.

(v) The evaluation of dealer performance, including without limitation the evaluation of the dealer's monthly financial statements and sales or service, consumer satisfaction with the dealer through direct consumer contact or consumer surveys.

(vi) Dealer and market analytics.

(vii) The identification of the dealer that sold or leased a specific motor vehicle and the date of the transaction.

(viii) Marketing purposes designed for the benefit of or to direct leads to dealers but does not include a consumer's financial information on the consumer's credit application or a dealer's individualized notes about a consumer which are not related to a transaction.

(ix) Motor vehicle diagnostic data.

(x) The development, evaluation or improvement of the manufacturer's products or services.

9. "Star standards" means the current, applicable security standards published by the standards for technology in automotive retail.

10. "Third party":

(a) Includes a service provider, vendor, including a dealer data vendor and authorized integrator, and any other person other than the dealer.

(b) Does not include a governmental entity acting pursuant to federal, state or local law, a third party acting pursuant to a valid court order or a manufacturer.

#### **Section 28-4652**

A manufacturer or a third party may not require a dealer to grant the manufacturer, the third party or any person acting on behalf of the manufacturer or third party direct or indirect access to the dealer's dealer data system. Instead of providing a manufacturer or third party with access to the dealer's data system, a dealer may submit or push data or information to a manufacturer or third party through any widely acceptable electronic file format or protocol that complies with the star standards or other generally accepted standards that are at least as comprehensive as the star standards.

#### **Section 28-4653**

A. A third party may not do any of the following:

1. Access, share, sell, copy, use or transmit protected dealer data without prior express written consent.

2. Engage in any act of cyber ransom.

3. Take any action by contract, technical means or otherwise to prohibit or limit a dealer's ability to protect, store, copy, share or use protected dealer data, including all of the following:

(a) Imposing any fee or other restriction on the dealer or an authorized integrator for accessing or sharing protected dealer data or for writing data to a dealer data system, including any fee on a dealer that chooses to submit or push data or information to the third party as prescribed in section 28-4652. A third party must disclose a charge to the dealer and justify the charge by documentary evidence of the costs associated with access or the charge will be deemed to be a fee pursuant to this subdivision.

(b) Prohibiting a third party that has satisfied or is compliant with the star standards or other generally accepted standards that are at least as comprehensive as the star standards and that the dealer has identified as one of its authorized integrators from integrating into the dealer's dealer data system or placing an unreasonable restriction on integration by an authorized integrator or other third party that the dealer wishes to be an authorized integrator. For the purposes of this subdivision, "unreasonable restriction" includes:

(i) An unreasonable limitation or condition on the scope or nature of the data that is shared with an authorized integrator.

(ii) An unreasonable limitation or condition on the ability of the authorized integrator to write data to a dealer data system.

(iii) An unreasonable limitation or condition on a third party that accesses or shares protected dealer data or that writes data to a dealer data system.

(iv) Requiring unreasonable access to a third party's sensitive, competitive or other confidential business information as a condition for accessing protected dealer data or sharing protected dealer data with an authorized integrator.

(v) Prohibiting or limiting a dealer's ability to store, copy, securely share or use protected dealer data outside of the dealer data system in any manner and for any reason.

(vi) Allowing access to or accessing protected dealer data without prior express written consent.

B. Prior express written consent may:

1. Be unilaterally revoked or amended by the dealer with thirty days' notice

without cause and immediately for cause.

2. Not be sought or required as a condition of or factor for consideration or eligibility for any manufacturer program, standard or policy, including those that offer or relate to a bonus, incentive, rebate or other payment or benefit to a dealer, except that if the bonus, incentive, rebate or other payment program requires the delivery of the information that is protected dealer data to qualify for the program and receive the program benefits, a dealer must supply the information to participate in the program.

C. This section does not prevent a dealer, manufacturer or third party from discharging its obligations as a service provider or otherwise under federal, state or local law to protect and secure protected dealer data or to otherwise limit those responsibilities.

D. Unless a dealer gives prior written consent, a manufacturer may not access, share, sell, copy, use or transmit or require a dealer to share or provide access to protected dealer data beyond the required manufacturer data and may use any required manufacturer data obtained from a dealer data system for the purposes listed in section 28-4651, paragraph 8.

E. A manufacturer may not engage in an act of cyber ransom or take an action by contract, technical means or otherwise to prohibit or limit a dealer's ability to protect, store, copy, share or use protected dealer data, including actions described in subsection A, paragraph 3, subdivision (b) of this section. A manufacturer or a manufacturer's selected third party may not require a dealer to pay a fee for the sharing of required manufacturer data if the manufacturer both:

1. Requires a dealer to provide required manufacturer data through a specific third party that the manufacturer selects.

2. Does not allow the dealer to submit the data using the dealer's choice of a third-party vendor and both of the following apply:

(a) The data is in a format that is compatible with the file format required by the manufacturer.

(b) The third-party vendor satisfies or is in compliance with the star standards or other generally accepted standards that are at least as comprehensive as the star standards.

F. A manufacturer shall indemnify a dealer for any third-party claims asserted against or damages incurred by the dealer to the extent caused by access to, use of or disclosure of protected dealer data in violation of this section by the manufacturer or a third party acting on behalf of a manufacturer to whom the manufacturer has provided the protected dealer data. A dealer bringing a cause of action against a manufacturer for a violation of this section has the burden of proof.

G. Notwithstanding subsection D of this section and except as provided in section 28-4655, this article does not restrict or limit a manufacturer's right to obtain required manufacturer data, use required manufacturer data for the purposes prescribed by subsection D of this section or use or control data that is proprietary to the manufacturer, created by the manufacturer, obtained from a source other than the dealer or that is public information.

#### **Section 28-4654**

A. A dealer data vendor shall:

1. Adopt and make available a standardized framework for the exchange, integration and sharing of data from dealer data systems with authorized integrators and the retrieval of data by authorized integrators using the star standards or a standard that is compatible with the star standards.

2. Provide access to open application programming interfaces to authorized integrators. If the application programming interfaces are not the reasonable commercial or technical standard for secure data integration, the dealer data vendor may provide a similar open access integration method if that method provides the same or better access to authorized integrators as an application programming interface and uses the required standardized framework.

B. A dealer data vendor and authorized integrator:

1. May access, use, store or share protected dealer data or any other data from a dealer data system only to the extent allowed in the written agreement with the dealer.

2. Must make any agreement relating to access to, sharing or selling of, copying, using or transmitting protected dealer data terminable on ninety days' notice from the dealer.

3. On notice of the dealer's intent to terminate the agreement, in order to prevent any risk of consumer harm or inconvenience, must work to ensure a secure transition of all protected dealer data to a successor dealer data vendor or authorized integrator, including:

- (a) Providing access to or an electronic copy of all protected dealer data and all other data stored in the dealer data system in a commercially reasonable time and format that a successor dealer data vendor or authorized integrator can access and use.

- (b) Deleting or returning to the dealer all protected dealer data before the contract terminates pursuant to the dealer's written directions.

4. On a dealer's request, must provide the dealer with a listing of all entities with whom it is sharing protected dealer data or with whom it has allowed access to protected dealer data.

5. Must allow a dealer to audit the dealer data vendor or authorized integrator's access to and use of any protected dealer data.

## Montana

### TITLE 30. TRADE AND COMMERCE

#### CHAPTER 11. SALES

##### Part 7. Canceled Dealership Contracts Repurchase Requirements

### Definitions

**30-11-717. Definitions.** As used in **30-11-718**, **30-11-719**, and this section, the following definitions apply:

(1) "Authorized integrator" means any third party with whom a dealer has entered into a contractual relationship to perform a specific function for the dealer that permits the third party to access protected dealer data or to write data to a dealer data system to carry out the specified function.

(2) "Dealer" has the same meaning as "new motor vehicle dealer" provided in **61-4-201** and includes any authorized dealer personnel acting on behalf of the dealer owner-operator.

(3) "Dealer data system" means any software, hardware, or firmware owned, leased, rented, or controlled by a dealer and used by the dealer in its business operations.

(4) "Dealer data vendor" means any dealer management system provider or customer relationship management system provider, or other vendor providing similar services, other than a motor vehicle manufacturer or distributor or a subsidiary or affiliate of a manufacturer or distributor, that permissibly stores protected dealer data pursuant to a contract with a dealer.

(5) "Fees" means charges for access to protected dealer data. Fees must be disclosed to the dealer prior to entering into a contract with a dealer data vendor and must be specified in the terms of the contract.

(6) "Protected dealer data" means:

(a) any nonpublic personal information, including information defined in 15 U.S.C. 6809 pertaining to a consumer, that is provided to a dealer by a consumer or otherwise obtained by a dealer and stored in the dealer's dealer data system; or

(b) any other data regarding a dealer's business operations that is stored in the dealer's dealer data system.

(7) "Third party" includes service providers, vendors, dealer data vendors, authorized integrators, and any other individual or entity other than the dealer. The



term does not include any government entity acting pursuant to federal, state, or local law, any entity acting pursuant to a valid court order, a motor vehicle manufacturer or distributor or a subsidiary or affiliate of a motor vehicle manufacturer or distributor, or an entity acting on behalf of and with whom the manufacturer or distributor has an express agreement to preserve the privacy of protected dealer data.

## **Prohibited Actions**

**30-11-718. Prohibited actions.** (1) A third party may not:

(a) access, share, sell, copy, use, or transmit protected dealer data from a dealer data system without the express written consent of the dealer;

(b) take any action by contract, by technical means, or by any other means that would prohibit or limit a dealer's ability to protect, store, copy, share, or use any protected dealer data. This includes but is not limited to:

(i) imposing any fees or other restrictions on the dealer or any authorized integrator for access to or sharing of protected dealer data or for writing data to a dealer data system;

(ii) prohibiting any third party that the dealer has identified as one of its authorized integrators from integrating into that dealer's dealer data system or placing unreasonable restrictions on integration by any such authorized integrator or other third party that the dealer wishes to be an authorized integrator. Examples of restrictions include but are not limited to:

(A) restrictions on the scope or nature of the data shared with an authorized integrator;

(B) restrictions on the ability of the authorized integrator to write data to a dealer data system;

(C) restrictions or conditions on a third party accessing or sharing protected dealer data or writing data to a dealer data system; and

(D) requiring access to sensitive, competitive, or other confidential business information of a third party as a condition for access to protected dealer data or sharing protected dealer data with an authorized integrator.

(c) prohibit or limit a dealer's ability to store, copy, securely share, or use protected dealer data outside the dealer data system in any manner or for any reason; or

(d) permit access to or access protected dealer data without the express written consent of the dealer.

(2) Nothing in this section prevents any dealer or third party from discharging its obligations as a service provider under federal, state, or local law to protect and secure protected dealer data or to otherwise limit those responsibilities.

(3) A dealer data vendor or an authorized integrator is not responsible for any action taken directly by the dealer, or for any action the dealer data vendor or authorized integrator takes in appropriately following the written instructions of the dealer, to the extent that the action prevents it from meeting any legal obligation regarding the protection of protected dealer data or results in any liability as a consequence of such actions by the dealer.

(4) A dealer is not responsible for any action taken directly by any of its dealer data vendors or authorized integrators, or for any action the dealer takes directly in appropriately following the written instructions of any of its dealer data vendors or authorized integrators, to the extent that the action prevents it from meeting any legal obligation regarding the protection of protected dealer data or results in any liability as a consequence of such actions by the dealer data vendor or authorized integrator.

### **Other Responsibilities And Restrictions**

**30-11-719. Other responsibilities and restrictions.** All dealer data vendors and authorized integrators:

(1) may access, use, store, or share protected dealer data only to the extent permitted in the contract with the dealer;

(2) shall make any agreement regarding access to, sharing or selling of, copying, using, or transmitting protected dealer data terminable upon no more than 90 days' notice from the dealer;

(3) must, on notice of the dealer's intent to terminate its contract and in order to prevent any risk of consumer harm or inconvenience, work to ensure a secure transition of all protected dealer data to a successor dealer data vendor or authorized integrator, including but not limited to:

(a) providing unrestricted access to, or an electronic copy of, all protected dealer data and all other data stored in the dealer data system in a format that a successor dealer data vendor or authorized integrator can access and use; and

(b) deleting or returning to the dealer all protected dealer data prior to termination of the contract pursuant to any written directions of the dealer;

(4) shall provide a dealer, on request, with a listing of all entities with whom it is sharing dealer data or with whom it has allowed access to protected dealer data; and

(5) shall allow a dealer to audit the dealer data vendor's or authorized integrator's access to and use of any protected dealer data.

## North Carolina

SENATE BILL DRS45158-MW-61S

### DEALERSHIP DATA

SECTION 8. G.S. 20-305.7 reads as rewritten:

(a) Except as expressly authorized in this section, no manufacturer, factory branch, distributor, or distributor branch shall require a new motor vehicle dealer to provide its customer lists, customer information, consumer contact information, transaction data, or service files. Any requirement by a manufacturer, factory branch, distributor, or distributor branch that a new motor vehicle dealer provide its customer lists, customer information, consumer contact information, transaction data, or service files to the manufacturer, factory branch, distributor, or distributor branch, or to any third party as a condition to the dealer's participation in any incentive program or contest that is either required or voluntary on the part of the dealer, for a customer or dealer to receive any incentive payments otherwise earned under an incentive program or contest, for the dealer to obtain consumer or customer leads, or for the dealer to receive any other benefits, rights, merchandise, or services for which the dealer would otherwise be entitled to obtain under the franchise or any other contract or agreement, or which shall customarily be provided to dealers, shall be voidable at the option of the dealer, void and the dealer shall automatically be entitled to the benefits offered under the applicable incentive program or contest or any other contract or agreement, unless all of the following conditions are satisfied:

(i) the customer information requested relates solely to the specific program requirements or goals associated with such manufacturer's or distributor's own vehicle makes and does not require that the dealer provide general customer information or other information related to the dealer;

(ii) such requirement is lawful and would also not require the dealer to allow any customer the right to opt out under the federal Gramm-Leach-Bliley Act, U.S.C., Subchapter I, § 1608, et seq.; and

(iii) the dealer is not required to allow the manufacturer or distributor or any third party to have direct access to is either permitted to restrict the data fields that may be accessed in the dealer's computer system, but or the dealer is instead permitted to provide the same dealer, consumer, or customer data or information specified by the manufacturer or distributor by timely obtaining and pushing or otherwise furnishing the required data in a widely accepted file format such as comma delimited in accordance with subsection (g1) of this section. Nothing contained in this section shall limit the ability of the manufacturer, factory branch, distributor, or distributor branch to require that

the dealer provide, or use in accordance with the law, such customer information related solely to such manufacturer's or distributor's own vehicle makes to the extent necessary to do any of the following:

- (1) Satisfy any safety or recall notice obligations.
- (2) Complete the sale and delivery of a new motor vehicle to a customer.
- (3) Validate and pay customer or dealer incentives.
- (4) Submit to the manufacturer, factory branch, distributor, or distributor branch claims for any services supplied by the dealer for any claim for warranty parts or repairs.

At the request of a manufacturer or distributor or of a third party acting on behalf of a manufacturer or distributor, a dealer may only be required to provide customer information related solely to such manufacturer's or distributor's own vehicle makes for reasonable marketing purposes, market research, consumer surveys, market analysis, and dealership performance analysis, but the dealer is only required to provide such customer information to the extent lawfully permissible; to the extent the requested information relates solely to specific program requirements or goals associated with such manufacturer's or distributor's own vehicle makes and does not require the dealer to provide general customer information or other information related to the dealer; and to the extent the requested information can be provided without requiring that the dealer allow any customer the right to opt out under the federal Gramm-Leach-Bliley Act, 15 U.S.C., Subchapter I, § 6801, et seq.

No manufacturer, factory branch, distributor, or distributor branch shall access or obtain dealer or customer data from or write dealer or customer data to a dealer management computer system utilized by a motor vehicle dealer located in this State, or require or coerce a motor vehicle dealer located in this State to utilize a particular dealer management computer system, unless the dealer management computer system allows the dealer to reasonably maintain the security, integrity, and confidentiality of the data maintained in the system. No manufacturer, factory branch, distributor, distributor branch, dealer management computer system vendor, or any third party acting on behalf of any manufacturer, factory branch, distributor, distributor branch, or dealer management computer system vendor shall prohibit a dealer from providing a means to regularly and continually monitor the specific data accessed from or written to the dealer's computer system and from complying with applicable State and federal laws and any rules or regulations promulgated thereunder. These provisions shall not be deemed to impose an obligation on a manufacturer, factory branch, distributor, distributor branch,

dealer management computer system vendor, or any third party acting on behalf of any manufacturer, factory branch, distributor, distributor branch, or dealer management computer system vendor to provide such capability. Notwithstanding the terms or conditions of any incentive program or contest that is either required or voluntary on the part of the dealer, or the terms or conditions of any other contract or agreement, it shall be unlawful for any manufacturer, factory branch, distributor, or distributor branch to fail or refuse to provide dealer notice, in a standalone written document, at least 60 days prior to making any changes in any of the dealer or customer data the dealer is requested or required to share with a manufacturer, factory branch, distributor, or distributor branch, or any third party. The changes in any of the dealer or customer data the dealer is required or requested to provide shall be void unless the applicable manufacturer, factory branch, distributor, or distributor branch complies with the notice requirements contained in this paragraph.

(b1) It shall be unlawful for any manufacturer, factory branch, distributor, distributor branch, dealer management computer system vendor, or any third party having access to any dealer management computer system, to:

(1) Take any action, by contract, by technical means, or otherwise, that would prohibit or limit a dealer's ability to protect, store, copy, share, or use any customer or dealer information maintained in a dealer management computer system utilized by a new motor vehicle dealer located in this State. Unlawful conduct prohibited by this section includes, but is not limited to:

a. Imposing any unreasonable fees or other restrictions of any kind on the dealer or any third party for access to or sharing of customer or dealer information, or for writing data to a dealer management computer system. For purposes of this section, the term "unreasonable fees" means charges for access to customer or dealer data beyond any direct costs incurred by any dealer management computer system vendor in providing access to the dealer's customer or dealer data to a third party that the dealer has authorized to access its dealer management computer system or allowing any third party that the dealer has authorized to access its dealer management computer system to write data to its dealer management computer system. Any charges must be (i) disclosed to the dealer and (ii) justified by documentary evidence of the costs associated with access or it will be deemed a prohibited unreasonable fee under this section.

b. Prohibiting any third party that the dealer has authorized to access its dealer management computer system from integrating into that dealer's dealer management computer system, or placing unreasonable restrictions on integration by any authorized third party that the dealer has selected to access its dealer management computer system. Examples of unreasonable restrictions include, but are not limited to, any of the following:

1. Unreasonable restrictions on the scope or nature of the data shared with a third party authorized by the dealer to access the dealer's dealer management computer system.
2. Unreasonable restrictions on the ability of a third party authorized by the dealer to access the dealer's dealer management computer system to write data to a dealer management computer system.
3. Unreasonable restrictions or conditions on a third party authorized by the dealer to access the dealer's dealer management computer system to share customer or dealer information.
4. Requiring unreasonable access to sensitive, competitive, or other confidential business information of a third party as a condition for access to customer or dealer information or sharing customer or dealer information with any third party authorized by the dealer to access the dealer's dealer management computer system.

c. Prohibiting or limiting a dealer's ability to store, copy, securely share, or use customer or dealer information outside the dealer's dealer management computer system in any manner and for any reason.

d. Permitting access to or accessing customer or dealer information without first obtaining the dealer's express written consent in a standalone document.

(2) Engage in any act of cyber ransom. For purposes of this section, the term "cyber ransom" shall mean to encrypt, restrict or prohibit access, or threaten or attempt to encrypt, restrict, or prohibit access to a dealer's customer or dealer data for monetary gain or for political or ideological purposes.

(b2) It is unlawful for any dealer management computer system vendor or other third party who has access to any dealer management computer system to fail or refuse to:

(1) Adopt and make available a standardized framework for the exchange, integration, and sharing of data from dealer management computer systems with any party authorized to access a dealer management computer system, and retrieval of such data by any party authorized to access a dealer management computer system (use of the Standards for Technology in Automotive Retail (STAR) or a standard compatible with the STAR Standards shall be deemed to be in compliance with this requirement).

(2) Provide access to open application programming interfaces (APIs) to any party authorized to access a dealer management computer system. In the event that APIs are no longer the reasonable commercial or technical standard for secure data integration, a similar open access integration method may be provided, to the extent it provides the same or better access to any party authorized to access a dealer management computer system as an API and utilizes the required standardized framework.

(3) Access, use, store, or share any data from a dealer management computer system only to the extent permitted in its written agreement with the dealer.

(4) Make any agreement regarding access to, sharing or selling of, copying, using, or transmitting data on any dealer management computer system terminable upon no more than 90 days' notice from the dealer.

(5) Upon receipt of notice of the dealer's intent to terminate its contract and in order to prevent any risk of consumer harm or inconvenience, work to ensure a secure transition to a successor dealer management computer system vendor or any other party authorized to access a dealer management computer system. This includes, but is not limited to: (i) providing unrestricted access to all data maintained on the dealer management computer system in a commercially reasonable time and format that a successor dealer management computer system vendor or other party authorized to access a dealer management computer system can access and use and (ii) returning to the dealer all confidential or proprietary information obtained from the dealer management computer system prior to termination of the contract pursuant to any written directions of the dealer.

(6) Promptly provide a dealer, upon the dealer's request, with a listing of all entities with whom it is sharing any data from the dealer management computer system, or to whom it has allowed access to any data from the dealer management computer system.

(7) Allow and facilitate a dealer to audit the dealer management computer system vendor's access and use of its dealer management computer system and any data obtained or obtainable from its dealer management computer system.

(b3) The rights conferred on dealers in this section are not waivable and may not be reduced or otherwise modified by any contract or agreement.



## Oregon

### [ORS 650.120](#)

Definitions for ORS 650.120 to 650.170 are available at the link above, but it appears that the relevant terms are actually defined in 650.123.

### [ORS 650.123](#)

Use of protected dealer data

- prohibitions
- liabilities

(l)As used in this section:

(a)“Access fee” means a requirement to pay money for access to protected dealer data.

(b)Intentionally left blank —Ed.

(A)“Authorized integrator” means a person with which a dealer has a contractual relationship or to which the dealer otherwise gives express written authorization to have access to protected dealer data stored on a dealer data system or to write protected dealer data to the dealer data system for the purpose of performing a specific function for the dealer.

(B)“Authorized integrator” does not include:

- (i)A manufacturer, distributor or importer or any entity that is a subsidiary or affiliate of, or acts on behalf of, a manufacturer, distributor or importer; or
- (ii)A governmental body or other person that is acting in accordance with federal, state or local law or a valid court order.

(c)“Dealer data system” means software, hardware or firmware that a dealer leases or rents from a dealer management system provider for the purpose of storing protected dealer data.

(d)“Dealer management system provider” means a person that for compensation maintains and provides access to a dealer data system in which a dealer stores protected dealer data.

(e)“Protected dealer data” means:

(A) Personal data or financial data about a consumer that a dealer generated or that the consumer provided to the dealer and that is not otherwise publicly available; and

(B) Any other data to which a dealer has rights in connection with the dealer's daily business operations and stores or maintains in a dealer data system.

(2) A dealer management system provider may:

(a) Condition a dealer's or authorized integrator's access to and ability to receive, share, copy, use, write or transmit protected dealer data from or to a dealer data system on the dealer's or authorized integrator's compliance with security standards;

(b) Require an authorized integrator to have express written authorization from a dealer before allowing the authorized integrator to gain access to, receive, share, copy, use or transmit protected dealer data; and

(c) Deny access to a dealer data system to a dealer if the dealer fails to pay an amount due to the dealer management system provider under a lease, contract or other agreement concerning the dealer's access to or use of the dealer data system.

(3) Except as provided in subsection (2) of this section, a dealer management system provider may not take any action that would limit or prohibit a dealer's or an authorized integrator's ability to receive, protect, store, copy, share or use protected dealer data using means that include, but are not limited to:

(a) Imposing an access fee on a dealer or authorized integrator.

(b) Restricting a dealer or an authorized integrator from sharing protected dealer data or writing data or having access to a dealer data system. Examples of restrictions this paragraph does not permit include, but are not limited to:

(A) Limits on the scope or nature of protected dealer data to which a dealer or authorized integrator has access or may share or write to a dealer data system; and

(B) A requirement for a dealer or authorized integrator to provide sensitive or confidential business information or information that a dealer or authorized integrator uses for competitive purposes in return

for access to protected dealer data or an authorization to share or write protected dealer data to a dealer data system.

(4) Except as otherwise provided in this section, any term or condition of a contract with a dealer management system provider that conflicts with the requirements set forth in subsection (3) of this section is void and unenforceable to the extent of the conflict.

(5) Intentionally left blank —Ed.

(a) An authorized integrator shall:

(A) Obtain express written authorization from a dealer before gaining access to, receiving, sharing, copying, using, writing or transmitting protected dealer data; and

(B) Comply with security standards in gaining access to, receiving, sharing, copying, using, writing or transmitting protected dealer data.

(b) A dealer may withdraw, revoke or amend any express written authorization the dealer provides under paragraph (a)(A) of this subsection:

(A) At the dealer's sole discretion, if the dealer gives 30 days' prior notice to an authorized integrator; or

(B) Immediately, for good cause.

(6) Intentionally left blank —Ed.

(a) This section does not prevent a dealer, a dealer management system provider or an authorized integrator from discharging the dealer's, dealer management system provider's or authorized integrator's obligations under federal, state or local law to secure and prevent unauthorized access to protected dealer data, or from limiting the scope of the obligations, in accordance with federal, state or local law.

(b) A dealer management system provider is not liable for any action that a dealer takes directly with respect to securing or preventing unauthorized access to protected dealer data, or for actions that an authorized integrator takes in appropriately following the dealer's written instructions for securing or preventing unauthorized access to protected dealer data, to the extent that the actions prevent the dealer management system provider from meeting a

legal obligation to secure or prevent unauthorized access to protected dealer data.

(c)A dealer is not liable for any action that an authorized integrator takes directly with respect to securing or preventing unauthorized access to protected dealer data, or for actions that the authorized integrator takes in appropriately following the dealer's written instructions for securing or preventing unauthorized access to protected dealer data, to the extent that the actions prevent the dealer from meeting a legal obligation to secure or prevent unauthorized access to protected dealer data.

(d)An authorized integrator is not liable for any action that a dealer takes directly with respect to securing or preventing unauthorized access to protected dealer data, or for actions that the dealer takes in appropriately following the authorized integrator's written instructions for securing or preventing unauthorized access to protected dealer data, to the extent that the actions prevent the authorized integrator from meeting a legal obligation to secure or prevent unauthorized access to protected dealer data. [2019 c.500 §2]

# Utah

Section 1. Section 13-70-101 is enacted to read:

## **CHAPTER 70. MOTOR VEHICLE CONSUMER DATA PROTECTION**

### **Part 1. General Provisions**

13-70-101 . Definitions.

As used in this chapter:

(1) "Authorized integrator" means a third party with whom a franchisee enters into a contract to perform a specific function for a franchisee that allows the third party to access protected dealer data or to write data to a dealer data system, or both, to carry out the specified function.

(2) "Consumer data" means non-public personal information defined in 15 U.S.C. Sec. 6809(4) as it existed on January 1, 2024.

(3) "Cyber ransom" means to encrypt, restrict, or prohibit, or to threaten or attempt to encrypt, restrict, or prohibit a franchisee's or a franchisee's authorized integrator's access to protected dealer data or other dealer data to obtain payment not agreed to by the franchisee or the franchisee's authorized integrator in a written contract for services or goods.

(4) (a) "Dealer data system" means a software, hardware, or firmware system that is owned, leased, or licensed by a franchisee, that includes a system of web-based applications, computer software, or computer hardware, whether located at the franchisee's dealership or hosted remotely, and that stores or provides access to protected dealer data.

(b) "Dealer data system" means a dealership management system or a consumer relationship management system.

(5) "Dealer data vendor" means a third party dealer management system provider, consumer relationship management system provider, or third party vendor providing similar services that store protected dealer data pursuant to a contract with the franchisee.

(6) "Dealership" means the same as that term is defined in Section 13-14-102.

(7) "Fee" means payment for access to protected dealer data which is in addition to charges written in an executed contract for goods or services.

(8) "Franchisee" means the same as that term is defined in Section 13-14-102.

(9) "Franchisee program" means a bonus, incentive, rebate, or other payment program that a franchisor offers to a franchisee.

(10) "Franchisor" means the same as that term is defined in Section 13-14-102.

(11) (a) "Manufacturer" means a manufacturer of new motor vehicles.

(b) "Manufacturer" does not include a manufacturer acting in the capacity of a vendor, service provider, dealer data vendor, or an affiliate or subsidiary of a manufacturer operating as a vendor, service provider, or a dealer data vendor.

(c) "Manufacturer" does not include a manufacturer that does not have a franchisee in the state.

(12) "Other generally accepted standards" means security standards that are at least as comprehensive as STAR standards.

(13) "Prior express written consent" means a franchisee's express written consent to protected dealer data sharing that:

(a) is in a document separate from any other:

- (i) consent;
- (ii) contract;
- (iii) franchise agreement; or
- (iv) writing;

(b) identifies all parties with whom the protected dealer data may be shared; and

(c) contains:

- (i) all details that the franchisee requires relating to the scope and nature of the protected dealer data to be shared, including the data fields and the duration for which the sharing is authorized; and
- (ii) all provisions and restrictions that are required under federal law to allow sharing the protected dealer data.

(14) (a) "Protected dealer data" means:

- (i) consumer data that:

- (A) (I) a consumer provides to a franchisee; or  
(II) a franchisee otherwise obtains; and
- (B) is stored in the franchisee's dealer data system;

(ii) other data that relates to a franchisee's daily business operations and is stored in the franchisee's dealer data system; and

(iii) motor vehicle diagnostic data.

(b) "Protected dealer data" does not include data that:

- (i) is otherwise publicly available; or
- (ii) a franchisor or third party obtains through another source.

(15) (a) "Required manufacturer data" means data that:

(i) a manufacturer is required to obtain under federal or state law;

(ii) is required to complete or verify a transaction between the franchisee and the manufacturer;

(iii) is motor vehicle diagnostic data; or

(iv) is reasonably necessary for:

(A) a safety notice, recall notice, manufacturer field action, or other legal notice obligation relating to the repair, service, and update of a motor vehicle;

(B) the sale and delivery of a new motor vehicle or certified used motor vehicle to a consumer, including necessary data for the vehicle manufacturer to activate services purchased by the consumer;

(C) the validation and payment of consumer or franchisee incentives;

(D) claims for franchisee-supplied services relating to warranty parts or repairs;

(E) the evaluation of franchisee performance, including the evaluation of the franchisee's monthly financial statements and sales or service, consumer satisfaction with the franchisee through direct consumer contact, or consumer surveys;

(F) franchisee and market analytics;

(G) the identification of the franchisee that sold or leased a specific motor vehicle and the date of the transaction;

(H) marketing purposes designed for the benefit of franchisees, or to direct leads to the franchisee providing the dealer protected data to the franchisor;

(I) the development, evaluation, or improvement of the manufacturer's products or services; or

(J) the daily operational interactions of the franchisee with the manufacturer or other franchisees through applications hosted on the manufacturer's dealer electronic communications system.

(b) "Required manufacturer data" does not include:

- (i) consumer data on the consumer's credit application; or
- (ii) a franchisee's individualized notes about a consumer that are not related to a transaction.

(16) "Service provider" means a person that processes protected dealer data on behalf of a franchisee and that receives, from or on behalf of the franchisee, consumer protected dealer data for a business purpose pursuant to a written contract, if the contract prohibits the person from:

- (a) selling or sharing the protected dealer data;
- (b) retaining, using, or disclosing the protected dealer data for any purpose other than for the business purposes specified in the contract for the franchisee, including retaining, using, or disclosing the protected dealer data for a commercial purpose other than the business purposes specified in the contract with the franchisee, or as permitted under this title;
- (c) retaining, using, or disclosing the protected dealer data outside of the direct business relationship between the service provider and the franchisee; or
- (d) combining the protected dealer data that the service provider receives from, or on behalf of, the franchisee with personal information that the service provider receives from, or on behalf of, another person or persons, or collects from the service provider's own interaction with the consumer.

(17) "STAR standards" means the current, applicable security standards published by the Standards for Technology in Automotive Retail.

(18) (a) "Third party" means a person other than a franchisee.

(b) "Third party" includes:

- (i) a service provider;
- (ii) a vendor, including a dealer data vendor and authorized integrator;
- (iii) a manufacturer acting in the capacity of a vendor, service provider, or dealer data vendor; or
- (iv) an affiliate of a manufacturer described in Subsection (18)(b)(iii).

(c) "Third party" does not include:

- (i) a governmental entity acting pursuant to federal, state, or local law;
- (ii) a person acting pursuant to a valid court order;
- (iii) a manufacturer, not acting in the capacity of a vendor, service provider, or dealer data vendor; or
- (iv) an affiliate of a manufacturer described in Subsection (18)(c)(iii).



(19) "Vendor" means a person to whom a franchisee makes available protected dealer data for a business purpose, pursuant to a written contract with the franchisee, if the contract:

(a) prohibits the vendor from:

(i) selling or sharing the protected dealer data;

(ii) retaining, using, or disclosing the protected dealer data for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the protected dealer data for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted under this title;

(iii) retaining, using, or disclosing the protected dealer data outside of the direct business relationship between the vendor and the franchisee; and

(iv) combining the protected dealer data that the vendor receives pursuant to a written contract with the franchisee with personal information that the vendor receives from or on behalf of another person or persons, or collects from the vendor's own interaction with the consumer;

(b) includes a certification made by the vendor that the vendor understands the restrictions in Subsection (19)(a)(i) and will comply with the restrictions; and

(c) permits, subject to agreement with the vendor, the franchisee to monitor the vendor's compliance with the contract through measures, including ongoing manual reviews, automated scans, regular assessments, audits, or other technical and operational testing at least once every 12 months.

(20) "Unreasonable restriction" means:

(a) an unreasonable limitation or condition on the scope or nature of the data that is shared with an authorized integrator;

(b) an unreasonable limitation or condition on the ability of an authorized integrator to write data to a dealer data system;

(c) an unreasonable limitation or condition on a third party that accesses or shares protected dealer data or that writes data to a dealer data system;

(d) requiring unreasonable access to a franchisor's or a third party's sensitive, competitive, or other confidential business information as a condition for accessing protected dealer data or sharing protected dealer data with an authorized integrator;

(e) prohibiting or limiting a franchisee's ability to store, copy, securely share, or use protected dealer data outside of the dealer data system in any manner or for any reason; or

(f) allowing access to, or accessing protected dealer data without, the franchisee's prior express written consent.

Section 2. Section 13-70-102 is enacted to read:

13-70-102 . Applicability.

This chapter does not:

- (1) govern, restrict, or apply to data outside of a dealer data system, including data that is generated by a motor vehicle or a device that a consumer connects to a motor vehicle;
- (2) authorize a franchisee or third party to use data that the franchisee or third party obtains from a person in a manner that is inconsistent with:
  - (a) an agreement with the person; or
  - (b) the purposes for which the person provides the data to the franchisee or third party; or
- (3) except as is necessary to fulfill a franchisee's obligation to provide warranty, repair, or service to consumers, grant a franchisee:
  - (a) ownership of motor vehicle diagnostic data; or
  - (b) rights to share or use motor vehicle diagnostic data.

Section 3. Section 13-70-201 is enacted to read:

## **Part 2. Data Protection Regulations**

13-70-201 . Data submissions to franchisors or third parties.

- (1) A franchisor or third party may not require a franchisee to grant to the franchisor, third party, or person acting on behalf of the franchisor or third party, direct or indirect access to the franchisee's dealer data system.
- (2) A franchisee may submit or push data or information to a franchisor or third party through an electronic file format or protocol if the electronic file format or protocol:
  - (a) is widely accepted; and
  - (b) complies with:
    - (i) STAR standards; or
    - (ii) other generally accepted standards.

Section 4. Section 13-70-202 is enacted to read:

13-70-202 . Service provider contracts -- Franchisors and third parties --

## Prohibitions -- Requirements.

(1) (a) A service provider contract may permit the franchisee to monitor the service provider's compliance with the contract through ongoing manual reviews, automated scans, regular assessments, audits, or other technical and operational testing, at least once every 12 months.

(b) If a service provider or vendor engages another person to assist the service provider or vendor in processing protected dealer data for a business purpose on behalf of the franchisee, or if another person engaged by the service provider or vendor engages a person to assist in processing protected dealer data for that business purpose, the service provider or vendor shall notify the franchisee of that engagement, and the engagement shall be pursuant to a written contract binding the person to observe all the requirements described in Subsection 13-70-101(16).

(2) A franchisor or third party may not:

(a) access, share, sell, copy, use, or transmit protected dealer data without prior express written consent;

(b) engage in any act of cyber ransom; or

(c) take action to prohibit or limit a franchisee's ability to protect, store, copy, share, or use protected dealer data, including:

(i) imposing a fee for, or other restriction on, the franchisee or authorized integrator:

(A) accessing or sharing protected dealer data;

(B) writing data to a dealer data system; or

(C) submitting or pushing data or information to the third party under Subsection 13-70-201(2);

(ii) unreasonably prohibiting a third party or an authorized integrator that satisfies STAR standards or other generally accepted standards from integrating into the franchisee's dealer data system; or

(iii) placing an unreasonable restriction on integration by an authorized integrator or third party.

(3) (a) Notwithstanding Subsection (2)(c)(i)(A), a franchisor or a third party may charge a franchisee the franchisor's or third party's actual third party costs, including a reasonable profit margin for providing access to protected dealer data to a franchisee, authorized integrator, or other third party if the franchisor or third party:

(i) discloses the charge to the franchisee in writing; and

(ii) upon written request by the franchisee, provides to the franchisee documentation that the charges were agreed to in writing by the franchisee or provided for in the contract for services or goods.

(b) If a third party fails to comply with Subsection (3)(a), a charge described in Subsection (3)(a) is a fee prohibited under Subsection (2)(c)(i).

(4) (a) A franchisee may unilaterally revoke or amend the prior express written consent described in Subsection (2)(a):

(i) with 60 days notice without cause; or

(ii) immediately for cause.

(b) (i) Except as provided in Subsection (4)(b)(ii), a franchisor may not seek or require prior express written consent as a condition of or factor for consideration or eligibility for a:

A) franchisor program;

(B) standard or policy; or

(C) benefit to a franchisee.

(ii) If a franchisor's program reasonably requires delivery of information that is protected dealer data to qualify for the program and receive franchisor program benefits, a franchisee shall provide the information to participate in the franchisor program.

(5) This section does not:

(a) limit a franchisee's, franchisor's, or third party's obligations:

(i) as a service provider;

(ii) under federal, state, or local law, to protect and secure protected dealer data; or

(iii) regarding required manufacturer data; and

(b) require a franchisor to pay a benefit to a franchisee if the franchisee refuses to provide data reasonably necessary to participate in the franchisor program.

(6) A franchisor or franchisor's selected third party may not require a franchisee to pay a fee for sharing required manufacturer data if:

(a) the franchisor requires a franchisee to provide required manufacturer data through a specific third party that the franchisor selects;

(b) the franchisor does not allow the franchisee to submit the required manufacturer data using the franchisee's choice of a third party vendor;

(c) the franchisee's data is in a format that is compatible with the format required by the franchisor; and

(d) the third party vendor satisfies the STAR standards or other generally accepted standards.

(7) A franchisor may not access, sell, copy, use, transmit, or require a franchisee to share or provide access to protected dealer data, unless:

- (a) the protected dealer data is required manufacturer data; or
- (b) the franchisee provides prior express written consent.

(8) A franchisor may only use required manufacturer data that the franchisor obtains from a dealer data system for the purposes described in Subsection 13-70-101(14).

(9) (a) A franchisor, authorized integrator, or other third party shall indemnify a franchisee for any claims or damages if:

- (i) the claims or damages directly result from a violation of this section by the party from whom the franchisee is seeking indemnification;
- (ii) the claims or damages directly result from a violation of this section by:

- (A) a vendor or contractor as an agent acting on behalf of the party from whom the franchisee is seeking indemnification; or
- (B) a vendor or other service provider who the party from whom the franchisee is seeking indemnification required the franchisee to use; and

(iii) the claims or damages result from a violation of this section for:

- (A) accessing or providing access to protected dealer data;
- (B) using protected dealer data; or
- (C) disclosing protected dealer data.

(b) A franchisee bringing a cause of action against a franchisor, authorized integrator, or other third party for a violation of this section has the burden of proof.

(10) Notwithstanding Subsection (6), this chapter does not restrict or limit a franchisor's right to:

- (a) access or obtain required manufacturer data;
- (b) use, share, copy, or transmit required manufacturer data for the purposes described in Subsection 13-70-101(15); or
- (c) use or control data that is:
  - (i) proprietary to the franchisor;
  - (ii) created by the franchisor;
  - (iii) obtained from a source other than the franchisee; or
  - (iv) public information.

Section 5. Section 13-70-203 is enacted to read:

13-70-203 . Dealer data vendors -- Authorized integrators -- Requirements.

- (1) (a) A dealer data vendor shall adopt and make available to a franchisee and authorized integrator in a standardized framework:
  - (i) the exchange, integration, and sharing of data between a dealer data system and an authorized integrator; and
  - (ii) the retrieval of data by an authorized integrator.(b) The standardized framework described in Subsection (1)(a) shall comply with STAR standards or other generally accepted standards.
  
- (2) (a) Except as provided in Subsection (2)(b), a dealer data vendor shall provide to an authorized integrator access to open application programming interfaces for the standardized framework described in Subsection (1) that meet the reasonable commercial or technical standard for secure data integration.
  - (b) If the open application interfaces described in Subsection (2)(a) do not meet the reasonable commercial or technical standard for secure data integration, a dealer data vendor may provide to an authorized integrator a similar open access integration method that:
    - (i) provides the same or better access; and
    - (ii) uses the standardized framework described in Subsection (1).
  
- (3) A dealer data vendor and an authorized integrator:
  - (a) may access, use, store, or share protected dealer data or any other data from a dealer data system only to the extent allowed in the written agreement with the franchisee;
  - (b) shall, upon a franchisee's request, provide the franchisee with a list of all persons:
    - (i) with whom the dealer data vendor or authorized integrator is sharing, or has shared, protected dealer data; or
    - (ii) to whom the dealer data vendor or authorized integrator has allowed or is allowing access to protected dealer data; and
  - (c) shall allow a franchisee to audit the dealer data vendor's or authorized integrator's access to and use of protected dealer data.
  
- (4) A franchisee may terminate an agreement between a dealer data vendor or authorized integrator and the franchisee relating to access to, sharing of, selling of, copying, using, or transmitting protected dealer data upon 90 days' notice.
  
- (5) (a) If a dealer data vendor or authorized integrator receives a franchisee's notice described in Subsection (4), the dealer data vendor or authorized integrator shall ensure a secure transition of all protected dealer data to a successor dealer data vendor or successor authorized integrator.
  - (b) In fulfilling the dealer data vendor's or authorized integrator's duties under Subsection (5)(a), a dealer data vendor or authorized integrator shall:
    - (i) provide access to or an electronic copy of all protected dealer data and all other data stored in the dealer data system in:
      - (A) a commercially reasonable time; and
      - (B) a format that the successor dealer data vendor or successor authorized integrator can access and use; and

(ii) before the agreement terminates, delete or return to the franchisee all protected dealer data pursuant to the franchisee's written directions.

Section 6. Effective date.

This bill takes effect on May 1, 2024.