EXC-02 Executive & Analytics Track: Product Overview | 25 Minutes 2026

Customer Privacy and Data Protection

TEKION ONE

Your Monday Morning Outcome

By following this guide, you will have your Data Privacy Preferences configured, your third-party app list audited, your customer request workflow operational, and a documented breach response sequence – so your dealership can demonstrate compliance when a regulator, customer, or breach forces the issue.

Before You Start

Pre-Implementation Checklist

- **Third-party app inventory complete**

  Complete list of every application receiving customer data from your DMS (marketing platforms, OEM portals, credit bureaus, lead providers).

- **Legal counsel contact confirmed**

  Outside legal counsel who will handle breach notification and regulatory filings. Contact information documented.

- **Security officer designated**

  FTC Safeguards Rule requires a designated security officer (since 2003). Confirm who holds this role.

- **State privacy requirements identified**

  Confirm which states your customers reside in. CPRA: 45 days. 18+ state laws with varying deadlines. Quebec: 72 hours.

- **Baseline captured**

  Note whether pending customer privacy requests exist and how they are currently tracked.

Before You Start

Setting	Configuration
Retention Period (Tab 1)	Default 6 years. Covers FTC 2-year disposal floor and state statutes. Do not reduce below 6.
Data Export Settings (Tab 2)	Controls what customer data can be exported. Not all fields should go out by default.
3rd Party Apps (Tab 3)	Every vendor receiving customer data must be listed and reviewed for Safeguards, Affiliate Marketing, and TCPA exposure.
Email Configurator (Tab 4)	Select all notification types. Creates the audit trail for every customer privacy request.

STEP 01/04

Configure Retention Period and Data Export Settings

Time: 15 minutes | **Navigation:** ARC → Core → Data Privacy Preferences → Tabs 1 and 2

Setting	Configuration
Retention Period	6 years (default) or longer per your policy. Covers FTC disposal floor and state statutes of limitations.
Data Export Fields	Review and restrict per vendor agreement. Internal ops fields (lead scoring, attribution) excluded by default.
Third-Party Redistribution	Confirm export settings align with vendor data sharing agreements. Unauthorized export = compliance risk.

CHECKPOINT

Retention Period is 6 years or greater. No fields exported beyond what vendor agreements require.

STEP 02/04

Audit and Configure 3rd Party Apps

Time: 20 minutes | **Navigation:** ARC → Core → Data Privacy Preferences → Tab 3

Setting	Configuration
Every vendor with customer data	Listed, reviewed, and configured. Unlisted vendors are invisible compliance exposure.
Safeguards Rule coverage	If vendor list includes any indication of financing or nonpublic financial info, it is covered. Safest posture: treat every entry as covered.
FTC Affiliate Marketing Rule	Vendors marketing back to your customers using your data trigger opt-out obligations.
TCPA / CAN-SPAM exposure	Vendors sending texts or emails on your behalf must honor opt-out within 10 days. CAN-SPAM ~$46,000/email. TCPA ~$44,000/call.

CHECKPOINT

Every vendor listed. For each: what data they receive, whether they market back, and whether opt-out meets the 10-day window.

STEP 03/04

Configure Email Notifications and Customer Request Handling

Time: 15 minutes | **Navigation:** ARC → Core → Data Privacy Preferences → Tab 4 | ARC → Data Privacy Requests log

Setting	Configuration
Email Configurator (Tab 4)	Select all notification types. Default is everything unchecked = no acknowledgment, no audit trail.
Verify Contact Toggle	Always ON. You must verify customer identity before touching their data. Every regulation requires it.
Red Flag Monitoring	Check dashboard weekly. Red = outside your legal response window. That is an action item, not a warning.
Supporting Documents	Upload for every request. Email copies, chat screenshots, phone conversation notes. Your evidence file.

CHECKPOINT

All notification types ON. Test deletion request submitted. Acknowledgment email sends. Request appears in log with correct status.

STEP 04/04

Document Your Breach Response Plan

Time: 15 minutes

Phase	Actions
Secure Your Operations	Take affected equipment offline (do not turn off). Lock physical areas. Change access codes. Mobilize response team.
Fix Vulnerabilities	Review service provider access. Check network segmentation. Work with forensics. Prepare communications plan.
Notify Appropriate Parties	Notify law enforcement first. Download audit files from ARC. File with FTC at ftc.gov via Safeguards Rule compliance resources.
Document Contacts	Single page: outside legal counsel, security officer, forensics provider, FTC filing URL, state AG contacts. Distribute to response team.

CHECKPOINT

All contact fields populated. Breach response document printed and distributed to every member of the response team.

Measure Your Results

Report	Navigation	What to Look For
Data Privacy Requests log	ARC → Data Privacy Requests	Request volume, response time, overdue items (red flags).
3rd Party Apps inventory	Data Privacy Preferences → Tab 3	Every vendor listed. Marketing and TCPA exposure flagged.
Email audit trail	Tab 4 + request log	Confirmations sending for every request stage.

Best Practices

- **Treat every entry on the 3rd Party Apps screen as covered**

  The safest posture eliminates ambiguity. Configure every vendor as if they hold customer financial information.

- **Make the dashboard part of your weekly review**

  Red flags are action items, not warnings. Data Privacy Requests dashboard: weekly during Month 1, then monthly.

- **Do not let front-line staff fulfill requests directly**

  They recognize and route. The Controller or compliance lead fulfills.

Common Pitfalls

What You See	Likely Cause	Fix
No audit trail for customer requests	Email Configurator left at defaults (everything unchecked)	Tab 4: select all notification types. Two minutes.
Unknown vendors receiving customer data	3rd Party Apps list incomplete – vendors onboarded by different departments	Make this screen mandatory for every vendor onboarding.
No breach response plan exists	Assumed it would not happen or counsel would handle it	Complete Step 4 on Day 1. Single page. Distribute. Review quarterly.

Workflow Integration

Role	Responsibility
Controller	Owns Data Privacy Preferences configuration. Approves retention and export settings. Finalizes breach response contacts.
Office Manager	Manages customer privacy request queue. Monitors dashboard. Trains front-line staff on routing.
Front-Line Staff	Recognize and route customer privacy requests. Do not attempt to fulfill.
Legal Counsel	Reviews breach response sequence. Confirms state notification requirements.