

Privacy & LLM Alignment Workshop

Workshop | 1 Tag | vorzugsweise vor Ort

LLM-basierte Systeme verarbeiten Daten auf grundlegend andere Weise als herkömmliche Software – wodurch blinde Flecken zwischen Rechts-, Datenschutz- und Engineering-Teams entstehen. Dieser Workshop schafft das gemeinsame Verständnis, das erforderlich ist, um von Anfang an konforme KI-Systeme zu entwickeln.

Rechts- und Datenschutzteams haben Schwierigkeiten, Datenschutzrisiken in LLM-Systemen zu bewerten, da sie die technischen Datenflüsse nicht verstehen. Technikteams entwickeln Lösungen, ohne die rechtlichen Auswirkungen der Verarbeitung personenbezogener Daten in KI-Pipelines vollständig zu verstehen. Diese Diskrepanz führt zu Compliance-Verstößen, Projektverzögerungen und kostspieligen Neugestaltungen.

Dieser kollaborative Workshop bringt die wichtigsten Stakeholder zusammen, um Datenflüsse in LLM-basierten Systemen systematisch abzubilden, Datenschutzrisiken zu identifizieren und geeignete Kontrollen zu definieren. Durch praktische Übungen und reale Szenarien schaffen wir ein gemeinsames mentales Modell davon, wie personenbezogene Daten durch KI-Systeme fließen und was das für die Compliance bedeutet. Am Ende haben Sie ein einheitliches Verständnis, dokumentierte Risiken und konkrete Strategien zur Risikominderung.

Setup

Zielunternehmen	Alle
Reifegrad	Noch nicht begonnen, Experimentierphase, bereits Praxiserfahrung
Teilnehmer	Datenschutzbeauftragte, Rechtsberater, KI-/ML-Ingenieure, Produktverantwortliche
iteratec	KI-Architekt
Voraussetzungen	Beschreibung geplanter/bestehender LLM-Anwendungsfälle, grundlegende Architekturdokumentation, Verfügbarkeit sowohl technischer als auch rechtlicher Stakeholder

Agenda

- LLM-Grundlagen für nicht-technische Stakeholder**
Verständliche Erklärung, wie LLMs Daten verarbeiten, einschließlich Training, Feinabstimmung und Inferenz
- Übung zum Datenfluss-Mapping**
Gemeinsame Visualisierung der personenbezogenen Datenflüsse in Ihren LLM-Anwendungsfällen von Anfang bis Ende
- Identifizierung von Datenschutzrisiken**
Systematische Analyse der DSGVO-/Datenschutzrisiken in jeder Phase des Datenflusses
- Definition und Priorisierung von Kontrollen**
Entwicklung technischer und organisatorischer Maßnahmen zur Minderung identifizierter Risiken
- Funktionsübergreifende Abstimmung**
Vereinbarung über Verantwortlichkeiten, Entscheidungskriterien und laufende Kooperationsprozesse

Ergebnisse

- **Gemeinsames technisches und rechtliches Verständnis**
Gemeinsame Sprache und gemeinsames Denkmodell, die es den Teams aus den Bereichen Recht, Datenschutz und Technik ermöglichen, effektiv über LLM-Datenschutzrisiken zu kommunizieren
- **Transparenz des Datenflusses**
Visuelle Dokumentation des Flusses personenbezogener Daten durch Ihre LLM-Systeme, von der Eingabe über die Verarbeitung bis hin zur Speicherung und Weitergabe an Dritte
- **Risikokontrollmatrix**
Systematische Zuordnung von Datenschutzrisiken zu bestimmten Datenflüssen mit priorisierten technischen und organisatorischen Kontrollen

Ergebnisse

- ✓ **Datenschutz-Risikomatrix**, in der identifizierte Risiken, deren Schweregrad und betroffene Datenflüsse dokumentiert sind
- ✓ **Kontrollkatalog** mit priorisierten technischen und organisatorischen Maßnahmen, die bestimmten Risiken zugeordnet sind
- ✓ **Kooperationsrahmenwerk**, das die laufende Koordination zwischen den Bereichen Recht, Datenschutz und Technik definiert

Privacy & LLM Alignment Workshop

Workshop | 1 day | on-site preferred

LLM-based systems process data in fundamentally different ways than traditional software – creating blind spots between Legal, Data Protection, and Engineering teams. This workshop creates the shared understanding needed to build compliant AI systems from the start.

Legal and Data Protection teams struggle to assess privacy risks in LLM systems because they don't understand the technical data flows. Engineering teams build solutions without fully grasping the legal implications of how personal data moves through AI pipelines. A disconnect that leads to compliance violations, project delays, and costly redesigns.

This collaborative workshop brings the critical stakeholders together to systematically map data flows in LLM-based systems, identify privacy risks, and define appropriate controls. Through hands-on exercises and real-world scenarios, we create a shared mental model of how personal data flows through AI systems and what that means for compliance. You leave with aligned understanding, documented risks, and concrete mitigation strategies.

Setup

Target Companies	All
Maturity Level	Not Started, Experimenter, Practitioner
Participants	Data Protection Officers, Legal Counsel, AI/ML Engineers, Product Owners
iteratec	AI Architect
Prerequisites	Description of planned/ existing LLM use cases, basic architecture documentation, availability of both technical and legal stakeholders

Agenda

- 1. LLM Fundamentals for Non-Technical Stakeholders**
Accessible explanation of how LLMs process data, including training, fine-tuning, and inference
- 2. Data Flow Mapping Exercise**
Collaborative visualization of personal data flows in your LLM use cases from end to end
- 3. Privacy Risk Identification**
Systematic analysis of GDPR/privacy risks at each stage of the data flow
- 4. Control Definition & Prioritization**
Development of technical and organizational measures to mitigate identified risks
- 5. Cross-Functional Alignment**
Agreement on responsibilities, decision criteria, and ongoing collaboration processes

Achievements

- **Shared Technical-Legal Understanding** Common language and mental model enabling Legal, Data Protection, and Engineering teams to communicate effectively about LLM privacy risks
- **Data Flow Transparency** Visual documentation of how personal data moves through your LLM systems, from input to processing to storage and third-party sharing
- **Risk-Control Matrix** Systematic mapping of privacy risks to specific data flows with prioritized technical and organizational controls

Deliverables

- ✓ **Privacy Risk Matrix** documenting identified risks, their severity, and affected data flows
- ✓ **Control Catalog** with prioritized technical and organizational measures mapped to specific risks
- ✓ **Collaboration Framework** defining ongoing coordination between Legal, Data Protection, and Engineering