



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") one of RMV's Systems. The crash data is stored in a Crash System that authorizes a user for work items and other tasks. Crash Data Portal is an application used to search and request copies of Police Crash Reports or request a bulk file. The authorized signatory ("Business Partner Contact") must complete Sections A and B. The End User must complete Section C, D and E. Completed forms must be uploaded in the RMV's Community Portal.

To deactivate user, send email to: RMVBusinessPartners@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 Users' Business)

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

Legal Business Name

DBA or Department

Federal Employer ID Number (FEIN)

Business Mailing Address:

Street

City

State

Zip Code

Business Contact (please print clearly)

Phone

Email

B. Business Partner Certification and Signature

I, _____, (print name) hereby certify the below named individual as a permitted user for this business.

Business Partner Contact Signature: _____ Date: _____

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

End User Name

End User MA Driver's License/ID #*:

Last 4 Digits of Social Security Number

*Non-Mass residents must attach a copy of their state-issued driver's license or if you are a local, state, or federal government employee, attach an unexpired employer-issued ID.

User's Business Mailing Address:

User's Business Email Address:

User's Business Phone:

Bulk Data End Users that do not receive PII data must attach a copy of their unexpired work ID/Badge.

D. RMV System Policy

End Users must read the RMV System Policy.

The RMV System(s) stores personal and confidential data. The Federal Driver Privacy Protection Act (DPPA, 18 U.S.C. § 2721 et seq.), the Massachusetts Identity Theft Act (M.G.L. c. 93H), 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) protect this data. The DPPA broadly defines personal information as information that identifies an individual, including an individual's photograph, social security number,

driver identification number, name, address, telephone number, and medical or disability information. Specifically excluded from the definition of personal information is information on vehicular accidents, driving violations, and driver's status.

Note: Bulk data end users receiving files may or may not contain personal information.

You have been granted access to RMV System(s) because your company is a permitted business partner allowed to access RMV records. If you are not clear on the business purpose for which you may access the RMV data, talk to your manager/supervisor. The RMV may 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 may not be authorized to access the RMV systems or view its data.

You will be held personally responsible for all activity that occurs on your issued security credentials including: Any money collected (if applicable); the accuracy of any transaction performed; and any inquiry conducted. All transactions 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 RMV's data for any particular transaction.

As the end user you will:

1. Never divulge your password to anyone;
2. Only access the RMV records and data for 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 RMV records and data to any agency that primarily enforces immigration law or to any employee or agent of any such agency; unless you are provided with a lawful court order or judicial warrant signed by a judge appointed pursuant to Article II of the U.S. Constitution, a federal grand jury or trial subpoena, or as otherwise required by federal law.
5. Notify the RMV immediately if you receive a court order or judicial warrant regarding RMV obtained records or data;
6. Never leave your computer unattended with the RMV system actively logged on. You must lock the computer or log off before leaving your computer unattended;
7. Ensure that RMV records and data are not visible to unauthorized individuals;
8. Shred or deposit RMV records and data into a locked shredder container when no longer needed;
9. Never bring RMV records or data or use the RMV system(s) outside the workplace, unless required to perform your job duties;
10. Never knowingly obtain, disclose, or use RMV records and data 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 RMV records and data unless such dissemination is required by your specific job duties; and
13. Never use RMV records and 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 RMV records and 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) agree and will abide by the policy described above. Violation of this policy may be subjected to disciplinary actions, including termination of RMV 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.