

Subject: DATA TRUST POLICY, GUIDELINES AND PRINCIPLES

1. PURPOSE. This Order establishes the U.S. Department of Transportation (Department or DOT) policy on the use of data trusts, and identifies key roles and associated responsibilities for DOT personnel. The goals of this order are to:
 - a. Standardize the activities that DOT undertakes when considering the use of data trusts. DOT may take on different roles in a data trust, including: serving as the independent steward, creating or administering a data trust, or participating as a member of the trust.
 - b. Articulate considerations on the use of data trusts to share sensitive data in furtherance of Departmental goals.
 - c. Mitigate potential implementation problems related to governance and data protection that lead to less than optimal program outcomes when executing a data sharing arrangement through a data trust.
2. BACKGROUND
 - a. A data trust is a tool for sharing sensitive data among trust members for advancing safety or other public benefits when there might otherwise be strong disincentives or significant barriers to sharing.
 - b. Data trusts are administered by an independent steward (i.e., a trusted third party) whose duty is to take actions to protect members' data and thus encourage sharing that would otherwise not occur. The independent steward takes on a legally binding obligation to hold, protect, and analyze the members' data in accordance with the members' direction, within the data trust's governance rules and any applicable law.
 - c. Data trust members include multiple parties such as:
 - Data producers or owners;
 - Data users and analysts;
 - Member representative groups (e.g., operator or employee groups);
 - The government or other regulatory bodies; and
 - Other relevant stakeholders.
 - d. Data trusts advance the Department's mission to advance transportation safety in the public's interest by encouraging a non-regulatory approach to public-private collaboration and bringing new data sources to the Department to spur discovery and innovation.
 - e. The Department has operated data trusts in support of aviation safety through the

Aviation Safety Information Analysis and Sharing program.

- f. The Department has funded additional external data trust activities—notably the Partnership for Analytics in Traffic Safety and the Rail Information Sharing Environment.
- g. The Department has also served in the role of independent steward. The Bureau of Transportation Statistics² has performed the independent steward role, including maintaining the SafeOCS Reporting System³ for the offshore oil and gas drilling industry and the Close Call Reporting program for the Washington Metropolitan Transit Authority (WMATA). Other confidential reporting programs operated by the Department may exhibit the characteristics of data trusts (e.g., Aviation Safety Reporting System and Confidential Close Calls Reporting System), but are narrower in scope and not considered data trusts.
- h. An interdisciplinary team with different competencies is needed for data trusts to work well. Such a team will typically include representation from program, policy, data and analytics, legal, cybersecurity, and information technology subject matter experts.

3. REFERENCES

- a. 49 U.S.C. § 301, Duties of the Secretary of Transportation: Leadership, consultation, and cooperation.
- b. Departmental Data Management Policy, DOT Order 1351.34, July 14, 2017.

4. DEFINITIONS

- a. Data trust: a voluntary and collaborative arrangement that uses independent stewardship via a third party to secure, share, and use sensitive data.
- b. Independent steward: a trusted third party that holds and protects sensitive data voluntarily submitted by the members of the data trust. An independent steward may be a government agency, a private company, a private research center, or other trusted entity acceptable by data trust members.

5. POLICY

- a. Data trusts should operate on a shared, clear purpose.

² As a principal Federal statistical agency, the Bureau of Transportation Statistics has unique authority to invoke the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) and provide strong data disclosure protection for information collected for statistical purposes. CIPSEA was enacted as Title V of the E-Government Act of 2002 and subsequently codified and revised by Title III of the Foundations for Evidence-Based Policymaking Act of 2018 (PL 115-435; January 14, 2019; codified at 44 USC Chapter 35, Subchapter III).

³ The SafeOCS Reporting System contains a mix of mandatory and voluntary reporting. The Bureau of Transportation Statistics role in the data trust applies only to the voluntary reporting elements. For further information, see: <https://www.safeocs.gov/about.htm>

- 1) DOT should ensure the purpose and public benefits of a given data trust are clearly detailed, documented and communicated from the outset.
 - 2) DOT should ensure that data trusts improve the Department's ability to gain new information in the pursuit of its mission and strategic goals.
 - 3) DOT should ensure the types of data that members will be expected to share are clearly linked to the purpose of the data trust.
 - 4) Because the purpose of a data trust may evolve over time, DOT should ensure that data trusts provide for periodic reviews and updates of their purpose to maximize the benefits of the data trust to DOT and its members.
- b. Data trusts should establish a program structure.
- 1) DOT should ensure that data trusts have a charter or equivalent document that specifies the purpose of the data trust, including the safety, operational, and policy issues the data trust will address.
 - 2) DOT should ensure that a data trust's charter or related governing documents⁴ provide for core operating mechanisms to be established. Core operating mechanisms include, but are not limited to, membership, governance and decision-making approaches, and the role of the independent steward in the data trust.
 - 3) DOT should ensure that a data trust's charter and related governing documents define clear roles and responsibilities.
 - 4) DOT should ensure that data trusts define member data rights through data sharing agreements or equivalent documents. Such agreements should outline withdrawal considerations.
 - 5) DOT should ensure that the structure of the data trust, including expectations about sharing specific types of data, conforms with all applicable legal requirements throughout the lifecycle of the trust. Applicable legal requirements include, but are not limited to, Federal information disclosure laws, privacy and confidentiality laws, and anti-trust laws.⁵
 - 6) When DOT is involved as an independent steward in the formation and ongoing

⁴ Related governing documents can include, but are not limited to, data sharing agreements between the independent steward and data trust members, related data handling procedures (e.g. deidentification protocols), standard operating procedures for how the data trust makes decisions about members joining or departing. The governing documents should cover a member's full lifecycle in the data trust.

⁵ Applicable legal requirements may change over time, as data flowing into the trust may change as study topics and use cases change, in accordance with data trust governance rules. DOT Counsel must be consulted in the creation of a data trust and on any legal issues.

operation of a data trust, careful consideration should be given to the legal authority⁶ used to form the data trust and to ensure it operates consistent with applicable Federal laws. In the cases where DOT is the independent steward, the responsibilities outlined for the independent steward apply to the appropriate DOT program office.

- c. Data trusts should clearly articulate how to execute data trust operations and decision-making processes.
 - 1) In establishing procedures for the operation of a data trust, DOT should strive to ensure governance and decision-making processes are open and transparent.
 - 2) DOT should maximize the use of members' consensus in data trust operation procedures. Furthermore, DOT should ensure the data trust has a party responsible for both implementing any needed decision-making processes for the data trust, and for ensuring decisions are appropriately documented. Data trusts should clearly delineate which decisions are made by members of the trust and which are made by the independent steward, in accordance with the data trust's governance rules.
 - 3) DOT should ensure that boards and committees that organize data trust members and stewards to work on decision items⁷ carefully document procedures for selecting and vetting members, in accordance with the data trust's governance rules. DOT should also ensure that the data trust sets clear expectations on the contributions of those members to the decision-making process within the data trust.
 - 4) DOT should periodically evaluate the efficacy of the charter and decision-making processes that form the foundation of the data trust.
- d. Data trusts should transparently address the allowable uses of data.
 - 1) DOT should ensure that data trust governance documentation clearly identifies and enumerates allowable uses of the data and results by its members, and external users if applicable.
 - 2) DOT should ensure the data trust provides each member with the ability to identify its own sensitive data, and to establish appropriate limitations on the use of its data, in accordance with the data trust's governance rules and applicable law. DOT should ensure that the data trust provides members and stewards mechanisms to continuously evaluate the risks of data sharing and what mitigation may be necessary.
 - 3) DOT should ensure that any limitations on allowable uses of data are transparent to members of the data trust and the public.
 - 4) DOT should ensure that data trust governance addresses rights in work products

⁶ DOT Counsel should be consulted for applicable legal authorities, which may be found in Operating Administration's authorizing statutes and may include, but are not limited to, safety and research authorities, as well as data confidentiality requirements.

⁷Any board or committee that is created should be established in accordance with applicable law.

produced from the use of members' data, maximizing the dissemination of the knowledge gained in support of the data trust's purpose.

- 5) DOT should ensure that a data trust's governance documents are cognizant of the statutory and regulatory scheme applicable to data trust members and stewards, and tailor allowable uses accordingly.
 - 6) If DOT provides data to the data trust (*i.e.*, in cases where DOT is a member and not an independent steward), DOT must ensure all legal requirements regarding the data are met and that providing such data does not diminish the Department's ability to act based on DOT data. DOT should make clear that membership in the data trust does not create immunity from civil or criminal liability for violations of Federal law or from private causes of action.
 - 7) DOT should ensure that the data trust has mechanisms in place to apprise members of any data usage resulting from the data trust, except where such appraisal would interfere with an investigation or enforcement action.
- e. Data trusts should implement appropriate data protections.
- 1) DOT should ensure that the structure of a data trust is predicated on the members' requirements for safeguarding, protecting, retaining, and handling of their data.
 - 2) DOT should ensure that data trust members expressly permit use of their data in accordance with the data trust's governance rules and applicable law. DOT should ensure the data trust has mechanisms for members to grant such permissions to the data trust using a data sharing agreement or equivalent document. Such agreements should cover the member's full involvement in the data trust from start to end.
 - 3) DOT should ensure that the data trust has mechanisms in place to demonstrate to members that technical protections and security protocols have been applied to members' data and that those protections are continuously evaluated for efficacy.
 - 4) DOT should ensure that data trusts do not protect data from disclosure that was readily available to the Government before a data trust is formed or restrict data disclosure in a manner that is inconsistent with the Federal Freedom of Information Act.⁸ Likewise, DOT should ensure data trusts do not affect the Department's regulatory, inspection, and enforcement authorities.⁹
- f. Delineating Departmental responsibilities in the acquisition of a data trust.

⁸ When dealing with data disclosures, it is important to remember that each State has different public records laws, which may also significantly differ from the Federal Freedom of Information Act (FOIA). When DOT is proposed as the independent steward, other protections regarding releasability of data may be applicable, such as the CIPSEA (see footnote 3), or regulations regarding the protection of human subjects (49 CFR Part 11).

⁹ Depending on the entity that assumes the independent stewardship role, its ability to limit liability and/or indemnify members may not be possible.

- 1) DOT should manage data trust activities consistent with other related Departmental programs, and data trust activities should complement existing activities.
- 2) DOT should ensure that inherently governmental decisions, such as obligating Federal funding, are accounted for in the formation and operation of a data trust.
- 3) DOT should ensure data trust activities are adequately resourced. Whether DOT funds the independent steward activities partially or completely, DOT must assess the data trust's commitment to funding the independent data steward.
- 4) When DOT is involved in creating or administering a data trust, DOT should establish the process for selecting the trusted independent steward, consistent with applicable law.¹⁰
- 5) When DOT is involved in creating or administering a data trust, DOT should work from the outset to ensure that the relationship with the independent steward is portable and severable, should the need arise.
- 6) When DOT is involved in creating or administering a data trust, DOT should continually monitor the independent steward to hold the steward accountable and ensure the data trust's good performance and reasonable costs. DOT officials should ensure that they can make reasonable changes, including replacement of the entity serving as the independent steward.
- 7) DOT should consider key questions regarding intellectual property rights surrounding the data and information technology infrastructure as well as appropriate rights to the analytical products of the data trust. DOT should expressly consider the implications of making the information technology infrastructure and analytical products inaccessible and the impact on data trust members, in accordance with data trust governance rules.
- 8) DOT should ensure that data trusts have mechanisms to evaluate cost-sharing and resource burden among themselves.

6. RESPONSIBILITIES

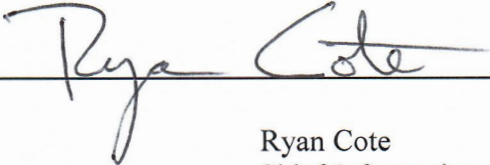
- a. The Assistant Secretary for Transportation Policy (OST-P): Establishes and oversees overall surface transportation policy initiatives, coordinating multi-modal initiatives and processes, including those related to data trusts established by DOT.
- b. The Office of the Chief Information Officer (OST S80): Serves as the principal information technology (IT) advisor to the Secretary and DOT Operating Administrations (OAs), including for enterprise data management¹¹.

¹⁰ For instance, the Federal Advisory Committee Act of 1972 (Pub. L. 92-463; 5 U.S.C. App. 2).

).

¹¹ To the extent the policy, herein, is consistent with 49 U.S.C. 106.

- c. The Chief Data Officer (OST S85): Manages the DOT's data program, including oversight over data policy and related systems. The Chief Data Officer has primary responsibility for overseeing the implementation of this policy and is responsible for promulgating and maintaining this Order, updating as needed.
 - d. Secretarial Offices and OAs: Ensure the Department's policy, guidelines and principles for data trusts are upheld, and are responsible for developing internal guidance and controls to support a well-managed data trust program. OAs may issue OA-specific guidance or procedures to adapt and tailor this guidance to their unique data trust initiatives or data trust needs not specifically addressed by this Order.
 - e. General Counsel (OST-C) and OA Chief Counsels: Responsible for reviewing specific authorities and applicable legal requirements for a contemplated data trust.
7. IMPLEMENTATION. Any further guidance or standard operating procedures (SOP) issued by DOT OAs to implement the provisions of this Order pertaining to the creation of or participation in a data trust must be forwarded to the Chief Data Officer for initial review and periodic evaluation.



Ryan Cote
Chief Information Officer