October 22-25, 2026 I Sheraton Boston Hotel

MAIA'S BIG EVENT 2026

Conference & Trade Show

Celebrating Independence!

10/24/2026
2:30 pm - 3:30 pm

Privacy & Ethics with RMV

Privacy and Ethics with RMV

Marlie M. Waterman, CISR
Massachusetts Association of Insurance Agents

FDPPA Overview

Federal Driver Privacy Protection Act (FDPPA)

The Federal Driver Privacy Protection Act (FDPPA), imposes restrictions on the disclosure of "personal information" contained in motor vehicle records. DPPA, which went into effect in 1997, limits to whom and for what purpose personal information can be disclosed.

FDPPA

Federal Driver Privacy Protection Act (FDPPA)

Definition of Personal Information. Under the DPPA, personal information is broadly defined and includes:

- Name
- Address
- Driver License Number
- Social Security Number
- Photo Image
- Medical Information

FDPPA

Federal Driver Privacy Protection Act (FDPPA)

Permitted Users include 14 different groups. Agents fall under number 6 of the 14:

6. **For use by an insurer or insurance support organization, or by a self-insured entity, or it's agents,** employees, or contractors, in connection with **claims investigation activities, anti-fraud activities, rating or underwriting.**

FDPPA

Federal Driver Privacy Protection Act (FDPPA)

Penalties for Violations

- Under the federal law, a state may be subject to a civil penalty of up to $5,000 per day, for each day of substantial noncompliance.
- A person who knowingly obtain, discloses or uses personal information for purposes not permitted under DPPA, may be liable to individuals that the information relates. The court may award the greater of actual damages or $2,500 punitive damages upon proof of willful or reckless disregard of the law, the attorney's fees and costs.



FDPPA

Federal Driver Privacy Protection Act (FDPPA)

Personal Information DOES NOT include:

- Vehicular accidents
- Driving violations (including citation information)
- Driver's status
- Vehicle-specific information (which does not identify an individual)
- Company or business information (which does not identify an individual)



FDPPA

Federal Driver Privacy Protection Act (FDPPA)

The Agent's Role

Agents access to driver records is limited to:

- C. 123, § 2721 (b),(6) – for use by an insurer or insurance support organization or by a self-insured entity, or its agents, employees, or contractor*, in connection with claims investigation activities, antifraud activities, rating or underwriting*; or
- C. 123, § 2721 (b), (9) – for use by an employer or its agent or insurer to obtain or verify information to a *holder of a commercial driver's license* that is required under the Commercial Motor Vehicle Safety Act of 1986 (49 U.S.C. App. 2710 et. Seq)



FDPPA

Federal Driver Privacy Protection Act (FDPPA)

The Agent's Role

The use of personal information by anyone (including insurance agents) for any other purpose would be governed by:

- C. 123, § 2727, (c) – Resale or Redisclosure – An authorized recipient of personal information (except a recipient under subsection (b)(11) or (12)) may resell or redisclose the information only for a use permitted under subsection (b)(but not for uses under subsection (b)(11) or (12)). An authorized recipient under subsection (b)(11) may resell or redisclose personal information for any purpose. An authorized recipient under subsection (b)(12) may resell or redisclose personal information pursuant to subsection (b)(12). ***Any authorized recipient*** (except a recipient under subsection (b)(11)) ***that resells or rediscloses personal information*** covered by this title ***must keep for a period of 5 years records identifying each person or entity that received information and the permitted purpose for which the information will be used and must make such records available to the motor vehicle department upon request.***



FDPPA

Federal Driver Privacy Protection Act (FDPPA)

The Agent's Role

Redisclosure of personal information by an insurance agent would still require that the requestor be a permitted user and would impose the additional requirement of retaining records for a 5-year period upon the agent.



FDPPA

Federal Driver Privacy Protection Act (FDPPA)

Definitions (FDPPA § 2727)

- **Motor vehicle record** means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration or identification card issued by a department of motor vehicles.
- **Person** means an individual, organization or entity, but does not include a state or agency thereof;



FDPPA

Definitions (FDPPA § 2727)

- **Personal Information** means information that:
  a. Identifies an individual, including an individual's photograph,
  b. Social security number,
  c. Driver identification number,
  d. Name,
  e. Address (but not the 5-digit zip code),
  f. Telephone number, and
  g. Medical or disability information
  h. But does not include:
    - Vehicular accidents
    - Driving Violations, and
    - Driver Status



FDPPA

Federal Driver Privacy Protection Act (FDPPA)

Definitions (FDPPA § 2727)

- **Highly restricted personal information** means an:
  a. Individual's photograph or image,
  b. Social security number,
  c. Medical or disability information;
- **Express Consent means** consent in writing, including consent conveyed electronically that bears an electronic signature as defined in section 106(5) of Public Law 106-229



RMV Driving Records

- **Revised Driving Records and DPPA Forms**
- The Driving Record Request Form and the Request for Personal Information RMV Records have both been revised due to the Work and Family Mobility Act requirements. A photocopy of the license/ID of the license holder/requestor/authorized recipient is required with both forms.

RMV Driving Records

- **Revised Driving Records and DPPA Forms**
- **Driving Record Request Form**

The revised Driving Record Request Form (DCU100) has a date "0923" in the lower right corner and is available online.

- **Request for Personal Information RMV Records**

The revised Request for Personal Information RMV Records (DCU140) has a date of "0923" in the lower right corner and is available online.

RMV Driving Records

- **Revised Driving Records and DPPA Forms**
- **Who can Request a Driving Record**
- All of the following can request a driving record:
  1. The data subject (license holder) using the *Driving Record Request Form*.
  2. An authorized recipient with authorization from the data subject using the *Driving Record Request Form*.
  3. A 3rd. Party DPPA requester using the *Request for Personal Information RMV Records.*



RMV Driving Records

- **Revised Driving Records and DPPA Forms**
- **How can you Request a Driving Record?**
- **Online: myRMV**
  - Data subjects may request their own driving record (either Unattested or True & Attested) by logging into their profile via myRMV.
- **Contact Center**
  - Data subject can request their own True & Attested driving record by calling the Contact Center. The driving record may ONLY be sent to the address on file.



RMV Driving Records

- **Revised Driving Records and DPPA Forms**
- **How can you Request a Driving Record?**
- **By Mail**
  - Driving records can be processed via mail. <u>All mailed requests must be accompanied by proper identification documentation. The documentation will vary depending on who is making the request:</u>
    - Data subjects will need to submit a completed *Driving Record Request Form,* the applicable fee, and a photocopy of their license/ID (or they can go to their myRMV profile to request their record).
    - Authorized recipients will need to submit a completed *Driving Record Request Form* signed by the license holder and the certification signed by the authorized recipient, the applicable fee, and a photocopy of both the license holder's and the authorized recipient's license/ID.
    - DPPA requestors will need to submit a completed *Request for Personal Information RMV Records form* with the certification signed by the requestor, the applicable fee, and a photocopy of the requestor's license/ID.

RMV Driving Records

- **Revised Driving Records and DPPA Forms**
- **How can you Request a Driving Record?**
- **In-Person**
- Service Centers may process data subject and "authorized recipient" driving record requests.
  - Data subjects will need to provide a completed *Driving Record Request Form*, the applicable fee, and the clerk will verify that the requestor is the data subject. If there is any doubt that the requestor is the data subject, the clerk must request to see their license/ID.
  - Authorized recipients will need to provide a completed *Driving Record Request Form* signed by the license holder and the certification signed by the authorized recipient, the applicable fee, and a photocopy of both the license holder's and the authorized recipient's license/ID.

RMV Driving Records

- **Revised Driving Records and DPPA Forms**
- **How can you Request a Driving Record?**
- **Court Records** may process all driving record requests, regardless of the requestor. The documentation will vary depending on who is making the request:
  - Data subject will need to provide a completed Driving Record Request Form, the applicable fee, and the clerk will verify that the requestor is the data subject. If there is any doubt that the requestor is the data subject, the clerk must request to see their license/ID.
  - Authorized recipients will need to provide a completed Driving Record Request Form signed by the license holder and the certification signed by the authorized recipient, the applicable fee, and a photocopy of both the license holder's and the authorized recipient's license/ID.
  - DPPA requestors will need to submit a completed Request for Personal Information RMV Records form with the certification signed by the requestor, the applicable fee, and a photocopy of the requestor's license/ID.



RMV Driving Records

- **Revised Driving Records and DPPA Forms**
- **Online Driving Records**
- Effective immediately, the "Request a Driving Record" online transaction is available again. It had been temporarily disabled.
- <u>The online transaction was changed to allow customers to request only their own driving records. The option to request somebody else's driving record has been removed, as this can no longer be done online.</u> Customers who want to request a driving record for themselves must log into their profile first and then request the driving record option.



DVS Program

- **The Driver Verification System (DVS) Program**
- The Driver Verification System (DVS) is a program that improves public safety in Massachusetts. DVS give your commercial clients the ability to track license statuses of their drivers and receive email notification from the RMV if there is a change in their license status at any time while the business is enrolled in DVS.
- You may use the eService Portal Driver Verification System (DVS) program to check the driving record of a potential new driver for your business in addition to existing employees.
- This is great news as this takes you, the agent, out of the loop to look at driving records for potential new hires!



DVS Program

- **The Driver Verification System (DVS) Program**
- **New Certification Language in the eService Portal**
- New language was added to the summary screen when adding a new subscribed driver.
- This language ensures that access to individual driving records and data is provided only to permissible users for permissible uses as required under the DPPA, 18.U.S. Code s. 2721.



DVS Program

- **The Driver Verification System (DVS) Program**
- The new language is:
  - *By clicking submit below, and accessing the required RMV data, you certify that this driver is your employee or a candidate for employment at your business and that you obtained their written consent to access their driving record and license status. The driver/employee or candidate understands that you will be able to access their driving history and/or receive notification of any change to their license status.*



DVS Program

- **The Driver Verification System (DVS) Program**
- What is DVS?
- DVS has two functions:
  1. The ability to track driver's license status of your current and/or future drivers/employees and receive email notification from the RMV if there is a change in the license status at any time while they are enrolled/subscribed in DVS. The DVS program will return the following data:



DVS Program

- **The Driver Verification System (DVS) Program**
- The DVS program will provide the following information for any driver enrolled:
  - License class held (CDL, Passenger, Motorcycle),
  - License status and Expiration Date
  - Organ Donor
  - Restrictions and Endorsements
  - 7D School Bus Certificate Expiration Date
  - CDL Self Certification Type & Expiration Date

DVS Program

- **The Driver Verification System (DVS) Program**
- The DVS program will provide the following information for any driver enrolled:
  - License class held (CDL, Passenger, Motorcycle),
  - License status and Expiration Date
  - Organ Donor
  - Restrictions and Endorsements
  - 7D School Bus Certificate Expiration Date
  - CDL Self Certification Type & Expiration Date

DVS Program

- **The Driver Verification System (DVS) Program**
  2. Allows you to request Driving Record of any current or future employee/driver enrolled in the program. The Driving Record is an Unattested Driving Record includes all surchargeable accidents, criminal and civil driving offenses for which a person was found either guiltily or responsible, plus discretionary, and administrative license suspension actions.



DVS Program

- **The Driver Verification System (DVS) Program**
- **What to know about the DVS Program?**
- Before you enroll any driver/employee you must obtain their written consent to access their driving record and/or license status. (this is an RMV form and not just a note).
- You are required to provide the license number, date of birth, and last and first name for each driver that is being enrolled in the DVS program.
- You are also required to delete any driver that is no longer in your employment or has not been hired.



DVS Program

- **The Driver Verification System (DVS) Program**
- **Who can participate in the DVS Program?**
- DVS is available to RMV permitted users as stated in Section 1 of the Agreement for Access to Records and Data Maintained by the Registry of Motor Vehicles.
- When the customer received a DVS notification via email you are required to log into your DVS account to view the driver(s) that has had a status change. DVS also allows you to obtain driving records for any driver enrolled in the DVS program.

DVS Program

- **The Driver Verification System (DVS) Program**
- The DVS Program also allows you to request and Unattested Public Driving Record. The Public Driving Record includes all surchargeable accidents, criminal and civil driving offenses for which a person was found either guilty or responsible, plus discretionary and administrative license suspension actions.
- The DVS program is FREE, however, the Unattested Public Driving Records are $8 and will be billed to the business account each month.

DVS Program

Driver Verification System (DVS) Program

- Customers can contact the RMV directly for this program:

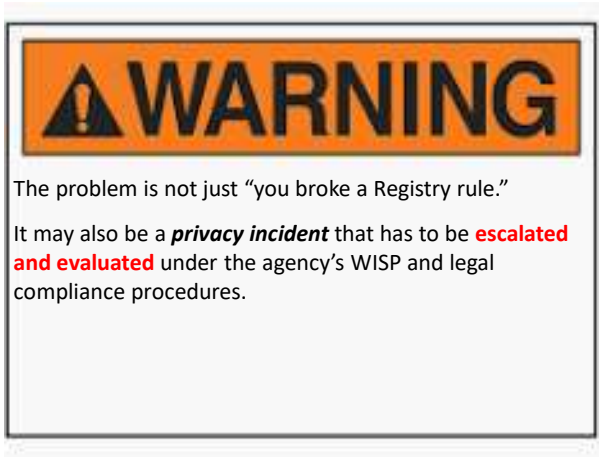
  Kristen Hagan: 857-368-7243 or Kristen.Hagan@dot.state.ma.us



RMV Privacy Ethics

Access Is Only the Beginning

- Employees who access RMV data are **handling legally protected personal information**.
- The duty is not only to access it lawfully, but also **to protect, limit, and properly handle it.**
- Improper access or disclosure can create individual and agency consequences.



The problem is not just "you broke a Registry rule."

It may also be a ***privacy incident*** that has to be **escalated and evaluated** under the agency's WISP and legal compliance procedures.

MAIA'S BIG EVENT 2026 Conference & Trade Show Celebrating Independence!

Having Registry access does not end the agency's responsibility.

- **DPPA**
- restricts who may obtain, use, or disclose personal information from
- motor vehicle records.
- **Massachusetts state regulation 201 CMR 17**
- requires protecting personal information (ie driver's license info, etc.) through
- administrative, physical, and technical safeguards including:
  - ✓ Restricting access to sensitive data and enforcing role-based controls
  - ✓ Regularly monitoring and updating security measures
- AND 201 CMR 17 mandates **civil penalties and legal action** by the Massachusetts Attorney General for non-compliance.
- **Massachusetts Identity Theft Act**
  - is designed to reduce the risk of identity theft or fraud when personal information is breached, misused, or accessed for an unauthorized purpose.

KEY POINTS

Privacy compliance is **part of the agency's duty to handle sensitive information responsibly.**

MAIA'S BIG EVENT 2026 Conference & Trade Show Celebrating Independence!

RMV Data Triggers More Than DPPA



- **DPPA answers the access question:**
- Who may obtain, use, or disclose RMV personal information, and for what permitted purpose?
- **Massachusetts Identity Theft Act answers the incident question:**
- What happens if personal information is acquired, used, or disclosed without authorization?
- **201 CMR 17.00 answers the safeguard question:**
- What written, administrative, technical, and physical safeguards must the agency maintain to protect personal information?

Once legally protected RMV information enters the agency workflow, the duty is not only to access it properly — **it must also be protected, limited, monitored, and escalated** if something goes wrong.

MAIA'S BIG EVENT 2026
Conference & Trade Show
Celebrating Independence!

Compliance Asks, "Can I?" Ethics Asks, "Should I?"

Both questions matter — and they are not the same question.

Can I?	Should I?
Is there a legal or contractual rule that permits access?	**Is there a legitimate insurance reason, a need to know, and a record I can defend?**

The AHA! Moment

"Because I can access it" is not the same as "I should access it."

The privacy rules explain access. **Ethics explains judgment.**

MAIA'S BIG EVENT 2026
Conference & Trade Show
Celebrating Independence!

Penalties and consequences are not theoretical

DPPA/201 CMR 17/Identity Theft Act exposure

Knowingly obtaining, disclosing, or using personal information for a non-permitted purpose **can create individual liability**. Courts may award actual damages or statutory damages, punitive damages for willful/reckless conduct, and attorney fees/costs.

Agency exposure

- Licensing/regulatory issues
- E&O allegations
- Employment discipline
- Carrier/market concerns
- Loss of client trust

Ethical point

DPPA history is tied to **real-world misuse** of motor vehicle data by stalkers, harassers, and criminals.
That is why this topic belongs in ethics, not only in compliance.

MAIA'S BIG EVENT 2026 Conference & Trade Show Celebrating Independence!

Why RMV Data Is Different



This is not ordinary customer-service information.

- RMV data can include information that identifies a person and helps locate them.
- Name, address, and driver license number are not casual lookup items.
- A misuse may create safety concerns, privacy harm, agency liability, and reputational damage.
- The ethical starting point is **respect for the individual** behind the record.

To agency staff, an RMV record may look like routine transaction data.
But under the DPPA, **it is legally protected personal information** that can identify an individual and may include information tied to that person's location, identity, or safety.

MAIA'S BIG EVENT 2026 Conference & Trade Show Celebrating Independence!

The 30- Second Ethical Test

A practical pause before accessing, using, or sharing RMV information.

1 **Purpose**	Is this for claims, anti-fraud, rating, or underwriting?
2 **Need**	Do I need this information to do my assigned job?
3 **Authority/Permission**	Am I relying on the agency's authorized RMV access for the correct purpose?
4 **Documentation**	Could I explain the lookup in an audit or E&O file?
5 **Minimum use**	Am I using only what is needed and nothing more?

When the answer is unclear, do not *just look it up*.

Escalate first!



MAIA'S BIG EVENT 2026 Conference & Trade Show Celebrating Independence!

Stay in the Agent's Permitted-Use Lane

The insurance lane is **narrow for a reason.**



- Claims investigation activities.
- Anti-fraud activities.
- Rating or underwriting.
- **Not personal curiosity, employment screening, favor requests, neighborhood disputes, or general client convenience.**

If it is not tied to a legitimate insurance function assigned to the agency, **stop and ask** before accessing or sharing RMV information.

Because the data is legally protected, agencies must control who accesses it, why they access it, how it is documented, and whether it may be shared.

MAIA'S BIG EVENT 2026 Conference & Trade Show Celebrating Independence!

Starts With the Agency's Certification

The agency's signed **authority does not belong to the individual employee.**

Staff are using the agency's access, so **every lookup must fit the agency's permitted purpose.**



Every Login Is a Certification



- The RMV End User Access Policy **makes the user's responsibility *personal***.
- Transactions are ***recorded, stored, monitored, and audited***.
- The RMV may require the user to explain or demonstrate the legitimate business purpose for accessing RMV data.
- Password sharing is not allowed.
- By logging in, ***the user certifies compliance under the pains and penalties of perjury.***

Curiosity Is Not a Business Purpose

The easiest **misuse** is often the most casual one.

- Do not look up neighbors, relatives, ex-spouses, friends, coworkers, celebrities, claimants outside your file, or people involved in a personal dispute.
- Do not access a record because someone "just wants to know."
- Do not use agency access to solve personal problems or satisfy curiosity.
- **ONE improper lookup can undermine the agency's trust, controls, and audit position.**



If the reason would sound bad when said out loud to a regulator, carrier, client, or judge, **do not do it.**

Ethical Redisclosure

Access is limited. **Sharing is limited too.**

- Do not assume information may be passed along because the agency obtained it properly.
- Redisclosure should be tied to a **permitted purpose** and a legitimate need to know.
- Be careful with emails, screenshots, printouts, downloads, and file notes that include RMV-derived information.
- If the agency cannot explain who received the information and why, pause before disclosing.



Client Service Has Limits

Being helpful does not make every request proper.

A client's request does not automatically create a permitted purpose.

- ***"Can you look up who owns this car?"*** is not an insurance underwriting reason by itself.
- ***"Can you check my applicant's driving record?"*** belongs with the employer's own authorized process — not the agent's RMV access.
- Agencies should be prepared to say: ***"We can't use our RMV access for that purpose."***

Professional boundary

Ethical service includes **saying no** when a request turns agency access into a personal, HR, or investigative shortcut.



MAIA'S BIG EVENT 2026 Conference & Trade Show Celebrating Independence!

Driver Verification System (DVS) Program : Keep the Agent Out of Employer Screening

DVS is useful — **but it is not an agency workaround.**

- DVS is designed for businesses to monitor current and/or prospective employee drivers through their own authorized process.
- The business must obtain the driver's written consent before enrollment/access.
- When a commercial client needs ongoing driver monitoring, **point them to the proper RMV process.**
- Do not let agency access become the client's informal HR screening tool.

The agent can **educate the client** about the existence of DVS, but should not become the employer's substitute access point.



MAIA'S BIG EVENT 2026 Conference & Trade Show Celebrating Independence!

Proper Access Still Requires Secure Transmission

Secure Transmission Is Not Just Best Practice

🔐 **Encryption is required when personal information is transmitted electronically**

201 CMR 17.00 requires encryption of personal information when they travel across public networks and transmitted wirelessly, where technically feasible.

📤 **Open email may not be appropriate for driver/MVR information**

Use the carrier portal, secure upload, encrypted email, or another approved secure method.

👤 **Verify the recipient before sending**

A proper underwriting, rating, claims, or anti-fraud purpose can still become **a privacy problem if the information is sent to the wrong person or through an insecure method.**



MAIA'S BIG EVENT 2026 Conference & Trade Show Celebrating Independence!

Ethics Requires a System

Good intentions are not enough when staff have access to legally protected RMV information.

📋 **A WISP**

- gives the agency written procedures for storing, accessing, transmitting, and protecting personal information.

🔐 **Access controls**

- help ensure only authorized staff can view protected information.

🎓 **Training**

- helps employees recognize improper requests, casual misuse, and reporting duties.

🔎 **Monitoring and audits**

- help the agency identify unusual access or weak procedures.

🚨 **Incident-response procedures**

- tell staff what to do when information is accessed, sent, or disclosed improperly.

Discipline

- reinforces that privacy is an agency standard.

MAIA'S BIG EVENT 2026 Conference & Trade Show Celebrating Independence!

Agency Controls That Support Ethical Behavior

Controls make **the right choice easier** — and **the wrong choice harder.**

Access	Unique credentials, role-based access, MFA, no shared logins.
Use	Document the business reason; avoid unnecessary screenshots, downloads, or printouts.
Storage	Keep records secure; do not leave RMV records visible or unattended.
Disposal	Shred or securely delete when the business purpose has expired.
Oversight	Periodic review, training refreshers, and escalation procedures. Deactivate access promptly when employees leave or roles change.



To explain the legitimate business reason for a transaction if questioned later.

MAIA'S BIG EVENT 2026 Conference & Trade Show Celebrating Independence!

When Something Goes Wrong

The ethical response is fast, honest, and **documented.**



- **Stop** the improper access or disclosure immediately.
- **Preserve the facts**: who accessed what, when, why, and where the information went.
- **Escalate** internally under the agency's WISP, privacy, incident-response, or management procedures.
- Do not minimize, conceal, delete, or "clean up" before the agency understands what happened.

A bad lookup is made worse by a poor response. **Treat unauthorized access as a privacy incident**, not just an employee mistake.

MAIA'S BIG EVENT 2026 Conference & Trade Show Celebrating Independence!



Discussion Scenarios

Ask: permitted purpose, ethical concern, and agency response.

Scenario 1	A CSR is asked by a friend to look up the address connected to a license plate.
Scenario 2	A commercial client asks the agency to pull driving records for job applicants.
Scenario 3	An employee looks up a claimant after recognizing the name from a personal dispute.
Scenario 4	A producer wants to email RMV-derived information to a contractor "just to confirm details."
Scenario 5	A carrier underwriter asks for driver information tied to a pending commercial auto quote.

What would you document? Who would you escalate to? What would you say to the requester?

MAIA'S BIG EVENT 2026
Conference & Trade Show
Celebrating Independence!

Final Takeaway

RMV access is a privilege. Treat it that way.

Use it only for a legitimate insurance purpose.

🛡 Protect it while you have it.

✓ Share it only when the purpose is permitted and necessary.

📝 Document the reason.

✋ Stop when the purpose is unclear.

Purpose • Need • Authority • Documentation • Minimum Use

MAIA'S BIG EVENT 2026
Conference & Trade Show
Celebrating Independence!