ITS AMERICA

ITS America Privacy Principles

202.484.4847

www.itsa.org | info@itsa.org

1100 New Jersey SE Suite 850, Washington DC 20003

March 2025

Privacy Principles

Introduction

The Intelligent Transportation Society of America (ITS America) is committed to protecting data privacy. Our transportation systems today rely on a backbone of data and technology to keep people and goods moving safely and efficiently. While a critical infrastructure sector like transportation benefits from technology and innovation to optimize safety and mobility, maintaining data privacy is essential to ensure consumer protections, foster public trust in solutions, and maintain the security of our transportation networks.

As the transportation system continues to evolve, balancing innovation with privacy is crucial. While large-scale data collection, processing, and analysis drive advancements in fields like artificial intelligence and machine learning, organizations that follow data privacy best practices ensure these activities respect individual privacy, allowing innovation to thrive ethically and responsibly. A shared understanding of privacy also fosters global competitiveness and interoperability. Finally, organizations that demonstrate a commitment to privacy are more likely to create buy-in and trust from those that they are looking to serve—communities, partners, and stakeholders who value data protection and transparency.

ITS America has developed this comprehensive set of privacy principles and recommended next steps to guide the development, deployment, and regulation of advanced technologies in surface transportation. This guidance will help organizations and governments balance the benefits of technology with the need to protect individuals' privacy and is meant to apply to organizations in both the private and public sector, including infrastructure owner operators (IOOs).

The principles focus on the following core tenets: protecting personal information, building trust, improving responsible data usage and governance, meeting consumers where they are, and evolving organization policies to adapt to new technologies.

1. Protecting Personal Information

Protecting personal information is a cornerstone of consumer privacy. Individuals have the right to know what data is being collected about them, how it is used, and with whom it is shared. Data collection and use should be aligned with the organizational purpose for which it was collected, and the kinds of personal information collected should be disclosed to the individual. By limiting data collection and use only to what aligns with organizational goals, organizations reduce the risk of misuse and protect user privacy by ensuring that unnecessary personal information is not collected or stored.

2. Building Trust Through Transparency and Accountability

Establishing and maintaining trust is essential for fostering positive relationships between individuals, organizations, and governments. When people trust that their data is handled responsibly, they are more likely to engage with services and share information, which is particularly important in enhancing safety

and mobility. Organizations should publicly disclose their data practices including rationales for use, not only to promote transparency, but also to ensure accountability, helping to prevent unethical practices and potential misuse of personal information.

3. Supporting Ethical and Responsible Use of Data

The ethical and responsible use of data is the foundation for data privacy. It ensures individuals' rights are respected, fostering trust and protecting sensitive information from potential misuse. As organizations increasingly rely on data to improve decision-making processes, drive innovation, and keep people safe, the use of any new data sources should be grounded in ethical business practices. Data should not be used in a way that leads to discriminatory practices and should be used in ways that are fair and just for all populations.

4. Improving Data Governance

Clear policies should be established for managing data across its lifecycle—from collection to disposal. Data governance is important because it helps organizations manage and use data in a way that is secure and reliable. Good data governance should improve operational efficiency and aid in compliance with regulations. Data governance often includes guidelines for accountability and review, ensuring that individuals have the means to challenge inappropriate data use and seek remedies. This reinforces an organization's responsibility to act in good faith when managing personal information.

5. Meeting and Anticipating Consumer Expectations

Organizations should acknowledge growing consumer expectations for privacy by enhancing protection of personal data, giving consumers more control over their information, improving user experiences, and ensuring their preferences are honored. Data collection processes should be aligned with consumer expectations, and those who collect and use data should be responsive to consumer inquiries ensuring a clear channel of communication between parties. With this clear communication comes trust and confidence that data is being used and stored responsibly and ethically.

6. Adapting to the Evolving Technological Landscape

Technology is constantly evolving, and privacy protections should be a foundational framework that can adapt to new and emerging tools, including privacy-enhancing technologies. Organizations should acknowledge the ever-changing nature of technology and ensure that data privacy protections are adaptable and able to meet these changes. With new technologies come new challenges related to privacy, and organizations must continually update and audit their privacy practices to ensure strong consumer protection and regulatory compliance

Recommended Next Steps for Organizations

- Establish a data governance framework that includes accountability, compliance, regular audits, employee training, consumer education, and a robust incident response plan.
- Develop and maintain policies that limit data collection to only what is necessary for to achieve an organization's stated goals. Regularly review data collection practices to reduce the risk of misuse. This ensures that data handling aligns with ethical guidelines and is purposeful.
- Establish comprehensive privacy policies that are easily accessible and understandable to promote transparency and build trust by ensuring individuals are well-informed about data practices.
- Implement robust consent management systems that allow individuals to easily give, withdraw, or modify their consent for data processing activities.
- Conduct regular privacy audits and assessments to ensure compliance with privacy policies and regulations, maintain accountability and prevent unethical practices through continuous monitoring and improvement.
- Incorporate privacy considerations into the design of new products and services, ensuring default settings prioritize user privacy.
- Periodically evaluate and update privacy policies to stay current with technological and regulatory changes.