Crash Data User Request Form

Instructions

This request form needs to be completed for all authorized Business Partner end users ("End Users") that will be granted access to the RMV's Crash Data Portal/System ("Crash Data"). The crash data is stored in a Crash System that authorized users access for work items and other tasks. The Crash Data Portal is the application used to search and request copies of Police Crash Reports. The authorized signatory ("Business Partner Contact") must complete Sections A and B. The End User must complete Section C, D and E. Return completed form to: MassDOTCrashReports@dot.state.ma.us

The permitted use for access is determined by the separate Crash Data Account Request Form (SEC119)

A. Business Entity Information (End User's Business)

The Business entity is a company authorized by the RMV to access the RMV Crash Data.

Requesting: (check one) ☐ Add/Reactivate a User   ☐ Deactivate User

Legal Business Name: _____

Physical Address: _____

Mailing Address: _____

B. Business Partner Certification and Signature

I, _____ (print name) certifies all information on this request form is true and the named End User below is a permitted user for this business.

Business Partner Contact Signature:_____ Date:_____

C. End User Information (Person authorized by the business to use the RMV's Crash Data)

End User's Full Legal Name: _____

End User's MA Driver's License/ID #:_____   Last 4 digits of SSN: _____

End User's Business Email Address:_____

End User's Phone Number:_____

Non-Mass Residents must attach a copy of state-issued drivers license or ID.

D. RMV System Policy for Crash Data

End Users must read, understand, and follow this policy

The RMV's Crash Data contains personal information. The Federal Driver Privacy Protection Act (18 U.S.C. § 2721) ("DPPA"), the Massachusetts Identity Theft Act (G.L. c. 93H), An Act Relative to Work and Family Mobility (Chapter 81 of the Laws of 2022), Regulations Authorizing Disclosure of Massachusetts Driver's License or Learner's Permit Applicant Information (940 CMR 37.00), and the Standards for the Protection of Personal Information of Residents of the Commonwealth (201 C.M.R. 17.00) protects this information. The DPPA broadly defines personal information that identifies an individual, including driver identification number, name, address, and telephone number. Highly restricted personal information is defined as an individual's photograph or image, social security number, medical or disability information. Specifically excluded from the definition of personal information is information on vehicular accidents, driving violations and the driver's license status.

If you are not clear on the business purpose for which you are authorized to access crash data, talk to your manager/supervisor.

The RMV will conduct background checks to ensure that you have not been convicted of a felony involving violence, dishonesty, deceit, or indecency. If you have been convicted of such a felony you will be denied access to the crash data.

You will be held personally responsible for all activity that occurs on your issued security credentials including: the accuracy and use of any transaction performed and/ or any inquiry conducted.

All transactions/inquiries are the official records of the RMV; they are recorded, stored, monitored, and audited. The RMV may in its sole discretion require you to explain and/or demonstrate the legitimate business purpose or permitted use for accessing the crash data for any particular transaction.

As the End User you will:
1. Never divulge your password to anyone.
2. Only access the crash data for approved business purposes.
3. Never use such records or information for the purpose of enforcing federal immigration law (including the investigation, participation, or cooperation with the enforcement of such law).
4. Never disclose crash data to any agency that enforces immigration law or to any employee or agent of any such agency.
5. Notify the RMV immediately if you receive a court order, judicial warrant, or a federal grand jury or trial subpoena regarding RMV obtained data or records.
6. Never leave your computer unattended with the crash data actively logged on. You must lock the computer or log off before leaving your computer unattended.
7. Ensure that crash data or records are not visible to unauthorized individuals.
8. Shred or deposit RMV records into a locked shredder container when no longer needed.
9. Never bring crash data or use the Crash System/Portal outside the workplace, unless required to perform your job duties.
10. Never knowingly obtain, disclose, or use RMV records for a purpose not permitted under the DPPA. You may be liable for impermissible dissemination of personal information to any individual to whom the personal information pertains.
11. Never misrepresent yourself or make a false statement in connection with a request for personal information with the intention of obtaining said information in a manner not authorized in your companies signed Agreement for Access to Records and Data Maintained by the Registry of Motor Vehicles or the DPPA.
12. Never disseminate crash data unless such dissemination is required by your specific job duties.
13. Never use crash data in the furtherance of an illegal act, including a violation of any criminal or civil laws.
14. Never sell, barter, charge a fee or receive any other consideration for crash data.

If you suspect your account has been compromised, contact RMV IS Security at RMVBusinesspartners@dot.state.ma.us or 857-368-7930 immediately.

E. End User Certification and Signature

I, _____, (print name) have read, agree, and certify to abide by the policy described above. I further certify that prior receipt or access to any crash data or records, and as a condition of renewal of any agreement for such receipt or access where applicable, I will not (a) use or disclose such records or information for the purpose of enforcing federal immigration law; or (b) disclose such records or information to any agency that primarily enforces immigration law or to any employee or agent of any such agency, unless provided with a lawful court order or judicial warrant signed by a judge appointed pursuant to Article III of the United States Constitution, a federal grand jury or trial subpoena, or as otherwise required by federal law.
Violation of this policy may subject you to disciplinary actions, including termination of Crash Data access, criminal proceedings and/or fines per each violation.

Signed and sworn to under the pains and penalties of perjury.

End User's Signature: _____   Date: _____

THE RMV RESERVES THE EXCLUSIVE RIGHT TO ALTER OR AMEND THIS DOCUMENT AT ANY TIME.