

II. FISCAL IMPACT ANALYSIS

A. Five Year Summary of Fiscal Impact

Fiscal Years	<u>2024</u>	<u>2025</u>	<u>2026</u>	<u>2027</u>	<u>2028</u>
Capital Expenditures	_____	_____	_____	_____	_____
Operating Costs	_____	_____	_____	_____	_____
External Revenues	_____	_____	_____	_____	_____
Program Income (County)	_____	_____	_____	_____	_____
In-Kind Match (County)	_____	_____	_____	_____	_____
Net Fiscal Impact	*	_____	_____	_____	_____
# ADDITIONAL FTE POSITIONS (Cumulative)	0	0	0	0	0

Is Item Included In Current Budget? Yes X No _____
 Does this item include the use of state funds? Yes ___ No x
 Does this item include the use of federal funds? Yes ___ No x


Budget Account Exp No: Fund 1429 Department 660 Unit 6241 Object 4901
 Budget Account Exp No: Fund 1430 Department 660 Unit 6252 Object 4901
 Rev No: Fund 1429 Department 660 Unit 6241 RevSc 2900
 Rev No: Fund 1430 Department 660 Unit 6252 RevSc 2900


B. Recommended Sources of Funds/Summary of Fiscal Impact:

*The fiscal impact is indeterminable at this time; however, fees paid for driver history checks are supported by revenue derived from fees collected.

Departmental Fiscal Review:  5/29
 (25) **III. REVIEW COMMENTS**

A. OFMB Fiscal and/or Contract Dev. and Control Comments:

 5/31/24
 M6 5/31 OFMB GA 5/29

 6/7/24
 Contract Administration
 6/6/24

B. Legal Sufficiency:

 6/10/24
 Assistant County Attorney

C. Other Department Review:

 Department Director

This summary is not to be used as a basis for payment.

Background and Justification: Continued from page 1: The Board of County Commissioners initially approved a MOU for Driver License and/or Motor Vehicle Record Data Exchange with FLHSMV (R2015-0737) on June 2, 2015 to receive driver records electronically with subsequent renewals on June 14, 2018 (R2018-0798) and May 21, 2021 (R2021-1121). These records, transmitted electronically, allow DCA to ensure that tow and VFH applicants meet PBC driver requirements. While applicants may acquire driver history records from other sources, this optional service allows tow truck and VFH applicants the ability to conveniently obtain this required transcript for their application at the DCA. More than 9,000 driver history records were requested from FLHSMV by DCA for VFH and tow truck driver applicants since June 2015. VFH and tow truck driver applicants pay the costs associated with the driver record requests as outlined in the fee resolution. There are no fees associated with searches in the DAVID system.

MOU Number: HSMV-0596-24

**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 Palm Beach County Board of County Commissioners hereafter referred to as the Requesting Party, and the Florida Department of Highway Safety and Motor Vehicles, hereafter 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, but are not limited to, 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 Providing Agency'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, et seq., the Driver's Privacy Protection Act (hereafter "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 MOU, 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 License Information, Insurance Record Information, and Motor Vehicle Information.

- B. Driver License Information - Driver license and identification card data collected and maintained by the Providing Agency, including Emergency Contact Information. This information includes Personal Information.
- C. Driver Privacy Protection Act (DPPA) - The Federal Act (see, 18 United States Code § 2721, et seq.) that prohibits release and use of Personal Information and highly restricted personal information, except as otherwise specifically permitted within the Act.
- D. Emergency Contact Information (ECI) - Information contained in Driver License Information listing individuals to be contacted in the event of an emergency.
- E. Government Entity - Any agency of the state, city or county government in Florida, college or state university in Florida, and all Federal agencies, which may include Federal law enforcement agencies.
- F. Insurance Record Information- Insurance information, such as insurance company name, policy type, policy status, and insurance creation and expiration date.
- G. Motor Vehicle Information - Title and registration data collected and maintained by the Providing Agency for motor vehicles and vessels. This information contains Personal Information.
- H. Parties - The Providing Agency and the Requesting Party.
- I. Personal Information - As described in section 119.0712(2)(b), Florida Statutes, and 18 U.S.C. §2725, information which includes, but is not limited to, the subject's driver license/identification card number, name, address, telephone number, social security number, race, gender, date of birth, height, medical or disability information.
- J. Point-of-Contact (POC) - A person(s) appointed by the Requesting Party as the administrator of the DAVID program in their agency.
- K. 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.
- L. 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.
- M. Requesting Party - A Government Entity that is expressly authorized by Florida Statutes and DPPA to receive Personal Information in Driver License Information, Insurance Record Information, and Motor Vehicle Information maintained by the Providing Agency.

III. Legal Authority

- A. The Providing Agency maintains computer databases containing information pertaining to driver's licenses and vehicles pursuant to Chapters 317, 319, 320, 322, 324, and 328, Florida Statutes. The Driver License Information, Insurance Record Information, and Motor Vehicle Information 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.
- B. As the custodian of the state's Driver License Information, Insurance Record Information, and Motor Vehicle Information, the Providing Agency is responsible for providing access only to records and information permitted to be disclosed by law.
- C. Under this MOU, the Requesting Party will be provided, via remote electronic means, Driver License Information, Insurance Record Information, and Motor Vehicle Information, including Personal Information authorized to be released pursuant to DPPA and sections 119.0712(2) and 324.242(2), Florida Statutes.
- D. 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 MOU and to ensure that any person or entity accessing or utilizing said information shall do so in compliance with DPPA and sections 119.0712(2) and 324.242(2), Florida Statutes..
- E. 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.
- F. This MOU is governed by the laws of the state of Florida, to the extent not in conflict with federal law, and venue of any dispute arising from this MOU shall be in Leon County, Florida.
- G. The Parties agree that all provisions herein concerning the protection, disclosure, or distribution of data providing by the Providing Agency to the Requesting Party shall survive the expiration or termination of this MOU and that the Providing Agency reserves the right to enforce the provisions of this MOU after the MOU's expiration or termination, including obtaining injunctive relief.

IV. Statement of Work

- A. The Providing Agency agrees to:
 - 1. Allow the Requesting Party to electronically access DAVID as authorized under this MOU.
 - 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., ET.

3. Provide an agency contact person for assistance with the implementation and administration of this MOU.

B. The Requesting Party agrees to:

1. Access or utilize all information obtained by the Providing Agency pursuant to this MOU, including ECI, in strict compliance with DPPA and sections 119.0712(2) and 324.242, Florida Statutes, and for the purposes prescribed by law and as further described in this MOU.
2. Only release or disclose ECI, without the express consent of the person to whom such emergency contact information applies, to a law enforcement agency for the purposes of contacting those listed in the event of an emergency, or to a receiving facility, hospital, or licensed detoxification or addictions receiving facility pursuant to sections 394.463(2)(a) or 397.6772(1)(a), Florida Statutes, for the sole purpose of informing a patient's emergency contacts of the patient's whereabouts. ECI shall not be released or utilized for any other purpose, including developing leads or for criminal investigative purposes.
3. Use information provided pursuant to this MOU only for the expressed purposes as described in Attachment I of this MOU.
4. Maintain the confidential and exempt status of all information provided by the Providing Agency pursuant to this MOU as required by DPPA and sections 119.0712(2) and 324.242, Florida Statutes.
5. 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.
6. Ensure that its employees and agents comply with Section V. Safeguarding Information.
7. Not assign, sub-contract, or otherwise transfer its rights, duties, or obligations under this MOU, without the express written consent and approval of the Providing Agency.
8. 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.
9. 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.
10. 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. This provision does not apply to federal agencies.
11. 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 workdays.
12. Complete and maintain Quarterly Quality Control Review Reports as defined in Section II.

Definitions, K, utilizing the form attached as Attachment II.

13. 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 (10) 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.
14. To the extent permitted by federal law, 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 MOU at all times that it is receiving, accessing, or utilizing DAVID information.
15. Timely submit the Internal Control Attestation Statements and Annual Certification Statements as required in Section VI. Compliance and Control Measures, subsections B and C, respectively.
16. 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.
17. Access and utilize the deceased date of an individual, or other information from the NTIS Limited Access Death Master File (DMF), 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 Chapter 119, Florida Statutes, is guilty of a misdemeanor of the first degree punishable as provided in sections 119.10 and 775.083, Florida Statutes. Further, pursuant to Section 119.0712(2)(e), Florida Statutes, any person who uses or releases any DAVID information for a purpose not specifically authorized by law commits a noncriminal infraction, punishable by a fine not exceeding \$2,000. 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 be liable to the Providing Agency for any Driver License Information, Insurance Record Information, 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 or in the Federal Torts Claim Act, 28 U.S.C §2671, et seq.
- 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, at a minimum, shall meet the requirements of Rule 60GG-2, Florida Administrative Code, and with Providing Agency's security policies (Attachment V.), 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 the 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, 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 MOU.

VI. Compliance and Control Measures

- A. **Quarterly Quality Control Review Report** – The Requesting Party must complete and file with the Providing Agency a Quarterly Quality Control Review Report, Attachment II, within ten (10) days after the end of each quarter and maintain copies of such filed reports for two years after the reports are filed with the Providing Agency. The following information must be included in each 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 Statement** - This MOU is contingent upon the Requesting Party having appropriate internal controls in place at all times that data is being provided or received pursuant to this MOU to ensure that such data is protected from unauthorized access, distribution, use, modification, or disclosure. The Requesting Party must conduct an Internal Control and Data Security Audit and, based upon that audit, submit an Internal Control Attestation Statement, utilizing Attachment III, completed by the Requesting Party's Internal Auditor, Inspector General, Risk Management IT Security Professional, or a currently licensed Certified Public Accountant.
 - 1. A completed Internal Control Attestation Statement shall be submitted to the Providing Agency not later than:
 - a) The third anniversary of the Effective Date of this MOU;
 - b) Ninety (90) days prior to the sixth anniversary of the Effective Date of this MOU, if the Requesting Party intends to enter a new MOU for DAVID access with the Providing Agency; and
 - c) One hundred eighty (180) days after the receipt by the Requesting Agency of a request from the Providing Agency for an Attestation Statement.

An Internal Control Attestation Statement submitted when the Requesting Party intends

to enter a new MOU (i.e., not later than ninety (90) days prior to the sixth anniversary of the Effective Date of this MOU) also shall certify that: i) appropriate controls over Personal Information were in place during the year preceding the date the Internal Control and Data Security Audit was completed; and ii) appropriate controls over Personal Information remain in place. Such Internal Control Attestation Statement must be submitted by the Requesting Party to the Providing Agency prior to execution of a new MOU.

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.

2. Each completed Internal Control Attestation Statement shall:

- a) Indicate that, within the past one hundred eighty (180) days, the Requesting Party conducted an Internal Control and Data Security Audit of the internal controls over Personal Information available through the DAVID system which has found that those internal controls have been evaluated and are adequate to protect such Personal Information from unauthorized access, distribution, use, modification, or disclosure.
- b) Certify that any and all deficiencies/issues found during the review have been corrected and measures enacted to prevent recurrence.
- c) Contain the original signature of the Requesting Party's Internal Auditor, Inspector General, Risk Management IT Security Professional, or a currently licensed Certified Public Accountant.
- d) Contain the original signature of the Requesting Agency's Agency Head or person designated by Letter of Delegation to execute contracts/agreements on their behalf.
- e) Be sent via U.S. Mail, facsimile transmission, or e-mail 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, utilizing Attachment IV, indicating that the Requesting Party has evaluated and certifies that it has adequate controls in place to protect the Personal Information available through the DAVID system 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, not later than 45 days after the anniversary date of the Effective Date of this MOU. (NOTE: During any year in which an Internal Control Attestation Statement is provided, submission of the Internal Control Attestation Statement will satisfy the requirement to submit an Annual Certification Statement.).

- 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. Memorandum of Agreement Term

This MOU shall take effect upon the date of last signature by the Parties (the "Effective Date") 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 MOU 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, including timely completion of the Quarterly Quality Control Review Reports, Internal Control Attestation Statements, and Annual Certification Statements required by Section VI, or with any applicable state or federal laws, rules, or regulations, including, but not limited to, 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:

Name of the Requesting Party's Contract Manager: Rob Shelt, Consumer Affairs Director
Address: 50 South Military Trail; Suite 201
Email address: rshelt@pbcgov.org
Phone: 561-712-6605

The Requesting Party's Contract Manager shall serve as a liaison between the Requesting Party and the Providing Agency concerning all notifications and communications related to this MOU. The Requesting Party's Contract Manager's role is to receive all notices required by or pertaining to this MOU and to stay informed about all of the terms and conditions in this MOU, including, but not limited to, Section IV, B 13, and VI of this MOU.

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 MOU. 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; Annual Certification Statement; and Internal Control Attestation Statement; and/or to have conducted one comprehensive internal control and data security 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 Parties to this MOU recognize and acknowledge that any Governmental Entity having custody of records made or received in connection with the transaction of official business remains responsible for responding to public records requests for those records in accordance with Florida law (including Chapter 119, Florida Statutes) or federal law, and that public records received by the Requesting Party pursuant to this MOU that are exempt or confidential from public records disclosure requirements will not be disclosed except as authorized by Florida law or DPPA.

XIII. Certification Information

Pursuant to Section IV. Statement of Work, subsection B. paragraph 17(a) above, the Requesting Party certifies that access to DMF information is appropriate based on the following specific purpose (please describe the legitimate purpose):

Administering the Palm Beach County Code of Ordinances relating to Vehicle for Hire, Moving, and Towing and Immobilization services ordinances (Chapter 17, Article VIII and Chapter 19 Articles IX, VIII) for enforcement and licensing assessment of drivers and business to protect the Health and safety of visitors and residents.

Please indicate whether the Requesting Party desires to re-disclose the deceased date of any individual to any other person or entity: Yes No N/A (if requesting Party is a Federal Agency)

If the Requesting Party desires to re-disclose the deceased date of any individual to any other person or entity, the Requesting Party agrees, unless the Requesting Party is a Federal Agency 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.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

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

REQUESTING PARTY

PROVIDING AGENCY

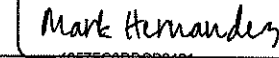
Palm Beach County Board of County Commissioners
Requesting Party Name
50 South Military Trail
Street Address
201
Suite
West Palm Beach FL 34997
City State Zip Code

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

BY:


Signature of Authorized Official

BY: DocuSigned by:


Signature of Authorized Official

Stephanie Sejnoha

Printed/Typed Name

Mark Hernandez

Printed/Typed Name

Director, Public Safety Department

Title

Bureau Chief, Purchasing & Contracts

Title

3/11/24

Date

April 25, 2024

Date

ssejnoha@pbcgov.org

Official Requesting Party Email Address

561-712-6473

Phone Number

59-6000785

FEIN

APPROVED AS TO FORM
AND LEGAL SUFFICIENCY


By: Richard Sena
Asst. County Attorney

Requesting Party Point of Contact:

Rob Shelt

Printed/Typed Name

APPROVED AS TO TERMS
AND CONDITIONS


By: Rob Shelt, Director
Consumer Affairs Division

rshelt@pbcgov.org

Official Requesting Party Email Address

561 / 712-6600 Phone Number

561 / 712-6610 Fax Number

ATTACHMENT I

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

The Driver's Privacy Protection Act, 18 United States Code sections 2721 ("DPPA") makes personal information contained in motor vehicle or driver license records confidential and exempt from disclosure. Personal information in a motor vehicle or driver license record includes, but is not limited to, an individual's social security number, driver license or identification number, name, address, and medical or disability information. Personal information does not include information related to driving violations and driver status. Personal information from these records may only be released to individuals or organizations that qualify under one of the exemptions provided in DPPA, which are listed on the back of this form.


I am an authorized representative of an organization requesting personal information for one or more records as described below. I declare that my organization is qualified to obtain personal information under exemption number(s) 1, as listed on page 2 of this form.

I understand that I shall not use or redisclose this personal information except as provided in DPPA and that any use or redisclosure in violation of these laws or statutes may subject me to criminal sanctions and civil liability.


Complete the following for each DPPA exemption being claimed (attach additional page, if necessary):


DPPA Exemption Claimed:	Description of how Requesting Party qualifies for exemption:	Description of how data will be used:
1	Government agency in carrying out its functions.	The data will be used to assist in the administration, licensing and enforcement, of consumer protection ordinances: Vehicle for Hire, Towing and Immobilization Services, and Moving, Chapter 17, Article VIII and Chapter 19 Articles IX, VIII respectively. The assessment and licensing is required to evaluate applicants wishing to obtain driver I.D. and vehicle permits, which exist to protect the health and safety of the visitors and residents in Palm Beach County.

Obtaining personal information under false pretenses is a state and federal crime. Under penalties of perjury, I declare that I have read the foregoing Request For Access to Driver And Vehicle Information Database System and that I am entitled to receive Exempt Personal Information in A Motor Vehicle/Driver License Record and that the facts stated in it are true and correct.


 Signature of Authorized Official
Stephanie Sejnoha
 Printed Name
3/11/24
 Date

Director, Public Safety Department
 Title
 Palm Beach County Board of County Commissioners

APPROVED AS TO FORM AND LEGAL SUFFICIENCY

 By: Richard Sena
 Asst. County Attorney

Name of Agency/Entity
 APPROVED AS TO TERMS AND CONDITIONS

 By: Rob Shell, Director
 Consumer Affairs Division



FLORIDA DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES

DATA EXCHANGE MEMORANDUM OF UNDERSTANDING

This Memorandum of Understanding (MOU) is made and entered into by and between Palm Beach County Board of County Commissioners, hereafter referred to as the Requesting Party, and the Florida Department of Highway Safety and Motor Vehicles, hereafter 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. Based upon the nature of this information, the Providing Agency is subject to the various disclosure prohibitions and restrictions contained in 18 U.S.C. §2721, the Driver’s Privacy Protection Act (hereafter “DPPA”), sections 119.0712(2), 316.066, 324.242, and 501.171, Florida Statutes, and other statutory provisions.

The Requesting Party is a Government Entity or Private Entity operating under the laws and authority of the state of Florida and/or operating under federal laws and is requesting Personal Information and declares that it is qualified to obtain Personal Information under the exception number(s), listed in Attachment I, authorized by DPPA.

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 Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and/or Insurance Record Information to the Requesting Party.

The types of data requested and the applicable statutory fees if applicable, are agreed to by both parties as indicated in Attachment II.

The Requesting Party is receiving a 9-digit, a 4-digit, or no social security number, pursuant to Chapter 119, Florida Statutes, or other applicable laws.

II. Definitions

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

- A. **Batch/File Transfer Protocol (FTP)/Secure File Transfer Protocol (SFTP)** - An electronic transfer of data in a secure environment.
- B. **Business Point-of-Contact** - A person appointed by the Requesting Party to assist the Providing Agency with the administration of the MOU.
- C. **Consumer Complaint Point-of-Contact** - A person appointed by the Requesting Party to assist the Providing Agency with complaints from consumers regarding misuse of Personal Information protected under DPPA.
- D. **Control Record** - A record containing fictitious information that is included in data made available by the Providing Agency and is used to identify inappropriate disclosure or misuse of data.
- E. **Crash Insurance Information** - Insurance information, such as insurance company name, policy type, policy status, insurance creation and expiration date, including insurance policy number, provided to the Requesting Party pursuant to section 324.242, Florida Statutes, on vehicles involved in a crash.
- F. **Crash Report Information** - Information derived from crash reports submitted by the investigating law enforcement agency to the Providing Agency and entered into a computerized database pursuant to section 316.066, Florida Statutes, which includes Personal Information and the employment street address, and the home and telephone

numbers of the Parties involved in the crash.

- G. Downstream Entity** - Any individual, association, organization, or corporate entity who receives Driver License Information, Crash Report Information, Crash Insurance Information, and/or Insurance Record Information from a Third Party End User in accordance with DPPA and section 119.0712(2), Florida Statutes.
- H. Driver License Information** – Driver license and identification card data collected and maintained by the Providing Agency. This data includes Personal Information .
- I. Driver’s 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.
- J. Government Entity** - Any federal, state, county, county officer, or city government, including any court or law enforcement agency.
- K. Highly Restricted Personal Information** – Information that includes, but is not limited to, medical or disability information and social security number.
- L. Insurance Record Information** - Insurance information, such as insurance company name, policy type, policy status, insurance creation and expiration date, but excluding insurance policy number, provided to the Requesting Party, pursuant to section 324.242, Florida Statutes.
- M. Motor Vehicle Information** - Title and registration data collected and maintained by the Providing Agency for vehicles and vessels. This information includes Personal Information.
- N. Parties** - The Providing Agency and the Requesting Party.
- O. Personal Information** - As described in section 119.0712(2)(b), Florida Statutes and 18 U.S.C. S.2725, information which includes, but is not limited to, the subject’s driver identification number, name, address, (but not including the 5–digit zip code), date of

birth, height, race, gender and medical or disability information.

- P. Private Entity** - Any entity that is not a unit of government, including, but not limited to, a corporation, partnership, limited liability company, nonprofit organization or other legal entity or a natural person.
- Q. Providing Agency** - The Department of Highway Safety and Motor Vehicles.
- R. Requesting Party** - Any entity type that is expressly authorized by section 119.0712(2), Florida Statutes and DPPA to receive Personal Information and/or Highly Restricted Personal Information that requests information contained in a driver license or motor vehicle record from the Providing Agency through remote electronic access.
- S. Requesting Party Number** - A unique number assigned to the Requesting Party by the Providing Agency that identifies the type of records authorized for release and the associated statutory fees for such records.
- T. Technical Contact** - A person appointed by the Requesting Party to oversee the maintenance/operation of setting up of Web Service and Batch/FTP/SFTP processes.
- U. Third Party End User** - Any individual, association, organization, or corporate entity who receives Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and Insurance Record Information from the Requesting Party in accordance with DPPA and sections 119.0712(2), 316.066, and 324.242, Florida Statutes.
- V. Web Service** - A service where the Requesting Party writes a call program to communicate with the Web Service of the Providing Agency to receive authorized motor vehicle and driver license data.

III. Legal Authority: Restrictions on the Dissemination of Information Provided by the Providing Agency

- A.** The Providing Agency maintains computer databases containing information pertaining to

driver's licenses and motor vehicles pursuant to Chapters 316, 317, 319, 320, 322, 328, and section 324.242, Florida Statutes. The Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, Insurance Record Information and vessel data contained in the Providing Agency's databases is defined as public record pursuant to Chapter 119, Florida Statutes and, as such, are subject to public disclosure, unless otherwise exempted from disclosure or made confidential by law.

- B.** As the custodian of the state's Driver License Information, Motor Vehicle Information Crash Report Information, Crash Insurance Information, and Insurance Record Information, , the Providing Agency is responsible for providing access only to records and information permitted to be disclosed by law.
- C.** Under this MOU, the Requesting Party will be provided, via remote electronic means, certain Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and Insurance Record Information, including Personal Information authorized to be released pursuant to DPPA and sections 119.0712(2), 316.066, or 324.242, Florida Statutes,
- D.** Highly Restricted Personal Information shall only be released in accordance with DPPA and Florida law.
- E.** The Providing Party only may provide information derived from crash reports to the Requesting Party pursuant to section 316.066(2), Florida Statutes. Sixty days after the date a crash report is filed, the Providing Agency may provide Crash Report Information to entities eligible to access the crash report pursuant to section 316.066(2)(b), Florida Statutes, and in accordance with any of the permissible uses listed in 18 U.S.C. s. 2721(b) and pursuant to the resale and redisclosure requirements in 18 U.S.C. s. 2721(c).
- F.** The Parties agree that all provisions herein concerning the protection, disclosure, or distribution of data provided by the Providing Agency to the Requesting Party shall survive the expiration or termination of this MOU, and that the Providing Agency reserves the right to enforce the provisions of this MOU after the MOU's expiration or termination, including obtaining injunctive relief.

- G. This MOU is governed by the laws of the State of Florida and venue for any dispute arising from this MOU shall be exclusively in Leon County, Florida.

IV. Statement of Work

A. The Providing Agency agrees to:

1. Provide the Requesting Party with the technical specifications, and Requesting Party Number if applicable, required to access data in accordance with this MOU and the access method being requested.
2. Allow the Requesting Party to electronically access Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and Insurance Record Information as authorized under this MOU, DPPA, and sections 119.0712(2), 316.066, and 324.242, Florida Statutes.
3. Collect all fees for providing the electronically requested data, pursuant to applicable Florida Statutes, rules and policies, including sections 320.05 and 322.20, Florida Statutes. The fee shall include all direct and indirect costs of providing remote electronic access, according to section 119.07(2)(c), Florida Statutes.
4. Collect all fees due for electronic requests through the Automated Clearing House account of the banking institution which has been designated by the Treasurer of the State of Florida for such purposes.
5. Terminate the access of the Requesting Party for non-payment of required fees. The Providing Agency shall not be responsible for the failure, refusal, or inability of the Requesting Party to make the required payments, or interest on late payments for periods of delay attributable to the action or inaction of the Requesting Party.
6. Notify the Requesting Party at least thirty (30) business days prior to changing any fee schedules, when it is reasonable and necessary to do so, as determined by the Providing Agency. All fees are established by Florida law. Any changes in fees shall be effective on

the effective date of the corresponding law change. The Requesting Party may continue with this MOU, as modified, or it may terminate the MOU in accordance with Section XI., subject to the payment of all fees incurred prior to termination.

7. Perform all obligations to provide access under this MOU contingent upon an annual appropriation by the Legislature.
8. Provide electronic access to Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and Insurance Record Information, pursuant to roles and times established other than scheduled maintenance or periods of uncontrollable disruptions. Scheduled maintenance normally occurs Sunday mornings between the hours of 6:00 A.M. and 10:00 A.M., Eastern Time.
9. Provide a contact person for assistance with the implementation of this MOU.

B. The Requesting Party agrees to:

1. Access or utilize all information provided by the Providing Agency pursuant to this MOU in strict compliance with DPPA and sections 119.0712(2), 316.066, and 324.242, Florida Statutes.
2. Maintain the confidential and exempt status of all information provided by the Providing Agency pursuant to this MOU as required by DPPA and sections 119.0712(2), 316.066, and 324.242, Florida Statutes.
3. Ensure that any Third Party End Users and Downstream Users accessing or utilizing information obtained by the Requesting Party by, through, or as a result of this MOU shall do so strictly in compliance with DPPA and sections 119.0712(2), 316.066, and 324.242, Florida Statutes.
4. Ensure that any Third Party End Users and Downstream Users accessing or utilizing information obtained by the Requesting Party by, through, or as a result of this MOU maintains the confidential and exempt status of such information as required by DPPA

and sections 119.0712(2), 316.066, and 324.242, Florida Statutes.

5. Ensure that Highly Restricted Personal Information, including that accessed by any Third Party End Users and Downstream Users by, through, or as a result of this MOU, only may be released as authorized by DPPA and Florida law.
6. Request access to Crash Insurance Information, including Vehicle Identification Number, if authorized pursuant to this MOU only for vehicles actually involved in a crash or for vehicles of persons involved in a crash. Access to Crash Insurance Information will be provided by the Providing Agency only upon the submission by the Requesting Party of the date of a specific crash, the associated crash report number, and evidence that the Requesting Party or a Third Party End User is the attorney of the person involved in a specific crash or a representative of the insurer of a person involved in a specific crash.
7. Use information provided pursuant to this MOU only for the expressed purposes as described in Attachment I of this MOU.
8. Not misuse its Requesting Party Number to obtain information pursuant to this MOU for any use which violates this MOU and the immediate termination of this MOU by the Providing Agency upon the discovery of any misuse by the Requesting Party of its Requesting Party Number.
9. Self-report to the Providing Agency all violations of the MOU within five (5) business days of discovery of such violation(s). The report shall include a description, the time period, the number of records impacted, the harm caused, and all steps taken as of the date of the report to remedy or mitigate any injury caused by the violation.
10. Accept responsibility for interfacing with any and all Third Party End Users. The Providing Agency will not interact directly with any Third Party End Users. Requesting Party shall not give Third Party End Users the name, e-mail address, or telephone number of any Providing Agency employee without the express written consent of the Providing Agency. In addition, the Requesting Party agrees to have controls in place to ensure Third Party End Users comply with all requirements of this MOU.

11. Have controls in place to ensure Third Party End Users who redisclose FLHSMV data to Downstream Entities are subject to the terms and conditions of this MOU and that such Downstream Entities comply with this MOU, DPPA, and sections 119.0712(2), 316.066, and 324.242, Florida Statutes
12. Establish procedures to ensure that its employees and agents, including any contractors carrying out work on behalf of the Requesting Party or Third Party End Users and/or Downstream Entities, comply with Section V., Safeguarding Information, and provide a copy of the procedures to the Providing Agency within ten (10) business days of a request.
13. Not assign, sub-contract, or otherwise transfer its rights, duties, or obligations under this MOU without the express written consent and approval of the Providing Agency.
14. Use the information received from the Providing Agency only for the purposes authorized by this MOU, DPPA, and sections 119.0712(2), 316.066, and 324.242, Florida Statutes. The Requesting Party shall not:
 - a. Redisclose the information received from the Providing Agency for bulk distribution for surveys, marketing or solicitations.
 - b. Share or provide any information to another unauthorized entity, agency or person.
15. 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 laws.
16. Indemnify the Providing Agency and its employees from any and all damages arising from the Requesting Party's negligent or wrongful use of information provided by the Providing Agency, to the extent allowed by law. This provision is not applicable to federal governmental entities.
17. For federal governmental entities: 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, agents, 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.

18. Update user access/permissions upon reassignment of users within five (5) business days.
19. Immediately inactivate user access/permissions following separation, negligent, improper, or unauthorized use or dissemination of any information.
20. For all records containing Personal Information released to a Third Party End User, maintain records identifying each person or entity that receives the Personal Information and the permitted purpose for which it will be used for a period of five (5) years. The Requesting Party shall provide such records or otherwise make such records available for inspection by the Providing Agency not later than five (5) business days after receipt of a request from the Providing Agency.
21. Pay all costs associated with electronic access of the Providing Agency's Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and Insurance Record Information. The Requesting Party shall:
 - a. Maintain an account with a banking institution as required by the Providing Agency.
 - b. Complete and sign the appropriate document(s) to allow the Providing Agency's designated banking institution to debit the Requesting Party's designated account.
 - c. Pay all fees due the Providing Agency by way of the Automated Clearing House account of the Providing Agency's designated banking institution. Collection of transaction fees from eligible and authorized Third Party End Users is the responsibility of the Requesting Party.
22. Notify the Providing Agency within five (5) business days of any changes to the name, address, telephone number or email address of the Requesting Party, its Point-of-Contact

for Consumer Complaints, and/or its Technical Contact. The information shall be e-mailed to DataListingUnit@flhsmv.gov. Failure to update this information as required may adversely affect the timely receipt of information from the Providing Agency.

23. Immediately notify the Providing Agency of any change of FTP/SFTP for the receipt of data under this MOU. Failure to update this information as required may adversely affect the timely receipt of information from the Providing Agency.
24. Understand that this MOU is subject to any restrictions, limitations or conditions enacted by the Florida Legislature, which may affect any or all terms of this MOU. The Requesting Party understands that it is obligated to comply with all applicable provisions of law.
25. Timely submit Internal Control and Data Security Audits required by Section VII., A. and the statements required in Section VII., B. and C.
26. A Requesting Party who has not previously received records from the Providing Agency shall utilize Web Services currently offered by the Providing Agency rather than batch/FTP/SFTP processes. Also, any Requesting Party using the FTP/SFTP processes agrees to transition to Web Services, where available, within six months (6) months of the Providing Agency's request.
27. Cooperate and ensure that its subcontractors, if any, cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing pursuant to section 20.055, Florida Statutes.
28. If the Requesting Party, a Third Party End User, or Downstream Entity that receives data from the Requesting Party has a public facing website that allows an individual to obtain Driver License Information or Motor Vehicle Information, the following minimum requirements must be in place prior to the transmission of data:
 - a. Safeguards to ensure information obtained through the website is only disclosed to individuals authorized to receive it under 18 U.S.C. §2721(b). This includes internal controls to prevent or detect instances in which an individual attempts to purchase a

record other than their own or to verify that the requestor meets a DPPA exemption.

- b. If the Requesting Party intends to allow an individual to purchase their own transcript from the Requesting Party's website utilizing the DPPA permissible use provided by 18 U.S.C. §2721(b)(13), a process to verify that the payment instrument used to authorize the purchase is in the same name as the transcript being requested.
- c. Safeguards to ensure that information is provided through the website only for the expressed purposes as described in Attachment I of this MOU.
- d. Use of Transport Layer Security version 1.2 or later for encryption of data in transit and in session state.
- e. Safeguards to ensure that the website is periodically scanned by a qualified external vendor for system vulnerabilities and all identified vulnerabilities are promptly remedied.
- f. Safeguards to ensure that all systems that process Driver License Information or Motor Vehicle Information adhere to a formalized patch management process.
- g. If the Requesting Party allows Third Party End Users or Downstream Entities to have a public facing website, the Requesting Party shall have controls in place to ensure the Third Party End User or Downstream Entity meets these requirements.

V. Safeguarding Information

- A. 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, sections 316.066 and 324.242, 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 laws. Any disclosure of information shall be in accordance with 18 U.S.C. §2721(c). In the event of a security breach, the Requesting Party agrees to comply with the provisions of section 501.171, Florida Statutes.

- B. Any person who knowingly violates section 119.0712(2), Florida Statutes or section 316.066, Florida Statutes, may be subject to criminal punishment and civil liability, as provided in sections 119.10 or 316.066, Florida Statutes. In addition, any person who knowingly discloses any information in violation of DPPA may be subject to criminal sanctions, including fines, and civil liability.

- C. In an effort to ensure information is only used in accordance with Chapter 119, Florida Statutes, and DPPA, the Providing Agency may include Control Records in the data provided in an effort to identify misuse of the data.

- D. The Requesting Party shall notify the Providing Agency of any of the following within five (5) business days:
 - 1. Termination of any agreement/contract between the Requesting Party and any other state or State Agency due to non-compliance with DPPA, data breaches, or any state laws relating to the protection of driver privacy. The Requesting Party shall also notify the Providing Agency if any state or State Agency declines to enter into an agreement/contract with the Requesting Party to provide DPPA protected data.

 - 2. Any pending litigation alleging violations of DPPA or any law of any state relating to the protection of driver privacy.

 - 3. Any instance where the Requesting Party is found guilty or liable by a court of competent jurisdiction for misuse of data under DPPA or under any law of any state relating to the protection of driver privacy.

 - 4. Any instance where the owner, officer, or control person of the Requesting Party owned a majority interest in, or acted as a control person of, an entity that was found guilty or liable by a court of competent jurisdiction for misuse of data under DPPA or under any law of any state relating to the protection of driver privacy.

 - 5. A breach of security as defined by section 501.171, Florida Statutes.

E. The Parties mutually agree to the following:

1. Information exchanged will not be used for any purposes not specifically authorized by this MOU and its attachments. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, and the dissemination, sharing, copying or passing of this or any unauthorized information to unauthorized persons.
2. The Requesting Party will not be liable to the Providing Agency for any Driver License Information or Motor Vehicle Information lost, damaged, or destroyed as a result of the electronic exchange of data pursuant to this MOU, unless resulting from a negligent or wrongful act or omission of the Requesting Party.
3. Information obtained from the Providing Agency will be stored in a location that is physically and logically secure from access by unauthorized persons.
4. The Requesting Party shall adopt cybersecurity standards that safeguard Department provided data, Department information technology and Department information technology resources to ensure confidentiality, and integrity. The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework, Florida Administrative Code 60GG-2, s. 282.318, 282.3185, Florida Statutes and applicable agency security policies set forth in Attachment III. Access to the information received from the Providing Agency will be protected in such a way that unauthorized persons cannot view, retrieve, or print the information.
5. All personnel with access to the information exchanged under the terms of this MOU will be instructed about, and acknowledge in writing their understanding of, the confidential nature of the information. These written acknowledgements must be maintained in a current status by the Requesting Party and provided to the Providing Agency not later than ten (10) business days after a written request from the Providing Agency to review the written acknowledgments.
6. All personnel with access to the information will be instructed about and acknowledge in

writing their understanding of the civil and criminal sanctions specified in state and federal law for unauthorized use of the data. These written acknowledgements must be maintained in a current status by the Requesting Party and provided to the Providing Agency not later than ten (10) business days after a written request from the Providing Agency to review the written acknowledgments.

7. All access to the information must be monitored on an ongoing basis by the Requesting Party. In addition, the Requesting Party must complete an Annual Certification Statement to ensure proper and authorized use and dissemination of information and provide it to the Providing Agency pursuant to Section VII. B, below.
8. All data received from the Providing Agency shall be encrypted during transmission to Third Party End Users using Transport Layer Security (TLS) version 1.2 or higher encryption protocols. Alternate encryption protocols are acceptable only upon prior written approval by the Providing Agency.
9. By signing the MOU, the representatives of the Providing Agency and Requesting Party, on behalf of the respective Parties, attest and ensure that the confidentiality of the information exchanged will be maintained.

VI. Third Party End Users

Any agreement by the Requesting Party to provide Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, or Insurance Record Information to a Third Party End User and any agreement by a Third Party End User to provide Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, or Insurance Record Information to a Downstream Entity shall:

- A. Be in writing.
- B. Include and incorporate this MOU by reference without any change to this MOU.
- C. Require the Third Party End User and any Downstream Entity to comply with DPPA and

sections 119.0712(2), 316.066, and 324.242, Florida Statutes.

- D. Require the Third Party End User and any Downstream Entity to acknowledge in writing that, by receipt of Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, or Insurance Record Information, such Third Party End User and Downstream Entity are subject to and must comply with DPPA, sections 119.0712(2), 316.066, and 324.242, Florida Statutes.
- E. Require the Requesting Party, Third Party End User, and any Downstream Entity to provide a copy of such agreement to the Providing Agency within ten (10) business days after a request by the Providing Agency for a copy of such agreement.

The failure of a Requesting Party, Third Party End User, and Downstream Entity to timely provide a copy of such agreement to the Providing Agency when requested by the Providing Agency shall be cause for the immediate termination of this MOU by the Providing Agency.

VII. Compliance and Control Measures

- A. Internal Control and Data Security Audit - This MOU is contingent upon the Requesting Party having appropriate internal controls in place at all times to ensure that the information provided or received pursuant to this MOU is protected from unauthorized access, distribution, use, modification, or disclosure. The Requesting Party must submit to the Providing Agency an Internal Control and Data Security Audit from a currently licensed Certified Public Accountant (CPA), on or before the first anniversary of the execution date of this MOU or within one hundred twenty (120) days from receipt of a written request from the Providing Agency. Government agencies may submit the Internal Control and Data Security Audit from their Agency's Internal Auditor or Inspector General. The audit report shall be sent to the Providing Agency in the manner prescribed in Section XII, for Notices.
 - 1. The audit report shall:
 - a. Indicate whether the internal controls governing the use and dissemination of personal data have been evaluated based on the requirements of this MOU (see item

- 2 below).
- b. Indicate whether those internal controls included data security policies/procedures in place for personnel to follow and data security procedures/policies in place to protect personal data.
 - c. Indicate whether those data security procedures/policies have been approved by a Risk Management IT Security Professional, with credentials such as, but not limited to: CISA, CISSP, CISM, or CRISC.
 - d. Indicate whether any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence.
 - e. Include an opinion on whether those internal controls are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure.
2. The audit must be based on the requirements of this MOU, Florida Administrative Code Rule 60GG-2, and the Providing Agency's External Information Security Policy (attachment III). Engagements that do not consider these specific criteria or do not render an independent auditor's opinion or conclusion will not meet the requirements for the Internal Control and Data Security Audit. The Parties agree that a SOC 2 Report, consulting service engagement, or other audit report type will not satisfy the requirements for the Internal Control and Data Security Audit if the SOC 2 Report, consulting service engagement, or other audit report does not specifically address each of the elements listed in Section VII., A., 1. a., b., c., d., and e.
 3. The Parties agree that an audit report which includes an audit period entirely outside the term of this MOU does not satisfy the requirements for the Internal Control and Data Security Audit.
 4. The Requesting Party is responsible for clearly specifying the above audit requirements to the CPA, or government agency auditor, before audit work commences.

- B. Annual Certification Statement -** The Requesting Party shall submit to the Providing Agency an annual statement, utilizing Attachment IV, 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 and applicable laws. The Requesting Party shall submit this statement to the Providing Agency annually, not later than fifteen (15) business days after the anniversary of the execution date of this MOU. (NOTE: During any year in which an Internal Control and Data Security Audit is conducted and submitted to the Providing Agency, submission of the Internal Control and Data Security Audit may satisfy the requirement for submission of an Annual Certification Statement.) Failure to timely submit the annual certification statement may result in an immediate termination of this MOU. The annual certification statement shall be sent to the Providing Agency in the manner prescribed in Section XII, for Notices.

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

- C. Misuse of Personal Information –** The Requesting Party must notify the Providing Agency in writing of any incident where it is suspected or confirmed that Personal Information has been compromised as a result of unauthorized access, distribution, use, modification, or disclosure, by any means, within five (5) business days of such discovery. The statement must be provided on the Requesting Party'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 persons whose Personal Information was compromised were notified. The statement shall also indicate the steps taken, or to be taken, by the Requesting Party to ensure that misuse of data does not continue or recur. This statement shall be sent to the Providing Agency in the manner prescribed in Section XII, for Notices. (NOTE: If an incident involving breach of Personal Information did occur and the

Requesting Party did not notify the owner(s) of the compromised records, the Requesting Party must indicate why notice was not provided.)

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 and be solely responsible for adhering to the provisions regarding notice provided therein.

- D. Consumer Complaints – The Requesting Party shall provide a point-of-contact for consumer complaints. In the event the Providing Agency receives a consumer complaint regarding misuse of DPPA protected information, the Requesting Party shall review and investigate the complaint. The Requesting Party shall provide its findings to the Providing Agency not later than fifteen (15) business days from the date the Requesting Party receives notice of such a complaint from the Providing Agency.

Consumer Complaint Point-of-Contact Information:

Name: Rob Shelt
Email: rshelt@pbcgov.org
Phone Number: 561-712-6605

- E. Control Records - In the event a Control Record inserted into data received by the Requesting Party is used in a manner that does not comply with DPPA or state law and upon the written request of the Providing Agency to the Requesting Party, the Requesting Party shall conduct an investigation of any Third Party End Users who obtained the record from the Requesting Party. As part of this provision, the Requesting Party shall also retain the authority to require Third Party End Users to investigate the Downstream Entities' handling and distribution of data subject to protection pursuant to DPPA and state law and to provide the results of the investigation to the Requesting Party. The Requesting Party shall provide the results of the investigation(s), together with all associated documents and information collected by the Requesting Party, Third Party Users and Downstream Entities, to the Providing Agency not later than fifteen (15) business days after receipt by the Requesting Party of the written request from the Providing Agency. When the Providing Agency requests the results of such

an investigation, the results of the investigation shall be sent to the Providing Agency in the manner prescribed in Section XII., for Notices.

VIII. Liquidated Damages

Unless the Requesting Party is a state agency, the Providing Agency reserves the right to impose liquidated damages upon the Requesting Party. The imposition of liquidated damages by the Providing Agency is separate from and unrelated to any other applicable criminal or civil penalties authorized by law for violations of DPPA and sections 119.0712, 316.066, or 324.242, Florida Statutes.

Failure by the Requesting Party to meet the established requirements of this MOU may result in the Providing Agency finding the Requesting Party to be out of compliance, and, all remedies provided in this MOU and under law, shall become available to the Providing Agency.

A. General Liquidated Damages

In the case of a breach or misuse of information received pursuant to this MOU due to non-compliance with DPPA, sections 119.0712(2), 316.066, 324.242, 501.171, Florida Statutes, or any other state laws designed to protect the privacy of a driver's Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, or Insurance Record Information, the Providing Agency may impose upon the Requesting Party liquidated damages of up to \$25.00 per record for each record involved in such breach or misuse.

In imposing liquidated damages, the Providing Agency will consider various circumstances including, but not limited to:

1. The Requesting Party's history with complying with DPPA, sections 119.0712(2), 316.066, 324.242, and 501.171, Florida Statutes, or any other state laws designed to protect a driver's privacy;
2. Whether the Requesting Party self-reported violations of this MOU to the Providing

Agency prior to discovery by the Providing Agency;

3. Whether the Requesting Party violated this MOU over an extended period of time;
4. Whether the Requesting Party's violation of this MOU directly or indirectly resulted in injury, and the nature and extent of the injury;
5. The number of records involved or impacted by the violation of this MOU;
6. Whether, at the time of the violation, the Requesting Party had controls and procedures that were implemented and reasonably designed to prevent or detect violations of this MOU; and,
7. Whether the Requesting Party voluntarily made restitution or otherwise remedied or mitigated the harm caused by the violation of this MOU.

In lieu of paying liquidated damages to the Providing Agency upon assessment of such damages by the Providing Agency, the Requesting Party may elect to temporarily suspend this MOU, contingent upon the Requesting Party submitting a written statement that the Requesting Party will not obtain information from the Providing Agency through remote electronic means until such time as the liquidated damages assessed by the Providing Agency are paid by the Requesting Party in full. Such statement shall be signed by the Requesting Party's authorized representative and shall be submitted to the Providing Agency in the manner prescribed in Section XII, for Notices not later than five days after receipt of notice by the Requesting Agency that liquidated damages have been assessed.

The Requesting Party agrees that the Providing Agency may refuse to enter a subsequent or replacement MOU with the Requesting Agency to allow the Requesting Party to access information available pursuant to this MOU through remote electronic means until the Requesting Party has paid all outstanding liquidated damages in full. The Requesting Party agrees that this subsection A shall survive the termination of this MOU.

B. Corrective Action Plan (CAP)

1. If the Providing Agency determines that the Requesting Party is out of compliance with any of the provisions of this MOU, including, without limitation thereto, submission of an Internal Control and Data Security Audit that does not meet the requirements set forth in Section VII., and requires the Requesting Party to submit a CAP, the Providing Agency may require the Requesting Party to submit a Corrective Action Plan (CAP) within a specified timeframe. The CAP shall provide an opportunity for the Requesting Party to resolve deficiencies without the Providing Agency invoking more serious remedies, up to and including MOU termination.
2. In the event the Providing Agency identifies a violation of this MOU, or other non-compliance with this MOU, the Providing Agency shall notify the Requesting Party of the occurrence in writing. The Providing Agency shall provide the Requesting Party with a timeframe for corrections to be made.
3. The Requesting Party shall respond by providing a CAP to the Providing Agency within the timeframe specified by the Providing Agency.
4. The Requesting Party shall implement the CAP only after the Providing Agency's approval of the CAP.
5. The Providing Agency may require changes or a complete rewrite of the CAP and provide a specific deadline for submission of such changes or rewritten CAP.
6. If the Requesting Party does not meet the standards established in the CAP within the agreed upon timeframe, the Requesting Party shall be in violation of the provisions of this MOU and shall be subject to liquidated damages and other remedies including termination of the MOU.
7. Except where otherwise specified, liquidated damages of \$25.00 per day may be imposed on the Requesting Party for each calendar day that the approved CAP is not implemented to the satisfaction of the Providing Agency.

IX. Agreement Term

This MOU shall take effect upon the date of last signature by the Parties and shall remain in effect for three (3) years from this date unless terminated or cancelled in accordance with Section XI., Termination and Suspension. Once executed, this MOU supersedes all previous agreements between the Parties regarding the same subject matter.

X. 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.

XI. Termination and Suspension

- 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 suspension or 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, but not limited to, DPPA, sections 119.0712(2), 316.066, 324.242 or 501.171, Florida Statutes, or any laws designed to protect driver privacy.
- C. This MOU may also be cancelled by either party, without penalty, upon thirty (30) business

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) business day notice period.

- D. This MOU may be terminated by the Providing Agency if the Requesting Party, or any of its majority owners, officers or control persons are found by a court of competent jurisdiction to have violated any provision of any state or federal law governing the privacy and disclosure of Personal Information. This MOU may be terminated in the event any agreement/contract between the Requesting Party and any other state or State Agency is terminated due to non-compliance with DPPA or data breaches, or any state laws designed to protect driver privacy. The Requesting Party will have ten (10) days from any action described above to provide mitigating information to the Providing Agency. If submitted timely, the Providing Agency will take the mitigation into account when determining whether termination of the MOU is warranted.

XII. Notices

Any notices required to be provided under this MOU shall be sent via Certified U.S. Mail and email to the following individuals:

For the Providing Agency:

Chief, Bureau of Records 2900 Apalachee Parkway
Tallahassee, Florida 32399
Tel: (850) 617-2702
Fax: (850) 617-5168
E-mail:Datalistingunit@flhsmv.gov

For the Requesting Party:

Requesting Party's Business Point-of-Contact listed on the signature page.

XIII. Additional Database Access/Subsequent MOU's

- A. The Parties understand and acknowledge that this MOU entitles the Requesting Party to

receive specific information included within the scope and subject to the requirements of this MOU. 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 audits, report submission, and the submission of Certification statements.

- B. 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, audits, and reports for each executed MOU. Accordingly, should the Requesting Party enter any subsequent MOU's 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 the Providing Agency's approval, to submit one of each of the following covering all executed MOU's: Certifications; Audit; or to have conducted one comprehensive audit addressing internal controls for all then-existing and effective MOU's with the Providing Agency. The Providing Agency shall have the sole discretion to approve or deny such request in whole or in part or to subsequently rescind any previously approved request based upon the Requesting Party's compliance with this MOU and/or any negative audit findings.

XIV. Public Records Requirements

- A. The Parties to this MOU recognize and acknowledge that any agency having custody of records made or received in connection with the transaction of official business remains responsible for responding to public records requests for those records in accordance with applicable law (specifically, Chapter 119, Florida Statutes) and that public records that are exempt or confidential from public records disclosure requirements will not be disclosed except as authorized by law.
- B. If the Requesting Party is a "contractor" as defined in section 119.0701(1)(a), Florida Statutes, 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 Providing Agency to perform the service.
2. Upon request from the Providing Agency's custodian of public records, provide the Providing Agency 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 term of this MOU and following completion of the MOU if the Requesting Party does not transfer the records to the Providing Agency.
4. Upon termination or expiration of the MOU, the Requesting Party agrees they shall cease disclosure or distribution of all data provided by the Providing Agency. In addition, the Requesting Party agrees that all data provided by the Providing Agency remains subject to the provisions contained in DPPA and sections 119.0712 and 501.171, Florida Statutes.

IF THE REQUESTING PARTY HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE REQUESTING PARTY'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS MOU, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (850) 617-3101, OGCFiling@flhsmv.gov, OFFICE OF GENERAL COUNSEL, 2900 APALACHEE PARKWAY, and STE. A432, TALLAHASSEE, FL 32399-0504.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

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

REQUESTING PARTY:

Palm Beach County Board of County Commissioners

Requesting Party Name

50 S. Military Trail

Street Address

201

Suite

WPB FL 33415

City State Zip Code

APPROVED AS TO FORM AND LEGAL SUFFICIENCY

By: 
Richard Sena, Asst. County Attorney

APPROVED AS TO TERMS AND CONDITIONS

By: 
Rob Shelt, Consumer Affairs Director

BUSINESS POINT-OF-CONTACT:

Rob Shelt

Printed/Typed Name

rshelt@pbcgov.org

Official Requesting Party Email Address

561-712-6605 / 561-712-6610

Phone Number / Fax Number

PROVIDING AGENCY:

Florida Department of Highway Safety and Motor Vehicles

Providing Agency Name

2900 Apalachee Parkway
Street Address

Suite

Tallahassee, Florida 32399
City State Zip Code

BY:


Signature of Authorized Official

Stephanie Sejnoha

Printed/Typed Name

Director, Public Safety Department

Title

3/11/24
Date

ssejnoha@pbcgov.org

Official Requesting Party Email Address

561-712-6473

Phone Number

TECHNICAL POINT-OF-CONTACT:

Dianne White

Printed/Typed Name

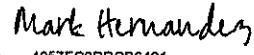
dwhite@pbcgov.org

Official Requesting Party Email Address

561-712-6621 / 561-712-6610

Phone Number / Fax Number

BY:

DocuSigned by:

4057FC0DDCB6421...
Signature of Authorized Official
Mark Hernandez

Printed/Typed Name

Chief, Bureau of Purchasing and Contracts
Title

April 25, 2024

Date

ATTACHMENT I

**FLORIDA DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES Request For
Exempt Personal Information In A Motor Vehicle/Driver License Record**

The Driver's Privacy Protection Act, 18 United States Code sections 2721("DPPA") makes personal information contained in motor vehicle or driver license records confidential and exempt from disclosure. Personal information in a motor vehicle or driver license record includes, but is not limited to, an individual's social security number, driver license or identification number, name, address and, medical or disability information. Personal information does not include information related to driving violations and driver status. Personal information from these records may only be released to individuals or organizations that qualify under one of the exemptions provided in DPPA, which are listed on the back of this form.

In lieu of completing this form, a request for information may be made in letter form (on company/agency letterhead, if appropriate) stating the type of information being requested, the DPPA exemption(s) under which the request is being made, a detailed description of the how the information will be used, and a statement that the information will not be used or redisclosed except as provided in DPPA. If the information is provided on letterhead it must include a statement that the information provided is true and correct, signed by the authorized official under penalty of perjury, and notarized.

I am a representative of an organization requesting personal information for one or more records as described below. I declare that my organization is qualified to obtain personal information under exemption number(s) 1, as listed beginning on page 4 of this form.

Pursuant to Section 316.066, F.S., Crash Report Information is confidential and exempt. 60 days after the date a crash report is filed, Crash Report Information may be provided which includes personal information to entities who are eligible to receive it under Section 316.066 (2), F.S., or in accordance with the Driver Privacy Protection Act. Crash Report Information cannot be used for commercial solicitation of crash victims or knowingly disclosed to any third party for purposes of such solicitation.

I understand that I shall not use or redisclose this personal information except as provided in DPPA and that any use or redisclosure in violation of these statutes may subject me to criminal sanctions and civil liability.

Complete the following for each DPPA exemption being claimed. For access to Crash Report Information, please provide justification of your organization’s eligibility under Section 316.066, F.S. below (attach additional page, if necessary):

DPPA Exemption Claimed:	Description of How Requesting Party Qualifies for Exemption:	Description of how Data will be used:
1	For use by any government agency in carrying out it's functions	The information requested is required for our agency to carry out its function of evaluating applicants, pursuant to county ordinance, who wish to receive an I.D. badge and/or vehicle decal for the purpose of operating in Palm Beach County, FL. The data will provide part of the information needed to assess applications based on Palm Beach County Code of Ordinances, Chapter 19, Article VIII - Towing and Immobilization Services and Article IX - Vehicle for Hire. The licensing is required to protect the health and safety of the citizens in Palm Beach County, FL.

Obtaining personal information under false pretenses is a state and federal crime. Under penalties of perjury, I declare that I have read the foregoing Request For Exempt Personal Information in A Motor Vehicle/Driver License Record and that the facts stated in it are true and correct.

Stephanie Sejnoha
Signature of Authorized Official

Stephanie Sejnoha
Printed Name

3/11/24
Date

Director, Public Safety Department

Title
Palm Beach County Board of County Commissioners

Name of Agency/Entity

APPROVED AS TO FORM AND LEGAL SUFFICIENCY

By: [Signature]
Richard Serra, Asst. County Attorney

APPROVED AS TO TERMS AND CONDITIONS

By: [Signature]
Rob Shell, Consumer Affairs Director

STATE OF Florida
COUNTY OF Palm Beach

Sworn to (or affirmed) and subscribed before me this 11th day of March 2024 by Stephanie Sejnoha.

Personally Known OR Produced Identification

Type of Identification Produced N/A

[Signature]
NOTARY PUBLIC (print name)

[Signature]
NOTARY PUBLIC (sign name)

My Commission Expires: _____



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, 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 under this subsection.
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.
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.

DATA ACCESS SPECIFICATIONS – Attachment II

Requesting Party: Palm Beach County Board of County Commissioners

Jobs and Processes Selected

Mode of Access	Type of Data Requested	Statutory Fees (subject to change by the Legislature)	
Batch (FTP)	DL Data (Driver License Information)	\$0.01/record, per s. 322.20, F.S.	No Charge
	MV Data (Motor Vehicle Information)	\$0.01/record, per s. 320.05, F.S.	No Charge
	DL Status (DSS600/605) (Driver License Information)	\$0.01, \$0.50/record, per s. 320.05, F.S.; \$2.00/record not found, per s. 322.20, F.S.	No Charge
Program/Job Name			
IP Address(es)			
Web Services			
Driver Transcript Web Service (Each service accesses Driver License Information)	DL Transcript (3 Year) (old DTR060)	\$8.00; \$2.00/record not found, per s. 322.20, F.S.	No Charge
	✓ DL Transcript (7 Year or Complete) (old DTR060)	✓ \$10.00; \$2.00/record not found, per s. 322.20, F.S.	No Charge
	Bulk Lookback (old DMS485)	\$0.01/record or \$2.00/record not found, per s. 322.20, F.S.	No Charge
Public Access Web Service	DL Status (Driver License Information)	\$0.50/ record, per s. 320.05, F.S.	No Charge
	MV Record (Motor Vehicle Information)	\$0.50/ record, per s. 320.05, F.S.	No Charge
	Insurance Record Information	\$0.50/ record, per s. 320.05, F.S.	No Charge
	Parking Permit Record Information	\$0.50/ record, per s. 320.05, F.S.	No Charge

DATA ACCESS SPECIFICATIONS – Attachment II

Mode of Access	Type of Data Requested	Statutory Fees (subject to change by the Legislature)	
Penny Vendor DL Web service	DL update file of issuance/ purge records (old DFO292) (Driver License Information	\$0.01/record, per s. 322.20, F. S.	No Charge
DL Status Verification	Driver License Status	\$0.01, \$0.50/record, per s. 320.05, F.S.; \$2.00/record not found, per s. 322.20, F.S.	No Charge
Residency Verification Web service			No Charge
Other Web Services			No Charge
Crash Report Information			No Charge



Dave Kerner
Executive Director

2500 Apalachee Parkway
Tallahassee, Florida 32399-0500
www.flhsmv.gov

Data Access Application

Prior to executing the Memorandum of Understanding (MOU) for Driver License and/or Motor Vehicle Data Exchange, the Requesting Party is required to complete this application. Please use additional pages as necessary.

- 1. In the last ten (10) years, has any agreement/contract between the Requesting Party and/or any other State/State Agency been terminated due to non-compliance with DPPA, data breaches, or any state laws relating to the protection of driver privacy? Yes No If yes, please explain and supply certified copies of the pertinent documents:

[Empty text box for response to question 1]

- 2. In the last ten (10) years, has any State/State Agency declined to enter into an agreement/contract with the Requesting Party to provide DPPA protected data? Yes No If yes, please explain:

[Empty text box for response to question 2]

- 3. Is there any pending litigation against the Requesting Party alleging violations of DPPA or any state law relating to the protection of driver privacy? Yes No If yes, please explain and provide a certified copy of the pertinent court documents:

[Empty text box for response to question 3]

- 4. In the last ten (10) years, has there been any instance where the Requesting Party has been found guilty or liable by a court of competent jurisdiction for misuse of data under DPPA or under any state law relating to the protection of driver privacy? Yes No If yes, please explain and provide certified copies of the pertinent documents:

[Empty text box for response to question 4]

5. In the last ten (10) years, has there been any instance where an owner, officer, or control person¹ of the Requesting Party who owned a majority interest in, or acted as a control person of, an entity that was found guilty or liable by a court of competent jurisdiction for misuse of data under DPPA or under any state law relating to the protection of driver privacy? Yes No If yes, please explain and provide certified copies of the pertinent documents:

6. In the last ten (10) years, has there been any breach of security as defined by Section 501.171, Florida Statutes? Yes No If yes, provide details of each breach and discuss all safeguards implemented as a result of the breach of security:

7. How you will ensure that all personnel with access to the information exchanged under the terms of the MOU are instructed of, and acknowledge their understanding of, the confidential nature of the information?

Instructions to personnel regarding the terms of the MOU are provided to personnel in face-to-face meeting. Personnel sign a statement acknowledging the confidential nature of the information.

8. Does your company or agency have a public facing website that allows an individual to purchase driver license/motor vehicle information? Yes No

If yes, please provide the URL: _____

In addition, please indicate whether your agency has the following minimum requirements listed below in place:

- A. Safeguards to ensure information obtained through the website is only disclosed to individuals authorized to receive it under 18 U.S.C. §2721(c). This includes internal controls to prevent or detect instances in which an impostor attempts to purchase a record other than their own and/or to verify that the requestor meets a DPPA exemption. Yes No N/A

Please describe safeguards:

N/A

¹ Control Person, for these purposes, means the power, directly or indirectly, to direct the management or policies of a company, whether through the ownership of securities, by contract, or otherwise. Any person that (i) is a director, general partner, or officer exercising executive responsibility (or having similar status or functions); (ii) directly or indirectly has the right to vote 25% or more of a class of a voting security or has the power to sell or direct the sale of 25% or more of a class of voting securities; or (iii) in the case of a partnership, has the right to receive upon dissolution, or has contributed, 25% or more of the capital, is presumed to control that company.

- B. Do you intend to allow individuals to purchase their own transcript from your public facing website, utilizing DPPA exemption number 13? Yes No N/A

- C. If the answer to the previous question is yes, do you have a process in place to verify that the payment instrument used to authorize the purchase is in the same name as the transcript being requested? Yes No N/A

Please explain the process:

- D. Do you only provide information through the website for the expressed purposes as described in Attachment I of this MOU? Yes No N/A

- E. Does the website utilize Transport Layer Security version 1.2 or later for encryption of data in transit and in session state? Yes No N/A

Please explain:

- F. Is the website periodically scanned by a qualified external vendor for system vulnerabilities? Yes No N/A

- G. If the answer to the previous question is yes, are identified vulnerabilities promptly remediated? Yes No N/A

Please explain:

- 9. Do all systems that process driver license / motor vehicle information adhere to a formalized patch management process? Yes No

Please explain:

Ivanti is the software used for patching.
Desktops are patched monthly.
Servers are patched quarterly.

In addition, the following documents are required:

- a. A copy of your business license.
- b. A copy of your State of Florida corporation licensure or certification.
- c. If providing services on behalf of a government entity, provide the supporting documentation to show or prove you are entitled to the DPPA exemption claimed. For example, a letter from each entity confirming the type of service being provided and/or an agreement with an entity authorizing you to conduct services.

Under penalty of perjury, I affirm that the information provided in this document is true and correct.

Stephanie Sejnoha
 Signature of Authorized Official

Stephanie Sejnoha
 Printed/Typed Name

Director, Public Safety Department
 Title

12/21/23
 Date

Palm Beach County Board of County Commissioners
 NAME OF AGENCY/ENTITY

APPROVED AS TO FORM AND LEGAL SUFFICIENCY

By: [Signature]
Richard Sena, Asst. County Attorney

APPROVED AS TO TERMS AND CONDITIONS

By: [Signature]
Rob Selt, Consumer Affairs Division Director

STATE OF Florida
COUNTY OF Palm Beach

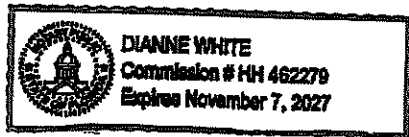
Sworn to (or affirmed) and subscribed before me this 21st day of Dec, 2023, by Stephanie Sejnoha.

Personally Known OR Produced Identification

Type of Identification Produced N/A
Dianne White

NOTARY PUBLIC (print name)

[Signature]
NOTARY PUBLIC (sign name)
My Commission Expires: _____



Dave Kerner
Executive Director



2900 Apalachee Parkway
Tallahassee, Florida 32399-0500
www.flhsmv.gov

CERTIFICATION STATEMENT

Under penalty of perjury I have read the requirements contained in the Memorandum of Understanding, Florida Administrative Code, Rule Chapter 60GG-2 (Formerly 74-2, FAC), and the Department of Highway Safety and Motor Vehicles External Information Security Policy and declare that the following is true:

The Requesting Party, Palm Beach County Board of County Commissioners hereby certifies that the Requesting Party has appropriate internal controls in place to ensure that the data is protected from unauthorized access, distribution, use, modification, or disclosure. This includes policies/procedures in place for both personnel to follow and data security procedures/policies to protect personal data. The data security procedures/policies have been approved by a Risk Management IT Security Professional.

STATE OF Florida
COUNTY OF Palm Beach

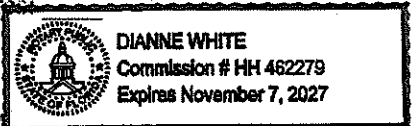
Sworn to (or affirmed) and subscribed before me this 21st day of Dec, 2023, by Stephanie Sejnoka.

Personally Known OR Produced Identification
Type of Identification Produced 33415

Dianne White
NOTARY PUBLIC (print name)

Dianne White
NOTARY PUBLIC (sign name)
My Commission Expires

Stephanie Sejnoka
Signature



APPROVED AS TO FORM AND LEGAL SUFFICIENCY

Stephanie Sejnoka
Printed Name

By: Richard Sena
Richard Sena, Asst. County Attorney

Director, Public Safety Department
Title

APPROVED AS TO TERMS AND CONDITIONS

12/21/23
Date

By: Rob Shelt
Rob Shelt, Consumer Affairs Division Director

Palm Beach County Board of County Commissioners
NAME OF AGENCY
(Rev. 01/23)