Collibra

Must know terms for AI governance

Key concepts for more reliable, traceable, compliant AI

RELIABLE

Data Quality:

Data quality determines if data is fit for use to deliver high quality AI model outputs. Data is considered high quality based on consistency, uniqueness, completeness and validity.

Validation Data:

A portion of a dataset that is not used to train an AI model but rather measure performance of an AI model during training.

Training Data:

A portion of a dataset that is used to train an AI model until it can proficiently predict results or uncover patterns.

Fine-tuning:

Fine-tuning is the process of adjusting and optimizing a pre-trained large language model on a specific dataset, set of questions and answers, or tasking to improve its performance.

TRACEABLE

Explainability:

The ability to detail outputs of AI Models, ensuring they are understood, to the best of their ability, by technical and non-technical audiences alike.

Accountability:

Clearly defined roles and responsibilities for all stakeholders involved in the AI lifecycle, including developers, data scientists, business users, legal and privacy professionals, to report, explain, or justify AI model output.

Transparency:

Ensuring that AI models, including algorithms and decision-making processes, are open and understandable to relevant stakeholders, such as developers, data scientists, business users, legal and privacy professionals.

Trustworthy AI:

Often used interchangeably with Ethical AI, Trustworthy AI is the development of AI models that are reliable, ethical, and can be trusted by users.

COMPLIANT

Regulatory Compliance:

Ensuring that AI models adhere to relevant laws and regulations including data protection laws, anti-discrimination laws and industry-specific regulations like HIPAA.

EU AI Act:

European Union law that provides AI developers with clear requirements and obligations regarding specific uses of AI.

Model Ops:

A collection of tools, technologies, and best practices to build, deploy, monitor and manage machine learning and AI models. It is the key capability for scaling and governing AI at the enterprise level.

Privacy:

Ensuring data used in AI is handled in accordance with all applicable data privacy laws and regulations to prevent unauthorized access, use, or disclosure of sensitive information.

AI Governance:

AI governance is the application of rules, processes, and responsibilities to drive maximum value from your automated data products by ensuring applicable, streamlined, and ethical AI practices that mitigate risk, adhere to legal requirements, and protect privacy.