Ass. iur. Florian Hallaschka, stellvertretender Datenschutzbeauftragter

Künstliche Intelligenz (KI) auf einen Blick

1. Definitionen:

KI ist ein System, das unterstützungshalber Aufgaben erfüllt, die sonst menschliches Denken erfordern, wie Texterstellung, Sprachverständnis und Datenauswertung.
Ein **KI-System** ist ein autonomes, anpassungsfähiges Computersystem, das aus den erhaltenen Eingaben **(Prompts)** Ergebnisse wie Inhalte und Entscheidungen ausgibt.
KI-Anwendung ist der konkrete Einsatz: Chatbot, Sprachassistent, Analyse-Software.
Anbieter ist der Entwickler des Systems, **Betreiber** ist der verantwortliche Verwender des KI-Systems; **Anwender** ist der konkrete Nutzer der Anwendung.
Unterschieden werden **KI mit verbotenen KI-Praktiken**, **Hochrisiko-KI** (**erlaubt**, aber mit besonderer Sorgfalt, weil das KI-System etwa zum Profiling dient), sowie **KI-Modelle mit allgemeinem Verwendungszweck** – ggf. mit **systemischem Risiko** für Gesundheit, (öffentliche) Sicherheit, Grundrechte oder die Gesellschaft insgesamt.

Anbieter, Betreiber und Anwender unterliegen einer **Schulungspflicht.**

2. Transparenz:

Dem Anwender muss durch besondere Vorkehrungen immer klar sein, dass er mit einer KI kommuniziert. Mit Hilfe von KI erlangte Ergebnisse sind als solche zu **kennzeichnen**.

3. Datenschutz und Informationssicherheit:

In eine nicht rein lokal betriebene KI dürfen **keine personenbezogenen Daten** eingegeben werden, sofern diese als **Trainingsdaten** für die Weiterentwicklung der KI fungieren, für den Verbleib in der KI-Anwendung oder dem KI-System vorgesehen sind oder gar zur Verbesserung des Systems auch für Dritte genutzt werden. Auch bei zugesichertem Verzicht auf Training der KI dürfen **keine Daten mit hohem Schutzbedarf** (sensible personenbezogenen Daten oder Forschungsgeheimnisse) in die externe KI-Anwendung eingegeben oder gespeichert werden.
Eine Verarbeitung personenbezogener Daten in einer KI aus Staaten außerhalb der EU bzw. des EWR ohne Angemessenheitsbeschluss der EU-Kommission (**unsichere Drittländer**) ist **verboten**.

4. Organisatorisches:

Eine KI-Software darf in keinem Falle eigenmächtig installiert und angewendet werden. Sie ist nur auf Dienstrechnern und nur nach ausdrücklicher Genehmigung (Lucom-Formular „Softwarefreigabe“) zu installieren. Auch Web-Anwendungen, die nicht installiert werden müssen, sind über Lucom zu beantragen.
Soll eine externe KI eingesetzt werden, muss dies dienstlich notwendig sein, und es ist dem Informationssicherheitsbeauftragten ein Betriebskonzept vorzulegen.

In der Regel ist aufgrund der Natur und des Umfangs der Daten vor dem systematischen Einsatz von KI eine **Datenschutzfolgenabschätzung** zu erstellen. Die Verantwortung hierfür trägt die zuständige Leitung, die Ausführung kann an die Fachverantwortlichen delegiert werden. Der Datenschutzbeauftragte wird hierbei beratend tätig.

Version 1.0, Stand: 11.03.2026, Autor: Florian Hallaschka