Der Einsatz von KI muss im Einklang mit den Gesetzen erfolgen

Künstliche Intelligenz: Vertraulichkeit als zentrales Thema

Im Gegensatz zur Europäischen Union, die mit dem EU AI Act ein umfassendes Regelwerk zur künstlichen Intelligenz verabschiedet hat, gibt es in der Schweiz bislang keine spezifischen Regeln. Massgebend sind das Datenschutzgesetz (DSG), das Obligationenrecht (OR) und das Strafgesetzbuch (StGB).

Martina Guillod

Datenübermittlung

Die Ausgangsfrage ist einfach: Bedeutet der Einsatz von KI, dass Daten an Dritte weitergegeben werden? In vielen Fällen lautet die Antwort «Ja». Noch problematischer ist, dass die Daten ins Ausland weitergegeben werden können. ChatGPT verarbeitet die Daten beispielsweise auf Servern in den USA und DeepSeek in China. Hinzu kommt, dass diese Tools die von Ihnen zur Verfügung gestellten Daten (z. B. die Fragen, die Sie ihnen stellen, oder die Dateien, die Sie ihnen zur Analyse vorlegen) auch nutzen können, um ihre eigenen Modelle zu trainieren und zu verbessern. Konkret bedeutet dies, dass die von Ihnen in diese KI-Tools eingegebenen Daten möglicherweise in den Antworten anderer Benutzerinnen und Benutzer erscheinen.

Personendaten

Das DSG verbietet die Weitergabe von Personendaten an Dritte nicht grundsätzlich. Allerdings muss nach Art. 19 DSG die Person, deren Personendaten bearbeitet werden, insbesondere über die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen die Daten bekannt gegeben werden, informiert werden. Eine doch sehr schwierige Aufgabe, wenn unklar ist, wo genau die in ein KI-Tool eingegebenen Daten wieder erscheinen.

Es wäre zwar denkbar, die Einwilligung der betroffenen Person einzuholen. Diese Zustimmung wäre jedoch rechtlich unwirksam. Die KI kann Personendaten weitergeben, ohne dass die betroffene Person erfährt, an wen, wo und in welchem Zusammenhang. Eine erteilte Einwilligung wäre somit zu allgemein gefasst und daher nicht ausreichend. Aufgrund der Intransparenz der Algorithmen und der KI im Allgemeinen können die Benutzerinnen und Benutzer zudem nicht klar und verständlich über die Verwendung ihrer Daten informiert werden, was eine hinreichende Einwilligung ausschliesst.

Aus Sicht des DSG ist es daher problematisch, Personendaten mittels frei zugänglicher KI-Tools zu bearbeiten. Wir raten deshalb von diesem Vorgehen ab (siehe auch Info Patronale Nr. 331). Falls Personendaten mithilfe von KI bearbeitet werden, ist sicherzustellen, dass sie nicht für das Training des KI-Systems genutzt werden. Als alternative Lösung kann es sinnvoll sein, Fachleute zu beauftragen, eine interne KI zu entwickeln.

Sonstige Daten

Eine gleiche Problematik besteht bei Daten, die zwar nicht personenbezogen, aber geheim sind. Die Übermittlung solcher Daten mithilfe von KI-Tools verstösst zwar nicht gegen das DSG, kann aber andere Rechtsnormen verletzen. Beispiele hierfür sind die Geheimhaltungspflicht der Arbeitnehmenden (Art. 321a OR) oder die Verletzung des Berufsgeheimnisses (Art. 321 StGB).

Fazit

KI bietet zahlreiche Möglichkeiten, birgt aber auch erhebliche Herausforderungen im Bereich Vertraulichkeit und Einhaltung des gesetzlichen Rahmens. Unternehmen müssen sicherstellen, dass der Einsatz von KI im Einklang mit den geltenden Gesetzen steht, um rechtliche und ethische Konsequenzen zu vermeiden. Es empfiehlt sich, auf interne Lösungen oder spezialisierte Fachleute zurückzugreifen, die das Unternehmen bei diesem Prozess begleiten können.