Mittelstand-Digital Zentrum Rostock

KI-Anwendungen datenschutzkonform einsetzen – So gelingt es

KURZ UND KNAPP

WORUM GEHT'S?

Der Schutz der Privatsphäre von Individuen ist essenziell, um Vertrauen in Systeme der Künstlichen Intelligenz (KI) zu schaffen. Da KI-Anwendungen häufig große Mengen personenbezogener Daten verarbeiten, bergen sie Risiken, wie Missbrauch, Diskriminierung oder Identitätsdiebstahl. Deshalb ist der sorgfältige Umgang mit sensiblen Informationen nicht nur eine rechtliche Verpflichtung, sondern auch ein ethisches Gebot, um faire und transparente Technologien zu gewährleisten.

Grundprinzipien der Datenverarbeitung

Bei der Nutzung von Daten in KI-Anwendungen müssen folgende Grundsätze eingehalten werden:

- **Zweckbindung**:
  Daten dürfen nur für klar definierte und rechtmäßige Zwecke verwendet werden.
- **Datenminimierung**:
  Es dürfen nur die Daten erhoben werden, die für den vorgesehenen Zweck unbedingt notwendig sind.
- **Transparenz**:
  Nutzer müssen klar und verständlich darüber informiert werden, wie ihre Daten verwendet werden, einschließlich einer Erklärung der Funktionsweise der KI-Systeme.

Spezielle Anforderungen bei sensiblen Daten

Besondere Vorsicht gilt bei sensiblen Daten, wie Gesundheits-, Finanz- oder biometrischen Informationen, da sie ein hohes Risiko für Missbrauch bergen. Um diese Daten sicher zu verarbeiten, sollten folgende Punkte beachtet werden:

- **Rechtliche Grundlage**:
  Für die Verarbeitung dieser Daten ist oft eine explizite Einwilligung erforderlich.
- **Hohe Sicherheitsstandards**:
  Verschlüsselung und Zugriffsbeschränkungen sind Pflicht.
- **Erhöhte Transparenz**:
  Nutzer müssen genau wissen, wie und warum ihre sensiblen Daten verwendet werden.

Ein datenschutzfreundlicher Umgang mit sensiblen Informationen ist essenziell, um Risiken wie Diskriminierung und Identitätsdiebstahl zu vermeiden.

Abgrenzung zwischen zulässigen und problematischen Anwendungen

Zulässige KI-Anwendungen zeichnen sich durch Datenschutzfreundlichkeit aus, indem sie die Vorgaben der Datenschutz-Grundverordnung (DSGVO) einhalten und die Rechte der Nutzer respektieren. Problematisch hingegen sind Anwendungen, bei denen:

- Daten ohne die erforderliche Einwilligung oder eine legitime rechtliche Grundlage verarbeitet werden
- diskriminierende Entscheidungen durch KI-Systeme getroffen werden, etwa bei Kreditvergaben oder Bewerbungsverfahren
- Algorithmen Entscheidungen auf undurchsichtige Weise treffen, ohne nachvollziehbare Begründungen zu liefern

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital Zentrum Rostock

KI-Anwendungen datenschutzkonform einsetzen – So gelingt es

Grundsätze für den datenschutzkonformen Einsatz

- **Rechtliche Grundlagen prüfen**:
  Ist die Verarbeitung durch Einwilligung oder andere DSGVO-Vorgaben gedeckt?
- **Daten minimal und gezielt nutzen**:
  Werden nur notwendige Daten für klar definierte Zwecke verwendet?
- **Transparenz sicherstellen:**
  Sind Nutzer über Datenverarbeitung und KI-Entscheidungen informiert?
- **Technische Schutzmaßnahmen implementieren:**
  Sind Anonymisierung, Verschlüsselung und Zugriffskontrollen aktiv?
- **Bias und Diskriminierung vermeiden:**
  Wurde der Algorithmus auf Verzerrungen geprüft?
- **Datenschutzfreundliche Gestaltung (Privacy-by-Design):**
  Wurde Datenschutz von Anfang an integriert?
- **Sensible Daten besonders schützen:**
  Werden sensible Daten wie Gesundheitsdaten sicher verarbeitet und ausreichend geschützt?
- **Externe Partner einbeziehen**:
  Sind alle externen Dienstleister datenschutzkonform und vertraglich gebunden?
- **Prozesse dokumentieren und überprüfen**:
  Ist die Datenverarbeitung vollständig dokumentiert und regelmäßig überprüft?
- **Nutzerrechte respektieren**:
  Können Nutzer ihre Rechte, z. B. auf Auskunft und Löschung, einfach wahrnehmen?

Beispiele für KI-Anwendungen

- **Medizinische Diagnosesysteme**:
  KI kann anonymisierte Patientendaten analysieren, um Krankheiten frühzeitig zu erkennen. Individuell passende Behandlungspläne können so datenschutzkonform erstellt werden. Um die Privatsphäre zu gewährleisten, werden strenge Sicherheitsmaßnahmen und klare Einwilligungen der Patienten beachtet.
- **Kundenanalyse**:
  KI-gestützte Kundenanalyse ermöglicht Unternehmen, die Bedürfnisse und Vorlieben ihrer Kunden besser zu verstehen, um personalisierte Services und Angebote zu entwickeln. Dabei können Daten, wie Kaufverhalten oder Feedback, analysiert werden, jedoch stets unter Beachtung datenschutzrechtlicher Vorgaben. Anonymisierung und Pseudonymisierung der Daten stellen sicher, dass die Privatsphäre gewahrt bleibt.
- **Chatbots**:
  Diese können unter Wahrung der Privatsphäre Anfragen bearbeiten, indem sie nur notwendige Informationen speichern und verarbeiten.

Datenschutzkonforme Anwendungen setzen oft auf Anonymisierung und Pseudonymisierung, um die Privatsphäre der Betroffenen zu schützen.

KONTAKT

SIE HABEN FRAGEN?

Ansprechpartnerin: Luisa-Elene Pissors
E-Mail: digitalzentrum@hochschule-stralsund.de
www.digitalzentrum-rostock.de

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages