Mittelstand-Digital Zentrum Rostock

Künstliche Intelligenz und Datenschutz – Risiken erkennen, Chancen nutzen

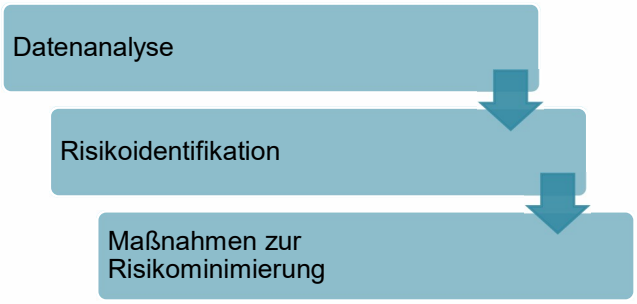
KURZ UND KNAPP

WORUM GEHT'S?

Künstliche Intelligenz (KI) bietet enorme Chancen für Unternehmen und Institutionen, birgt aber auch Risiken, die im Vorfeld erkannt und gemindert werden müssen. Die Risikoanalyse ist ein zentraler Bestandteil für den sicheren und datenschutzkonformen Einsatz von KI-Systemen, insbesondere im Hinblick auf die EU-Datenschutz-Grundverordnung (DSGVO) und die KI-Verordnung (AIA - Artificial Intelligence Act) der Europäischen Union.

Was ist eine Risikoanalyse bei KI?

Eine Risikoanalyse ist der systematische Prozess zur Identifikation und Bewertung von Risiken, die mit der Entwicklung und dem Einsatz von KI verbunden sind. Sie hilft dabei, potenzielle Schäden oder Probleme, die durch den Einsatz von KI entstehen könnten, im Voraus zu erkennen und geeignete Maßnahmen zur Minderung dieser Risiken zu ergreifen.



Methoden zur Risikoabschätzung

- **Datenschutz-Folgenabschätzung (DSFA)**:
  Eine DSFA ist dann erforderlich, wenn ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Hierbei werden potenzielle Datenschutzrisiken systematisch ermittelt und bewertet.
- **Risikoanalyse gemäß ISO-Normen**:
  Normen wie ISO/IEC 27005 bieten Leitlinien für die Durchführung einer umfassenden Risikoanalyse im Bereich der Informationssicherheit, einschließlich der spezifischen Anforderungen für KI-Systeme.
- **Ethikbewertung**:
  Ein Bewertungsprozess, der sicherstellt, dass KI-Systeme in Übereinstimmung mit ethischen Grundsätzen handeln, z.B. Vermeidung von Diskriminierung oder unfairer Behandlung.

Relevante Regularien

- **Datenschutz-Grundverordnung (DSGVO)**:
  Die DSGVO legt fest, dass alle Systeme, die mit personenbezogenen Daten arbeiten, besondere Datenschutzanforderungen erfüllen müssen. KI-Systeme, die mit sensiblen Daten arbeiten, müssen daher so entwickelt werden, dass der Schutz dieser Daten jederzeit gewährleistet ist. Eine Datenschutz-Folgenabschätzung ist oft erforderlich, um Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten durch KI zu analysieren.
- **KI-Verordnung (AIA - Artificial Intelligence Act)**:
  Diese Verordnung der EU soll einen einheitlichen Rechtsrahmen schaffen, um die Sicherheit und ethische Nutzung von KI-Systemen zu gewährleisten. Sie kategorisiert KI-Systeme in verschiedene Risikostufen (z.B. niedriges, hohes oder unannehmbares Risiko) und legt fest, welche Sicherheitsanforderungen zu erfüllen sind.

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital Zentrum Rostock

Künstliche Intelligenz und Datenschutz – Risiken erkennen, Chancen nutzen

Schlüsselrisiken bei KI-Systemen

- **Datenschutzverletzungen**:
  KI-Systeme verarbeiten oft große Mengen an Daten. Die unsachgemäße Handhabung dieser Daten kann zu Datenschutzverletzungen führen. Risiken, die hier berücksichtigt werden müssen, betreffen vor allem die Integrität, Vertraulichkeit und Verfügbarkeit der Daten.
- **Ethik und Diskriminierung**:
  KI-Systeme können unbeabsichtigt diskriminierende Entscheidungen treffen, etwa aufgrund von verzerrten Trainingsdaten. Die Risikoanalyse muss sicherstellen, dass die KI fair und transparent agiert, um ethische Risiken zu minimieren.
- **Sicherheitslücken**:
  KI-Systeme sind potenziell anfällig für Cyberangriffe. Ein besonderes Risiko besteht in der Manipulation von Trainingsdaten (Data Poisoning) oder Modellangriffen. Die Sicherheit der KI muss regelmäßig überprüft werden.
- **Rechtsrisiken**:
  Der Einsatz von KI könnte gesetzliche Anforderungen verletzen, insbesondere im Hinblick auf die DSGVO und andere regulatorische Rahmenbedingungen. Eine strikte Einhaltung der gesetzlichen Vorgaben ist daher unerlässlich.

Weitere Quellen für Risikoanalyse und Datenschutz in KI

- **Standard-Datenschutzmodell (SDM)**:
  Das SDM bietet eine methodische Grundlage, um Datenschutzanforderungen systematisch und einheitlich in IT-Systemen zu implementieren. Besonders wichtig ist es für die Beurteilung von KI-Systemen in Bezug auf Datenschutprinzipien.
- **Hambacher Erklärung zur Künstlichen Intelligenz**:
  Diese Erklärung formuliert ethische und datenschutzrechtliche Grundsätze im Umgang mit KI. Die Erklärung dient als Leitfaden, um sicherzustellen, dass KI-Systeme menschenzentriert und datenschutzkonform entwickelt werden.
- **Positionspapier der Datenschutzkonferenz (DSK)**:
  Dieses Positionspapier bietet Empfehlungen zu technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen. Es umfasst Anforderungen wie Transparenz und Rechenschaftspflicht.
- **Orientierungshilfe „Künstliche Intelligenz und Datenschutz“**:
  Die Orientierungshilfe bietet eine praxisnahe Anleitung für Unternehmen und Entwickler, um KI-Systeme datenschutzkonform zu gestalten. Sie behandelt Themen wie Datenminimierung, Zweckbindung und die Rechte der betroffenen.
- **„AI How-to Sheets“ der CNIL**:
  Die französische Datenschutzbehörde CNIL bietet praktische Anleitungen, sogenannte „How-to-Sheets“, die konkrete Hilfestellungen für den datenschutzkonformen Einsatz von KI geben.

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