



ARTICLE

Privacy and data literacy are key considerations for agencies' generative artificial intelligence rollouts. The goal of a data literacy program is for decision makers to understand the power of data, the value of data, and the importance of that data management, governance, and protection.

This potential cannot be realized without the readiness of the data government programs hold, and AI models are only as good as the data fed into them. Data readiness is the foundation upon which successful data-driven initiatives and AI solutions are built. It encompasses a range of factors including data quality and governance, data security, and data infrastructure.

Agencies need to aggregate data from multiple systems and ensure it is of superior quality. This is essential to fulfilling the potential of augmented government, automating administrative processes intelligently, and facilitating better decisions for citizens.



To instill public confidence, however, organizations must also abide by a set of shared standards and values in using AI. Establishing clear policies, controls, and standards including roles and responsibilities for data management, can ensure that data is used ethically and responsibly, while also helping agencies comply with regulations and safeguards privacy.



Model trust needs data trust. It is critical to ensure organizations are creating quality data inputs for trustworthy AI solutions.



Agencies should conduct data assessments and identify strengths and weaknesses in their data readiness and management so they can formulate tailored strategies to improve data quality, governance, and security.





Bias, security, accessibility, and constitutional protections are paramount in importance.



Information and Data Officers need to ensure that their agency is taking an approach that protects against data-use risks, driving quality, trust, privacy, and security.



This means developing and investing in a robust data transformation strategy that includes optimizing data extraction, standardization, storage, and access to create a unified, precise, and trustworthy data source.



With agencies ingesting and managing growing amounts of data, it is critical that their technology providers maintain exceptional data privacy and security controls and deploy encryption and security frameworks, to protect citizens and agencies against emerging AI threats.

Garbage In, Garbage Out: Why Third-Party Data Sources Matter When Using AI

Al has emerged as a potent tool across various domains, from content creation to bolstering decision support systems. The efficacy of generative Al is intrinsically tied to the quality of its training data.

And therein lies the challenge, aptly summarized by the adage, "Garbage in, garbage out." For that reason alone, it pays to understand how any third-party data you use has been aggregated and enriched before you feed it into your Al applications.

The domino effect of poor-quality data

As digital transformation and use of AI accelerates, the implications of low-quality data can turn the potential of AI from promising to perilous in an instant. From misguiding algorithms to yielding impractical results, choosing the wrong third-party data provider can lead to a cascade of unintended consequences.



Perpetuating Biases: Poor quality data, especially data marred by inherent biases, gives AI a skewed perspective. Consequently, the AI may generate content that not only reinforces harmful biases but also alienates citizens and harms trust among constituents and other government agencies.



Reputation Under Fire: When AI produces content that is inaccurate, biased, or otherwise misaligned with reality or societal norms, your organizations could wind up in the crosshairs of public scrutiny and reputational damage.



Misinformation Proliferation: All is currently devoid of discernment, making it easy to perpetuate misinformation, eroding trust in the technology and the agency and/or organization using it. Giving access to a large amount of quality data creates a broad foundation on which the Al can cross-reference and validate data, acting as a buffer against misinformation.



Strategic Derailment: Misleading or incomplete data can cause the Al to generate insights or content that pushes strategic planning astray, fostering decisions that misalign with realities and mission goals.



Impaired Citizen Interactions: Lack of relevant and accurate data might lead the AI to produce content or responses that miss the mark in constituent interactions, souring relationships, and diminishing user experience.



Wasted Resources: Inaccurate or irrelevant data may misguide Al-powered automated processes, leading to misallocated resources, squandered opportunities, and ultimately financial losses.



Inhibited Innovation: If the data AI ingests is not timely or relevant, the outputs will likewise present an inadequate picture of diverse and current trends, leading to stagnation and a lack innovation that hampers your agency's ability to stay forward-thinking.

Each of the above risks underscores the importance of selecting third-party data sources you intend to fuel AI. They should undergo robust vetting and ongoing monitoring to safeguard against these potential problems.

What to look for in third-party data

The journey from selecting to consuming data is nuanced, demanding a meticulous understanding of what you need from the data. Navigating it requires you to verify that you source data that offers relevance, volume, and quality that aligns with your objectives for AI.



Reliable Sources: Ingesting data from a wide range of reputable sources helps safeguard the AI from internalizing and propagating errors or narrow perspectives.



Abundant Volume: Vast pools of historical and current data to support backwards-looking as well as future-focused analysis.



Enrichments to Enhance Useability: Facilitating smooth data ingestion and incisive insights extraction are pivotal in today's data-abundant ecosystem. Topic tags, industry tags, sentiment, and other metadata amplifies its usability and relevance.

By choosing an experienced data aggregator and provider, you get the transparency, volume, variety, and value you need from the third-party data you ingest.



Anchor trust by using a proven third-party data science provider

Aligning with a proficient third-party data provider can pivot your AI towards a trajectory defined by accuracy, relevancy, and insightful data generation. Here, the credibility of a trusted and responsible provider becomes paramount, especially one that not only brings to the table a profound depth and breadth in its data sources, but also adheres to a rigorous process of crafting semi-structured, enriched data.

Look to harness a rich tapestry of third-party data on both businesses and individuals (Deceased—not just Death Master File, Best Name, Address, Date of Birth (DOB), Social Security Number (SSN), Relatives and Associates, Mailing Contacts/Address Verification, Bank Account Ownership Verification, Financial Information (Collections/ Liens/Bankruptcy), De-identified Referential Data—without exchanging personally identifiable information (PII), Device Intelligence, Vital Records, and more)—spanning across various regions and agency types.

The caliber of AI is a direct reflection of the quality, volume, and variety of data it is nurtured on. Ensuring that the data you ingest is well-structured, enriched, and insightful paves the way towards unleashing the true potential of AI.

Turn to a trusted leader in data aggregation and delivery.



Strategic Identity Data Management for Optimized AI Use

Agencies can benefit from collaborating with data solutions providers and scientists, like LexisNexis® Risk Solutions, to manage identity data effectively within their Al ecosystems. A scalable and agile data infrastructure that supports Al-driven analytics is crucial for handling extensive datasets, and for delivering precise, Al-driven analytics.

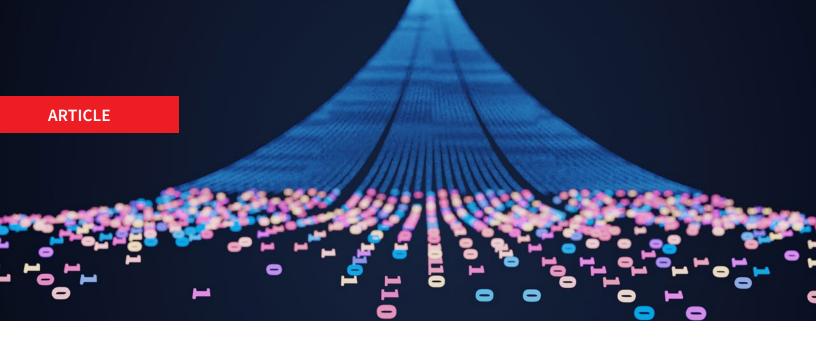


Working with Data Solutions Providers for Enhanced Identity Management

Agencies can benefit from collaborating with data solutions providers to manage identity data effectively within their AI ecosystems.

A scalable and agile data infrastructure that supports AI-driven analytics is crucial for handling extensive datasets, and for delivering precise, AI-driven analytics.





We Can Guide the Way

For over a decade, responsible AI and machine learning have been integrated into LexisNexis® Risk Solutions and plays a crucial role in helping us drive innovation and enhance our products and services. Together with our parent company, RELX, we remain committed to the ethical and responsible use of AI technology, which includes protecting the privacy and security of our systems and data while working to eliminate bias. Trustworthy and transparent identity data management requires an enterprise-wide focus on data quality, as well as responsible and vigilant AI practices. Our solutions can assist agencies with managing and maintaining quality identity data for successful AI adoption and deployment. We can also help agencies mitigate evolving AI threats while providing a reduced risk experience.

For more information or assistance, scan the QR code or call 1-888-216-3544.





About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com, and www.relx.com.