KI in Unternehmen sicher nutzen

Um Künstliche Intelligenz kommt kaum ein Unternehmen mehr herum. Wer keine hauseigene Lösung hat, nutzt häufig kommerzielle KIs. Doch was mit den Daten passiert, die von Dienstleistern verarbeitet werden, weiß man oft nicht so genau. Das Verbundprojekt DAISY hilft Unternehmen, KI verantwortungsvoll zu nutzen. Die Forschenden der Universitäten Bochum, Duisburg-Essen und Witten/Herdecke schauen sich Use Cases an, entwickeln technische Lösungen zum sicheren KI-Einsatz und beziehen organisations- und individualpsychologische Aspekte ein. Alle Ergebnisse werden öffentlich zur Verfügung gestellt.

Der Verbund wird ab September 2026 für drei Jahre mit 1,29 Millionen Euro im Rahmen der Förderlinie "Plattform Privatheit" vom Bundesministerium für Forschung, Technologie und Raumfahrt gefördert.

Kooperationspartner

Neben der Ruhr-Universität Bochum, die die Koordination übernimmt, sind an dem Verbund beteiligt: die Universität Duisburg-Essen, die Universität Witten/Herdecke und die WirtschaftsEntwicklungsGesellschaft Bochum.

Im Spannungsfeld zwischen Effizienz und Datenschutz

"In vielen Unternehmen schlummern wertvolle Daten, die bislang kaum jemand systematisch nutzen konnte. Künstliche Intelligenz ändert das gerade grundlegend", sagt Projektkoordinator Dr. Steffen Becker vom Research Center Trustworthy Data Science and Security an der Ruhr-Universität Bochum. Egal ob es darum geht, Kundenanfragen zu beantworten, Verträge zusammenzufassen oder Besprechungen zu protokollieren: KI-Anwendungen können viele Aufgaben im Arbeitsalltag erleichtern und beschleunigen - und greifen dabei fast immer auf interne Unterlagen, Kunden- oder Personaldaten zu. "Wir stehen also immer im Spannungsfeld zwischen der Effizienzsteigerung durch die KI und dem Schutz sensibler Daten", so Steffen Becker.

Technische Lösungen

Das Forschungsteam will sich die gelebte Praxis in den Unternehmen zunächst genau ansehen, um dann Lösungen für einen sicheren KI-Einsatz zu entwickeln. "Was mit den Daten geschieht, sobald sie an einen KI-Dienst übermittelt sind, lässt sich von außen kaum vollständig nachvollziehen. Wir wollen deshalb systematisch prüfen, welche Datenschutzrisiken die gängigen Dienste tatsächlich mit sich bringen - und Unternehmen Werkzeuge an die Hand geben, mit denen sensible Daten gar nicht erst ungeprüft abfließen", erklärt Becker. Die Forschenden denken dabei zum Beispiel an Filterlösungen, die vertrauliche Informationen erkennen, bevor sie das Unternehmen verlassen, und Nutzende warnen oder die Übermittlung blockieren.

Das richtige Maß an Vertrauen und Skepsis

Die Forschenden der Universität Witten/Herdecke sehen sich die KI-bezogenen Prozesse in den Unternehmen aus organisationspsychologischer Warte an. Wie entscheiden zum Beispiel die Geschäftsführungen? Welche Haltung haben die Betriebsräte? Die individualpsychologische Sicht bringt das Team der Universität Duisburg-Essen ein. Hier stehen die Beschäftigten im Mittelpunkt: Welche mentalen Modelle über KI bringen sie mit? Welche Fehlannahmen gibt es? Wie kann man das richtige Maß an Vertrauen in die KI erreichen? Hier werden etwa Schulungsformate entwickelt. "Über ein Rechtsgutachten decken wir auch die juristischen Aspekte ab, insbesondere das Zusammenspiel von Datenschutz, KI-Verordnung und Arbeitsrecht", sagt Steffen Becker.

Über das RC Trust

Das Research Center Trustworthy Data Science and Security (RC Trust) erforscht, wie vertrauenswürdige intelligente Systeme für sicherheitskritische Anwendungen gestaltet werden können. Der menschenzentrierte Ansatz verbindet vier Forschungsschwerpunkte: vertrauenswürdige Datenanalyse, erklärbares Maschinelles Lernen, Cybersicherheit und Datenkontrolle. Ziel ist es, sichere und nachvollziehbare Technologien zu entwickeln und Menschen dabei zu unterstützen, ihre Möglichkeiten und Grenzen zu verstehen.

Das RC Trust wird gemeinsam von Ruhr-Universität Bochum, TU Dortmund und Universität Duisburg-Essen in der Universitätsallianz Ruhr (UA Ruhr) getragen. Es ist Teil der aus der Ruhr-Konferenz hervorgegangenen Research Alliance Ruhr, die das Land Nordrhein-Westfalen seit 2025 dauerhaft fördert.