DUE DILIGENCE OF POTENTIAL VENDORS-PROCESSORS:

Procurement Guide for AI Systems

Considerations when procuring third party software with AI features

✓ Develop criteria (in collaboration with procurement and enterprise risk management teams) to assess and approve new or updated third-party software and services that integrate with AI APIs or offer AI features:

→ Have internal reviewers consider the data sets used to create the outputs (e.g., for generative AI models) to determine the unique risks associated with each software and service.

→ Review outputs for explainability, fairness, and bias — do the outputs make sense based on the inputs, are the outputs fair and nondiscriminatory?

→ Assess the terms of use and system documentation of the third party vendor — are they sufficiently transparent about the AI features?

✓ Establish requirements for sharing data with vendors that ensure compliance with relevant laws, regulations, and best practices for sharing or the sale of data to third parties:

→ Minimize the sharing of personal data as part of data sets used to train third party AI systems.

✓ Review contractual terms to ensure that any uses of data by vendors reflect mandatory regulatory contractual language, or are subject to approved exceptions:

→ As required by local law, ensure the appropriate notices and consent are obtained prior to sharing personal data with vendors.

→ Ensure vendors are able to comply with individual requests regarding the use of their personal data in systems using AI (e.g., Do Not Sell requests under US state laws, access and deletion requests).

✓ Put in place contingency processes to handle failures or incidents in third-party data or AI systems deemed to be high-risk:

→ Ensure the AI system can fail safely, such as when made to operate beyond its knowledge limits, and that residual negative risks do not exceed the business's risk tolerance.

Do your regulatory research — better yet, let us do it.

Spending hours online searching and understanding privacy regulatory changes is time-consuming. Nymity Research does it for you, keeping you on top of the latest laws, regulations, standards, and operational best practices around privacy, across a multitude of jurisdictions.

TrustArc

Start your free trial