



MEMORANDUM OF UNDERSTANDING FOR GOVERNMENTAL ENTITY ACCESS TO DRIVER AND VEHICLE INFORMATION DATABASE SYSTEM (DAVID)

This Memorandum of Understanding (MOU) is made and entered into by and between
City of Fort Lauderdale ,

hereinafter referred to as the Requesting Party, and the Florida Department of Highway Safety and Motor Vehicles, hereinafter referred to as the Providing Agency, collectively referred to as the Parties.

I. Purpose

The Providing Agency is a government entity whose primary duties include issuance of motor vehicle and driver licenses, registration and titling of motor vehicles, and enforcement of all laws governing traffic, travel, and public safety upon Florida's public highways.

In carrying out its statutorily mandated duties and responsibilities, the Providing Agency collects and maintains personal information that identifies individuals. This information is stored in the Department's Driver and Vehicle Information Database system, commonly referred to as "DAVID." Based upon the nature of this information, the Providing Agency is subject to the disclosure prohibitions contained in 18 U.S.C. §2721, the Driver's Privacy Protection Act (hereinafter "DPPA"), Section 119.0712(2), Florida Statutes, and other statutory provisions.

The Requesting Party is a government entity operating under the laws and authority of the state of Florida and/or operating under Federal laws. As a government entity, the Requesting Party may receive personal information from DAVID under the government agency exception provided in DPPA as indicated in Attachment I. The Requesting Party utilizes DAVID information for the purposes of carrying out its statutorily mandated duties and functions.

This MOU is entered into for the purpose of establishing the conditions and limitations under which the Providing Agency agrees to provide electronic access to DAVID information to the Requesting Party. Use of the data by the Requesting Party shall only be for lawful purpose.

II. Definitions

For the purposes of this Agreement, the below-listed terms shall have the following meanings:

- A. DAVID - The Providing Agency's Driver and Vehicle Information Database system that accesses and transmits driver and vehicle information.
- B. Driver License Information - Driver license and identification card data collected and maintained by the Providing Agency. This information includes personal information as defined below.
- C. Emergency Contact Information (ECI) - Information contained in a motor vehicle record listing individuals to be contacted in the event of an emergency. Emergency contact information may be released to law enforcement agencies through the DAVID system for purposes of contacting those listed in the event of an emergency, as noted in Section 119.0712 (2)(d), Florida Statutes.
- D. Driver Privacy Protection Act (DPPA) - The Federal Act (see, 18 United States Code § 2721, et seq.) that prohibits release and use of personal information except as otherwise specifically permitted within the Act.
- E. Government Entity - Any non-law enforcement agency of the state, city or county government and all Federal agencies, which may include Federal law enforcement agencies.
- F. Insurance Record - Insurance information, such as Insurance Company name, policy type, policy status, insurance creation and expiration date provided to the Requesting Party, pursuant to Section 324.242(2), Florida Statutes.

- G. Parties - The Providing Agency and the Requesting Party.
- H. Personal Information - As described in Chapter 119, Florida Statutes, information found in the motor vehicle record, which includes, but is not limited to, the subject's driver identification number, name, address, telephone number, social security number, medical or disability information, and emergency contact information.
- I. Point-of-Contact (POC) - A person(s) appointed by the Requesting Party as the administrator of the DAVID program in their agency.
- J. Providing Agency - The Florida Department of Highway Safety and Motor Vehicles. The Providing Agency is responsible for granting access to DAVID information to the Requesting Party.
- K. Quarterly Quality Control Review Report - Report completed each quarter by the Requesting Party's POC to monitor compliance with the MOU. The following must be included in the Quarterly Quality Control Review Report:
 - 1. A comparison of the DAVID users by agency report with the agency user list;
 - 2. A listing of any new or inactivated users since the last quarterly quality control review; and
 - 3. Documentation verifying that usage has been internally monitored to ensure proper, authorized use and dissemination.
- L. Requesting Party - Any Government Entity that is expressly authorized by Florida Statutes and DPPA to receive personal information contained in a motor vehicle record maintained by the Providing Agency.
- M. Vehicle Information - Title and registration data collected and maintained by the Providing Agency for vehicles.

III. Legal Authority

The Providing Agency maintains computer databases containing information pertaining to driver's licenses and vehicles pursuant to Chapters 317, 319, 320, 322, 328, and Section 324.242(2), Florida Statutes. The driver license and motor vehicle data contained in the Providing Agency's databases is defined as public record pursuant to Chapter 119, Florida Statutes, and as such, is subject to public disclosure unless otherwise exempted by law.

As the custodian of the state's driver and vehicle records, the Providing Agency is required to provide access to records permitted to be disclosed by law and may do so by remote electronic means, pursuant to Sections 119.0712(2), 320.05, 321.23, 322.20, and 324.242(2), Florida Statutes, and applicable rules.

Under this MOU, the Requesting Party will be provided, via remote electronic means, information pertaining to driver licenses and vehicles, including personal information authorized to be released pursuant to Section 119.0712(2), Florida Statutes and DPPA. By executing this MOU, the Requesting Party agrees to maintain the confidential and exempt status of any and all information provided by the Providing Agency pursuant to this agreement and to ensure that any person or entity accessing or utilizing said information shall do so in compliance with Section 119.0712(2), Florida Statutes and DPPA. In addition, the Requesting Party agrees that insurance policy information shall be utilized pursuant to Section 324.242(2), Florida Statutes. Furthermore, the deceased date of an individual shall only be provided to a Requesting Party that meets the qualifications of 15 CFR §1110.102. Disclosure of the deceased date of an individual, which is not in compliance with 15 CFR §1110.102, is punishable under 15 CFR §1110.200. Additionally, because the Social Security Administration does not guarantee the accuracy of the Death Master File (DMF), the Requesting Party is reminded that adverse action should not be taken against any individual without further investigation to verify the death information listed (A notice from the Social Security Administration addressing the foregoing is attached hereto and incorporated herein by reference).

This MOU is governed by the laws of the state of Florida and jurisdiction of any dispute arising from this MOU shall be in Leon County, Florida.

IV. Statement of Work

A. The Providing Agency agrees to:

1. Allow the Requesting Party to electronically access DAVID as authorized under this agreement.
2. Provide electronic access pursuant to established roles and times, which shall be uninterrupted except for periods of scheduled maintenance or due to a disruption beyond the Providing Agency's control, or in the event of breach of this MOU by the Requesting Party. Scheduled maintenance will normally occur Sunday mornings between the hours of 6:00 A.M. and 10:00 A.M., EST.
3. Provide an agency contact person for assistance with the implementation and administration of this MOU.

B. The Requesting Party agrees to:

1. Utilize information obtained pursuant to this MOU, including Emergency Contact Information (ECI), only as authorized by law and for the purposes prescribed by law and as further described in this MOU. In the case of ECI, such information shall only be used for the purposes of notifying a person's registered emergency contact in the event of a serious injury, death, or other incapacitation. ECI shall not be released or utilized for any other purpose, including developing leads or for criminal investigative purposes.
2. Retain information obtained from the Providing Agency only if necessary for law enforcement purposes. If retained, information shall be safeguarded in compliance with Section V. Safeguarding Information, subsection C.
3. Ensure that its employees and agents comply with Section V. Safeguarding Information.
4. Refrain from assigning, sub-contracting, or otherwise transferring its rights, duties, or obligations under this MOU, without the prior written consent of the Providing Agency.
5. Not share, provide, or release any DAVID information to any law enforcement, other governmental agency, person, or entity not a party or otherwise subject to the terms and conditions of this MOU.
6. Protect and maintain the confidentiality and security of the data received from the Providing Agency in accordance with this MOU and applicable state and federal law.
7. Defend, hold harmless and indemnify the Providing Agency and its employees or agents from any and all claims, actions, damages, or losses which may be brought or alleged against its employees or agents for the Requesting Party's negligent, improper, or unauthorized access, use, or dissemination of information provided by the Providing Agency, to the extent allowed by law.
8. Immediately inactivate user access/permissions following termination or the determination of negligent, improper, or unauthorized use or dissemination of information and to update user access/permissions upon reassignment of users within five (5) business work days.
9. Complete and maintain Quarterly Quality Control Review Reports as defined in Section II. Definitions, K, and utilizing the form attached as Attachment II.
10. Update any changes to the name of the Requesting Party, its Agency head, its POC, address, telephone number and/or e-mail address in the DAVID system within ten calendar days of occurrence. The Requesting Party is hereby put on notice that failure to timely update this information may adversely affect the time frames for receipt of information from the Providing Agency.

11. Immediately comply with any restriction, limitation, or condition enacted by the Florida Legislature following the date of signature of this MOU, affecting any of the provisions herein stated. The Requesting Party understands and agrees that it is obligated to comply with the applicable provisions of law regarding the subject matter of this Agreement at all times that it is receiving, accessing, or utilizing DAVID information.
12. Timely submit the Attestation and Certification statements as required in Section VI. Compliance and Control Measures, subsections B and C.
13. For Federal Agencies Only: The Requesting Party agrees to promptly consider and adjudicate any and all claims that may arise out of this MOU resulting from the actions of the Requesting Party, duly authorized representatives, or contractors of the Requesting Party, and to pay for any damage or injury as may be required by Federal law. Such adjudication will be pursued under the Federal Tort Claims Act, 28 U.S.C. § 2671, et seq., the Federal Employees Compensation Act, 5 U.S.C. § 8101, et seq., or such other Federal legal authority as may be pertinent.
14. Access and utilize the deceased date of an individual, or other information from the NTIS Limited Access Death Master File, as defined in 15 CFR §1110.2, in conformity with the following requirements:
 - a) Pursuant to 15 CFR §1110.102, the Requesting Party certifies that its access to DMF information is appropriate because the Requesting Party: (i) has a legitimate fraud prevention interest, or a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty; (ii) has systems, facilities, and procedures in place to safeguard such information, and experience in maintaining the confidentiality, security, and appropriate use of such information, pursuant to requirements reasonably similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986; and (iii) agrees to satisfy such similar requirements.
 - b) Pursuant to 15 CFR §1110.102, the Requesting Party certifies that it will not: (i) disclose DMF information to any person other than a person who meets the requirements of Section IV. Statement of Work, subsection B. paragraph 14 (a), above; (ii) disclose DMF information to any person who uses the information for any purpose other than a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty; (iii) disclose DMF information to any person who further discloses the information to any person other than a person who meets the requirements of subsection IV. B. 14 (a), above; or (iv) use DMF information for any purpose other than a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation or fiduciary duty.

V. Safeguarding Information

The Parties shall access, disseminate, use and maintain all information received under this MOU in a manner that ensures its confidentiality and proper utilization in accordance with Chapter 119, Florida Statutes, and DPPA. Information obtained under this MOU shall only be disclosed to persons to whom disclosure is authorized under Florida law and federal law.

Any person who willfully and knowingly violates any of the provisions of this section is guilty of a misdemeanor of the first degree punishable as provided in Sections 119.10 and 775.083, Florida Statutes. In addition, any person who willfully and knowingly discloses any information in violation of DPPA may be subject to criminal sanctions and civil liability. Furthermore, failure to comply with 15 CFR §1110.102 pertaining to the deceased date of an individual may result in penalties of \$1,000 for each disclosure or use, up to a maximum of \$250,000 in penalties per calendar year, pursuant to 15 CFR §1110.200.

The Parties mutually agree to the following:

- A. Information exchanged will not be used for any purposes not specifically authorized by this MOU. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, or the dissemination, sharing, copying, or passing of this information to unauthorized persons.
- B. The Requesting Party shall not indemnify and shall not be liable to the Providing Agency for any driver license or motor vehicle information lost, damaged, or destroyed as a result of the electronic exchange of data pursuant to this MOU, except as otherwise provided in Section 768.28, Florida Statutes.
- C. Any and all DAVID-related information provided to the Requesting Party as a result of this MOU, particularly data from the DAVID system, will be stored in a place physically secure from access by unauthorized persons.
- D. The Requesting Party shall comply with Rule 60GG-2, Florida Administrative Code, and with Providing Agency's security policies, and employ adequate security measures to protect Providing Agency's information, applications, data, resources, and services. The applicable Providing Agency's security policies shall be made available to Requesting Party. Additionally, with respect to the deceased date of an individual, the Requesting Party shall have systems, facilities, and procedures in place to safeguard such information, and experience in maintaining the confidentiality, security, and appropriate use of such information, pursuant to requirements reasonably similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986 and agrees to satisfy such similar requirements.
- E. When printed information from DAVID is no longer needed, it shall be destroyed by cross-cut shredding or incineration in accordance with Florida law.
- F. The Requesting Party shall maintain a list of all persons authorized within the agency to access DAVID information, which must be provided to the Providing Agency upon request.
- G. Access to DAVID-related information, particularly data from the DAVID System, will be protected in such a way that unauthorized persons cannot view, retrieve, or print the information.
- H. Under this MOU agreement, access to DAVID shall be provided to users who are direct employees of the Requesting Party and shall not be provided to any non-employee or contractors of the Requesting Party.
- I. By signing this MOU, the Parties, through their signatories, affirm and agree to maintain the confidentiality of the information exchanged through this agreement.

VI. Compliance and Control Measures

- A. **Quarterly Quality Control Review Report** - Must be completed by the Requesting Party, utilizing Attachment II, Quarterly Quality Control Review Report, within 10 days after the end of each quarter and maintained for two years. The following must be included in the Quarterly Quality Control Review Report:
 - 1. A comparison of the DAVID users by agency report with the agency user list;
 - 2. A listing of any new or inactivated users since the last quarterly quality control review; and
 - 3. Documentation verifying that usage has been internally monitored to ensure proper, authorized use and dissemination utilizing the auditing features available in DAVID.
- B. **Internal Control Attestation** - This MOU is contingent upon the Requesting Party having appropriate internal controls in place at all times that data is being provided/received pursuant to this MOU to ensure that the data is protected from unauthorized access, distribution, use, modification, or disclosure. The Requesting Party must submit an Attestation Statement from their Agency's Internal Auditor, Inspector General, Risk Management IT Security Professional, or a currently licensed Certified Public

Accountant, on or before the third and sixth anniversary of the agreement or within 180 days from receipt of a request for an Attestation from the Providing Agency. The Attestation Statement shall indicate that the internal controls over personal data have been evaluated and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. The Attestation Statement shall also certify that any and all deficiencies/issues found during the review have been corrected and measures enacted to prevent recurrence. The Providing Agency may extend the time for submission of the Attestation Statement upon written request by the Requesting Party for good cause shown by the Requesting Party.

The Attestation Statement must have an original signature of the Agency Head or person designated by Letter of Delegation to execute contracts/agreements on their behalf, and may be sent via U.S. Mail, facsimile transmission, or e-mailed to the Providing Agency's Bureau of Records at the following address:

Department of Highway Safety and Motor Vehicles
Chief, Bureau of Records
2900 Apalachee Parkway, MS89
Tallahassee, Florida 32399-0500
Fax: (850) 617-5168
E-mail: DataListingUnit@flhsmv.gov

- C. **Annual Certification Statement** - The Requesting Party shall submit to the Providing Agency an annual statement indicating that the Requesting Party has evaluated and certifies that it has adequate controls in place to protect the personal data from unauthorized access, distribution, use, modification, or disclosure, and is in full compliance with the requirements of this MOU. The Requesting Party shall submit this statement annually, within 45 days after the anniversary date of this MOU. (NOTE: During any year in which an Attestation Statement is provided, submission of the Internal Control Attestation will satisfy the requirement to submit an Annual Certification Statement.)

In addition, prior to expiration of this MOU, if the Requesting Party intends to enter into a new MOU, a certification statement attesting that appropriate controls remained in place during the final year of the MOU and are currently in place shall be required to be submitted to the Providing Agency prior to issuance of a new MOU.

- D. **Misuse of Personal Information** - The Requesting Party must notify the Providing Agency in writing of any incident where determination is made that personal information has been compromised as a result of unauthorized access, distribution, use, modification, or disclosure, by any means, within 30 days of such determination. The statement must be provided on the Requesting Agency's letterhead and include each of the following: a brief summary of the incident; the outcome of the review; the date of the occurrence(s); the number of records compromised; the name or names of personnel responsible; whether disciplinary action or termination was rendered; and whether or not the owners of the compromised records were notified. The statement shall also indicate the steps taken, or to be taken, by the Requesting Agency to ensure that misuse of DAVID data does not continue. This statement shall be mailed to the Bureau Chief of Records at the address indicated in Section VI. Compliance and Control Measures, subsection B., above. (NOTE: If an incident involving breach of personal information did occur and Requesting Party did not notify the owner(s) of the compromised records, the Requesting Party must indicate why notice was not provided, for example "Notice not statutorily required".)

In addition, the Requesting Party shall comply with the applicable provisions of Section 501.171, Florida Statutes, regarding data security and security breaches, and shall strictly comply with the provisions regarding notice provided therein.

VII. Agreement Term

This MOU shall take effect upon the date of last signature by the Parties and shall remain in effect for six (6) years from this date unless sooner terminated or cancelled in accordance with Section IX. Termination. Once executed, this MOU supersedes all previous agreements between the parties regarding the same subject

matter.

VIII. Amendments

This MOU incorporates all negotiations, interpretations, and understandings between the Parties regarding the same subject matter and serves as the full and final expression of their agreement. This MOU may be amended by written agreement executed by and between both Parties. Any change, alteration, deletion, or addition to the terms set forth in this MOU, including to any of its attachments, must be by written agreement executed by the Parties in the same manner as this MOU was initially executed. If there are any conflicts in the amendments to this MOU, the last-executed amendment shall prevail. All provisions not in conflict with the amendment(s) shall remain in effect and are to be performed as specified in this MOU.

IX. Termination

- A. This MOU may be unilaterally terminated for cause by either party upon finding that the terms and conditions contained herein have been breached by the other party. Written notice of termination shall be provided to the breaching party; however, prior-written notice is not required, and notice may be provided upon cessation of work under the agreement by the non-breaching party.
- B. In addition, this MOU is subject to unilateral termination by the Providing Agency without notice to the Requesting Party for failure of the Requesting Party to comply with any of the requirements of this MOU, or with any applicable state or federal laws, rules, or regulations, including Section 119.0712(2), Florida Statutes.
- C. This MOU may also be cancelled by either party, without penalty, upon 30 days' advanced written notice to the other party. All obligations of either party under the MOU will remain in full force and effect during the thirty (30) day notice period.

X. Notices

Any notices required to be provided under this MOU may be sent via U.S. Mail, facsimile transmission, or e-mail to the following individuals:

For the Providing Agency:

Chief, Bureau of Records
2900 Apalachee Parkway
Tallahassee, Florida 32399
Fax: (850) 617-5168
E-mail: DataListingUnit@flhsmv.gov

For the Requesting Party:

Agency Point-of-Contact listed on the signature page.

XI. Additional Database Access/Subsequent MOU's

The Parties understand and acknowledge that this MOU entitles the Requesting Party to specific information included within the scope of this agreement. Should the Requesting Party wish to obtain access to other personal information not provided hereunder, the Requesting Party will be required to execute a subsequent MOU with the Providing Agency specific to the additional information requested. All MOU's granting access to personal information will contain the same clauses as are contained herein regarding Compliance and Control Measures.

The Providing Agency is mindful of the costs that would be incurred if the Requesting Party was required to undergo multiple audits and to submit separate certifications, attestations, and reports for each executed MOU. Accordingly, should the Requesting Party execute any subsequent MOU with the Providing Agency for access

to personal information while the instant MOU remains in effect, the Requesting Party may submit a written request, subject to Providing Agency approval, to submit one of each of the following covering all executed MOU's: Quarterly Quality Control Review Report; Certification; and Attestation; and/or to have conducted one comprehensive audit addressing internal controls for all executed MOU's. The Providing Agency shall have the sole discretion to approve or deny such request in whole or in part or to subsequently rescind an approved request based upon the Requesting Party's compliance with this MOU and/or negative audit findings.

XII. Application of Public Records Law

The Requesting Party agrees to comply with the following requirements of Florida's public records laws:

1. Keep and maintain public records required by the Department to perform the service.
2. Upon request from the Department's custodian of public records, provide the Department with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes, or as otherwise provided by law.
3. Ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the contract term and following completion of the contract if the contractor does not transfer the records to the public agency.
4. Upon completion of the contract, transfer, at no cost, to the Department all public records in possession of the Requesting Party or keep and maintain public records required by the public agency to perform the service. If the Requesting Party transfers all public records to the Department upon completion of the contract, the Requesting Party shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Requesting Party keeps and maintains public records upon completion of the contract, the contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the Department, upon request from the Department's custodian of public records, in a format that is compatible with the information technology systems of the Department.

IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLA. STAT., TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATED TO THIS CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (850) 617-3101, OGCFILING@FLHSMV.GOV, OFFICE OF GENERAL COUNSEL, 2900 APALACHEE PARKWAY, STE. A432, TALLAHASSEE, FL 32399-0504.

XIII. Certification Information

Pursuant to Section IV. Statement of Work, subsection B. paragraph 14(a) above, the Requesting Party certifies that access to DMF information is appropriate based on the following specific purpose (please describe the legitimate purpose):

Please indicate whether the Requesting Party desires to re-disclose the deceased date of any individual to any other person or entity: Yes ☐ No ☐

If the Requesting Party desires to re-disclose the deceased date of any individual to any other person or entity, the Requesting Party agrees that it will not re-disclose the data received from the Providing Agency, but rather, will contact NTIS at <https://classic.ntis.gov/products/ssa-dmf/#> to become a Certified Person, as defined by 15 CFR §1110.2. A Requesting Party who is a Certified Person may only disclose the deceased date of an individual pursuant to the Requesting Party's obligations under 15 CFR §1110.102.

IN WITNESS HEREOF, the Parties hereto, have executed this Agreement by their duly authorized officials on the date(s) indicated below.

REQUESTING PARTY

City of Fort Lauderdale		
Agency Name		
100 North Andrews Avenue		
Street Address		
Suite		
Fort Lauderdale	FL	33301
City	State	Zip Code

BY:

Signature of Authorized Official
Greg Chavarria
Printed/Typed Name
City Manager
Title
Date
Gchavarria@fortlauderdale.gov
Official Agency Email Address
954-828-6174
Phone Number

Agency Point of Contact:
Elane Costa
Printed/Typed Name
ecosta@fortlauderdale.gov
Official Agency Email Address
954-828-3703 /
Phone Number
/
Fax Number

PROVIDING AGENCY:

Florida Department of Highway Safety and Motor
Vehicles
2900 Apalachee Parkway
Tallahassee, Florida 32399

BY:

Signature of Authorized Official
Printed/Typed Name
Title
Date

IMPORTANT NOTICE

On November 1, 2011, the Social Security Administration (SSA) implemented an important change in the Death Master File (DMF) data. NTIS, a cost-recovery government agency, disseminates the Limited Access DMF on behalf of SSA. The Limited Access Death Master File contains data on decedants who died less than 3 years ago.

Please see the Q and A below, provided by SSA (and edited by NTIS to change the tense once the change had been implemented) for an explanation of the change.

Should you have any questions, please email jhounsell@ntis.gov who will forward any questions not answered below to the Social Security Administration for reply.

IMPORTANT NOTICE: Change in Public Death Master File Records

NTIS receives Death Master File (DMF) data from the Social Security Administration (SSA). SSA receives death reports from various sources, including family members, funeral homes, hospitals, and financial institutions.

Q: What change has SSA made to the Public DMF?

A: Effective November 1, 2011, the DMF data that NTIS receives from SSA no longer contains protected state death records. Section 205(r) of the [Social Security] Act prohibits SSA from disclosing the state death records SSA receives through its contracts with the states, except in limited circumstances. (Section 205r link - http://www.ssa.gov/OP_Home/ssact/title02/0205.htm)

Q: How did this change affect the size of the Public DMF?

A: The historical Public DMF contained 89 million records. SSA removed approximately 4.2 million records from this file and adds about 1 million fewer records annually.

**REMINDER:
DMF users should always investigate and verify the death listed before taking any adverse action against any individual."**

FLORIDA DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES
Request For Access to Driver And Vehicle Information Database System (DAVID)

ATTACHMENT I

Pursuant to section 119.0712(2), F. S., personal information in motor vehicle and driver license records can be released for the following purposes, as outlined in 18 United States Code, section 2721:

Personal information referred to in subsection (a) shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of Titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 U.S.C. 1231 et seq.), the Clean Air Act (42 U.S.C. 7401 et seq.), and chapters 301, 305, and 321-331 of Title 49, CFR, and, subject to subsection (a)(2), may be disclosed as follows:

1. For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.
2. For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.
3. For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only:
 - a) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and
 - b) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by pursuing legal remedies against, or recovering on a debt or security interest against, the individual.
4. For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.
5. For use in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.
6. For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.
7. For use in providing notice to the owners of towed or impounded vehicles.
8. For use by any licensed private investigative agency or licensed security service for any purpose permitted in accordance with 18 USC 2721 (b).
9. For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of Title 49, CFR.
10. For use in connection with the operation of private toll transportation facilities.
11. For any other use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains.
12. For bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains.
13. For use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.
14. For any other use specifically authorized under the law of the State that holds the record, if such use is related to the operation of a motor vehicle or public safety.



QUARTERLY QUALITY CONTROL REVIEW REPORT

Point of Contacts (POC) must do the following to satisfy the MOU Quarterly Quality Control Review:

- Compare the DAVID Users by Agency report with the agency user list.
 - Reconcile any differences to ensure state and agency records are consistent.
- Keep a record of any new or inactivated users since the last Quarterly Quality Control Review.
 - Update any users/user information as needed, document the reason for the change in access, and the date the change is made.
- Monitor usage to ensure proper, authorized use and dissemination.
 - Randomly select a sample of users and run an audit report for a period during the quarter. Look for any misuse, including, but not limited to reason codes, running siblings, spouses, ex-spouses, celebrities, and political figures. Look at the times of day the data was accessed, repeated runs of same record, and unexplained access to the Emergency Contact Information.
 - **Please note:** DHSMV highly recommends the agency audit users as frequently as possible to ensure misuse is not occurring.
- Complete the below report and ensure all actions are documented.

Quarter:	Year:
Total active users in DAVID:	
Total active users in agency records:	
Users inactivated during quarter:	
Users audited during quarter:	
Total cases of misuse found:	
Total cases of misuse reported to DHSMV:	

POC Signature

Date

POC Name Printed

ATTESTATION STATEMENT

Contract Number _____

In accordance with Section VI., Part B, of the Memorandum of Understanding between **Department of Highway Safety and Motor Vehicles** and _____ (Requesting Party), this MOU is contingent upon the Requesting Party having appropriate internal controls in place to ensure that data provided/received pursuant to this MOU is protected from unauthorized access, distribution, use, modification, or disclosure. The Requesting Party must submit an Attestation Statement from their Agency's Internal Auditor, Inspector General, Risk Management IT Security Professional, or a currently licensed Certified Public Accountant, on or before the third and sixth anniversary of the agreement or within 180 days from receipt of an Attestation review request from the Providing Agency. The Attestation Statement shall indicate that the internal controls over personal data have been evaluated and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. The Attestation Statement shall also certify that any and all deficiencies/issues found during the review have been corrected and measures enacted to prevent recurrence. The Providing Agency may extend the time for submission of the Attestation Statement upon written request by the Requesting Party for good cause shown by the Requesting Party.

_____ (Requesting Agency) hereby attests that the Requesting Party's controls were evaluated as required in Section VI. Part B of the MOU and the controls are adequate to protect personal data from unauthorized access, distribution, use, modification or disclosure, and is in full compliance with requirements of the contractual agreement. Furthermore, any and all deficiencies/issues found during the review were corrected and measures enacted to prevent recurrence.

The above evaluation was conducted by Requesting Party's Internal Auditor; Inspector General; Risk Management IT Security Professional; Currently licensed Certified Public Accountant, identified below as the Auditor.

Signature of Authorized Official or
Delegated Official with letter of Authority

Signature of Auditor

Printed Name

Printed Name

Title

Title

Date

Date