AAMVA

American Association of Motor Vehicle Administrators

INTERIM REPORT

Managing Data Privacy and External Access

May 2020

MANAGING DATA PRIVACY WORKING GROUP

Introduction

The demand for privacy protection and records management is an ever-expanding challenge to jurisdiction leaders, further compounded by significant leaks or breaches of federal and corporate databases and current federal and jurisdiction laws governing personally identifiable information (PII). These challenges must be met within the context of a proliferation of entities seeking driver and vehicle record data under public access laws.

To address these demands, the Managing Data Privacy and External Access Working Group (Working Group) is examining the issues and will identify best practices for jurisdictions to protect driver and vehicle records, provide access, authorize usage consistent with law, and apply effective and efficient approaches to internal and external audit practices.

Purpose of this Interim Report

The Working Group was approved by the AAMVA Board of Directors within the FY19 budget in the fall of 2018. A final best practices document is expected by early 2021. Recognizing that it takes time to establish a working group of member volunteers, research the issues, and develop guidance, the Board asked the Working Group to provide a document that can be helpful to jurisdictions in the interim.

This Interim Report provides a look at the topics the group is working through and some early recommendations. It should be noted that the recommendations will be refined and further developed in the final best practices document. This is not a comprehensive list of all recommendations. Examples of topics still being explored include:

- Offshoring of data
- Pre-approval of all sub-recipients receiving data
- Opt in and opt out
- Risk and impact structures as they relate directly to governance

Within this document, the following terms are used when referring to entities that receive data from a motor vehicle agency (MVA) either directly or indirectly.

Data recipients: entities receiving MVA data, especially PII or other data that can be used to identify one or more data subjects.

Sub-recipients: entities to which MVA data, especially PII, is re-disclosed by the data recipient.

Areas of Focus

As a result of the Working Group's efforts completed to date, we anticipate the final best practices document will include detailed information on the following topics:

- Purpose and Key Definitions
- Overview and Legal Foundation of Privacy
- Contracts
- Analysis of Request

- Records Management
- Compliance/Audit
- Misuse Response
- Public Safety
- Training
- Personnel
- Security
- Impact/Risk
- Data Governance
- Challenges

Structure of the Best Practices and Preliminary Recommendations for Jurisdictions

1. Purpose and Key Definitions

Provides an overview of the purpose of the best practices and describes benefits of releasing MVA data and PII.

2. Overview and Legal Foundation of Privacy

Outlines information regarding relevant U.S. and Canadian laws that address privacy and the foundation for protecting MVA data and PII.

Also considers the implications of identifying, tracking, and reporting ongoing privacy compliance requirements, e.g., federal and state law, case law, codes, etc.

3. Contracts

Describes exemplar agreements between motor vehicle agencies and data recipients. It establishes rules for sharing data and PII, data being shared, duration of agreements, permitted uses, how the data is shared, and any costs associated with sharing. Security provisions and third-party (data recipient and sub-recipient) risk management governance are also covered.

Recommended contract provisions include:

- Data and information ownership and property rights
- An "Information Security Audit" clause for the on-going review of security measures for both data recipients and sub-data recipients
- Requirement that data recipients track any further disclosures made to sub-recipients, including who the information was disclosed to, authorized usage, and ongoing monitoring of data usage
- Restriction on resale/re-disclosure or, at a minimum, definition of the parameters for re-disclosure, requiring the authorized recipient track every re-disclosure, including the permitted use
- Procedures to address instances of non-compliance with contracts and agreements

4. Analysis of Request

Includes best practices for analyzing requests and guidance on release of data. The chapter considers separate components of data requests such as who made the request, what data is being requested, previous requests, intended use of the data, volume and frequency of the request, planned re-disclosure, and method of receipt. The chapter also discusses, in detail, the appropriate risk assessment of the requested data.

It is recommended that MVAs consider developing and implementing an application process for all customers who wish to receive data maintained by MVAs on a one-time, regular, or bulk basis.

The application needs to collect sufficient information to determine if data will be released to the requester, what information the requester is entitled to receive, and the appropriate method of data transmission.

Following the application process and approval, the contract will ultimately define the controlling terms and allowable conditions of use.

At a minimum, the application requests the identity of the requesting individual or organization, any history of misuse or contract violations from previous data uses, the type of data requested, the purpose of the request, the volume and frequency of the requests, the requested method of data transfer, and security information.

MVAs can consider requiring data recipients to indicate if the data will be re-released to sub-recipients and the intended use.

The Working Group recommends setting up a procedure under which each application is reviewed by agency representatives who are business, legal, information technology, and information security personnel. If the large volume of requests render individual review by each area mentioned above impractical for the MVA, the MVA can create agreed-upon criteria to help identify which applications need to be elevated for further scrutiny.

5. Records Management

This chapter explains the concepts of data minimization, data anonymization, security of data once released to the customer (including minimum security safeguards, information technology, personnel, performance security {bond or escrow account} and physical security), logging, tracking and accounting, monitoring, data integrity/accuracy, customer data retention, data destruction, opt-in/opt-out, and special data type considerations.

It is recommended MVAs practice, and expect of those receiving MVA data to practice, minimization and anonymization of data.

MVAs can restrict how much data to share beyond the permissible uses in the contract. The results of a survey issued by the Working Group showed most respondents do not limit the number of records that can be provided with each request: most limitations are related to the specific data requested and the intended data recipient.

MVAs may consider establishing minimum security safeguards for data recipients to follow in order to protect MVA data. MVAs can consider requiring designation of a data security officer at each organization with a use agreement for communication and update purposes.

MVAs can implement logging, tracking, and accounting practices to ensure that data recipients are accessing data only for permissible purposes and in accordance with contract requirements. In addition to logging and tracking, jurisdictions can actively review data recipients' use of, and access to, MVA records (for example, using a desk audit or other monitoring process).

The data recipient can be required to obtain and maintain a bond, escrow account, or data privacy breach insurance coverage for the MVA's benefit. A suggested default amount is **ten percent** of the annual payments due to the MVA from the data recipient under the agreement.

The length of time the data recipient is permitted to retain the data provided by the jurisdiction, and approved methods of destruction, must be clearly identified prior to any data transfer. As a default best practice, the data recipient can be required to destroy jurisdiction data within **24 hours** of when it is no longer needed to meet the stated purpose and performance obligation specified in the use agreement.

It is recommended that MVAs understand and adhere to jurisdiction records disposal schedules and include a privacy statement on their websites.

6. Compliance/Audit

This chapter explains the key differences between compliance and audits, the types of audits (desk, on-site, operational, etc.), the importance and benefits of audits, and various audit approaches.

It is recommended that MVAs create an audit finding database/matrix to track all audit findings, recommendations, and corrective action plans for auditees (data recipients and sub-recipients). This database/matrix is used to trigger follow-up audits.

An annual audit plan can be developed by designing a risk assessment process of third-party/bulk user qualifiers (i.e., amount of transactions yearly, number of log-ins by a certain user, the type of data the user receives, etc.) weighted by risk of occurrence. Yearly audits can be planned based on the results of the risk assessments.

It is recommended that MVAs have the right to audit data recipients' data processing activities and systems including demonstrated compliance.

Additionally, the MVA can have the right to review the data recipient and sub-recipient information security processes and safeguards before providing PII or MVA data.

To improve the efficiency and value of data recipient audits, it is recommended that MVA's consider developing an audit guideline or model that if used by a comparable jurisdiction, could be accepted by another jurisdiction as compliant for that data recipient, in effect enabling audit portability.

7. Misuse Response

This section explains definitions of data misuse, data breach, and unauthorized access to MVA data. It covers incident handling and response, such as what steps to take before, during, and after a breach.

The guidelines recommend MVAs follow established response plans. However it is recommended that response plans include prompt investigation of incidents involving loss, damage, or misuse of information assets.

The Working Group recommends that MVAs promptly report incidents in accordance with the notification requirements in their jurisdictions.

MVAs are encouraged to establish and maintain an incident management plan and procedures for the following:

- Ensuring a breach is properly reported
- Assembling a team of experts
- Identifying a forensics team (if needed)
- Consulting with legal counsel
- Securing access and stopping additional data loss
- Preserving evidence
- Notifying appropriate parties

8. Public Safety

This chapter offers a history of criminal justice information systems and their interaction with MVAs, the importance of MVA data use by law enforcement to support public safety, and guidelines for sharing data with law enforcement.

It is recommended that MVAs retain governance authority and ownership of their data within the statutory and regulatory restrictions of their jurisdiction.

MVAs and law enforcement can maintain a collaborative working relationship and have a joint approval process for acceptable access to, and usage of, MVA data for authorized law enforcement purposes. MVAs need to have knowledge of all entities who may access driver and vehicle data.

It is recommended agreements be established between MVA and law enforcement agencies if one does not exist currently.

MVAs can individually and collaboratively review jurisdiction laws, contracts, and/or agreements in place that allow access to and secondary dissemination of MVA data for approved purposes.

9. Training

This chapter explains the importance of data privacy training, including new MVA employee onboarding and ongoing training and overseeing data recipient training.

MVAs are encouraged to consider establishing an audit program and to develop guidance for training needed and areas of risk for data privacy exposure.

MVAs can implement privacy training and regular refresher training, including training that relates to specific job content.

It is recommended that agents doing work on behalf of the jurisdiction document all provided training.

MVAs can consider maintenance of data privacy requirements for third parties.

MVAs can consider a certification program that would ensure agents are proficient in their data privacy management work.

Data recipients may adhere to industry standards including a vetting process for entities to which they sell their data.

10. Personnel

This chapter lists and defines key MVA staff roles that protect data privacy and data governance roles. It is recommended that MVA staff, at a minimum, fill the following roles to protect MVA data and PII:

- Data Privacy Officer (DPO)
- Contracts Compliance Officer
- Chief Information Security Officer (CISO)
- Auditor
- Data Steward(s)
- Data Sharing Manager
- Information Security and Privacy Compliance Manager

Survey respondents indicated that the Data Privacy Officer may be a shared role within the MVA (for instance with the CISO) or the MVA may use parent organization staff to fill this role. It further recommended the Data Privacy Officer be a dedicated position and not part of someone's multiple responsibilities/disciplines within the MVA.

It is recommended MVAs assign responsibility for data privacy to an individual who is in an independent oversight role.

MVAS may conduct regular communication with the privacy officer, legal, audit, IT, and others responsible/accountable for data privacy.

11. Security

This chapter contains general guidance for setting up a security plan or program, determining the scope of a plan/program, holding a high level discussion of what the "cloud" is and is not, general guidance on industry standards for data protection, lessons learned, and real life examples of data protection in a law enforcement and criminal justice context.

All MVA staff with access to PII must have a criminal history background check.

It is recommended all MVA data be encrypted whether in-transit or at rest.

MVAs can consider adopting and communicating common practices that safeguard personal data, including but not limited to the following:

- Do not use email for data sharing
- Do not use consumer grade file sharing tools
- Do not share any unnecessary information
- Do not create generic accounts for others to use while accessing your data

12. Impact/Risk

The Impact and Risk chapter provides guidance for risk assessment and risk mitigation, data classification, and security control selection.

MVAs can conduct regular risk assessments based on well-founded standards, specifically the National Institute of Standards and Technology (NIST) Risk Management Framework and associated publications. MVAs may also:

- Classify data and apply security controls to the systems that store PII
- Integrate data privacy risk into security risk assessments
- Maintain an inventory of PII and/or processing activities
- Maintain documentation of data flows between systems, processes, organizations etc.

MVAs may consider risk and data privacy assessments for new programs, systems, and processes and again when there are changes to existing programs, systems, and processes.

13. Data Governance

This chapter explains the basic concept of data governance and initial steps needed to develop a data governance model. Data governance policies cover security, privacy, integrity, usability, integration, compliance, availability, roles and responsibilities, roles of stakeholders, and overall management of the internal and external data flows within an organization.

It is recommended MVAs consider adoption of a minimum data governance structure or model as a foundation for adoption of a more mature structure or model. Survey results indicated that about half the respondents said yes - there is a data governance program at their MVA, while about the same number of yes responses said either no - there was no data governance program, they weren't familiar with data governance, or they weren't sure if their jurisdiction governed the use of data.

14. Challenges

This chapter includes a list of challenges for MVAs and jurisdictions to consider and a resource list of jurisdictional best practices.

Anticipated Guidance from MDPEA Working Group

The information provided in this Interim Report is a preview of the final best practices document. It should be noted that the recommendations will be refined and further developed.

The Working Group has developed content over the course of ten months. The group has met in person three times and provided multiple opportunities for industry input, including a face-to-face meeting in August 2019 and industry/work group conference calls for each section of the best practices. More research, best practice development, and several conference calls are planned. It is anticipated the final guidance document will be published by early 2021.

Working Group Members

CHAIR

Minty Patel
Pennsylvania Driver and Vehicle Services
Manager, Driver and Vehicle Information

Members

Albert Hwang
California Department of Motor Vehicles
Chief Privacy Officer

Ann Perry
Wisconsin Division of Motor Vehicles
Director, Bureau of Driver Services

Bradford Booth
Rhode Island Division of Motor Vehicles
Deputy Chief of Legal Services

Brooklyn Wasser
Missouri Department of Revenue
Deputy Director, Motor Vehicle and Driver Licensing Division

Dominick Capotosto
Georgia Department of Revenue
Manager, Legal Affairs

Kevin Baird
Washington State Patrol
Information Security Officer

Marcy Klein
New Jersey Motor Vehicle Commission
Manager

Jeff Smith
Georgia Department of Driver Services
Information Security Officer/Acting CIO

Saundra Jack
Virginia Department of Motor Vehicles
Director Data Management Services

Joe Mandala
Kansas Bureau of Investigation
Chief Information Officer

Board Advisor

Terri Egan
New York Department of Motor Vehicles
Executive Deputy Commissioner

AAMVA Staff

Julie Knittle
AAMVA
Director, Member Services, Regions 3 & 4

Pierre Yves Boyer
AAMVA
Chief Information Security Officer

Consultant

Brad Hanscom
BerryDunn Consulting

OUR VISION

Safe drivers
Safe vehicles
Secure identities
Saving lives!

American Association of
Motor Vehicle Administrators
4401 Wilson Blvd, Suite 700
Arlington, Virginia 22203
703.522.4200 | **aamva.org**