

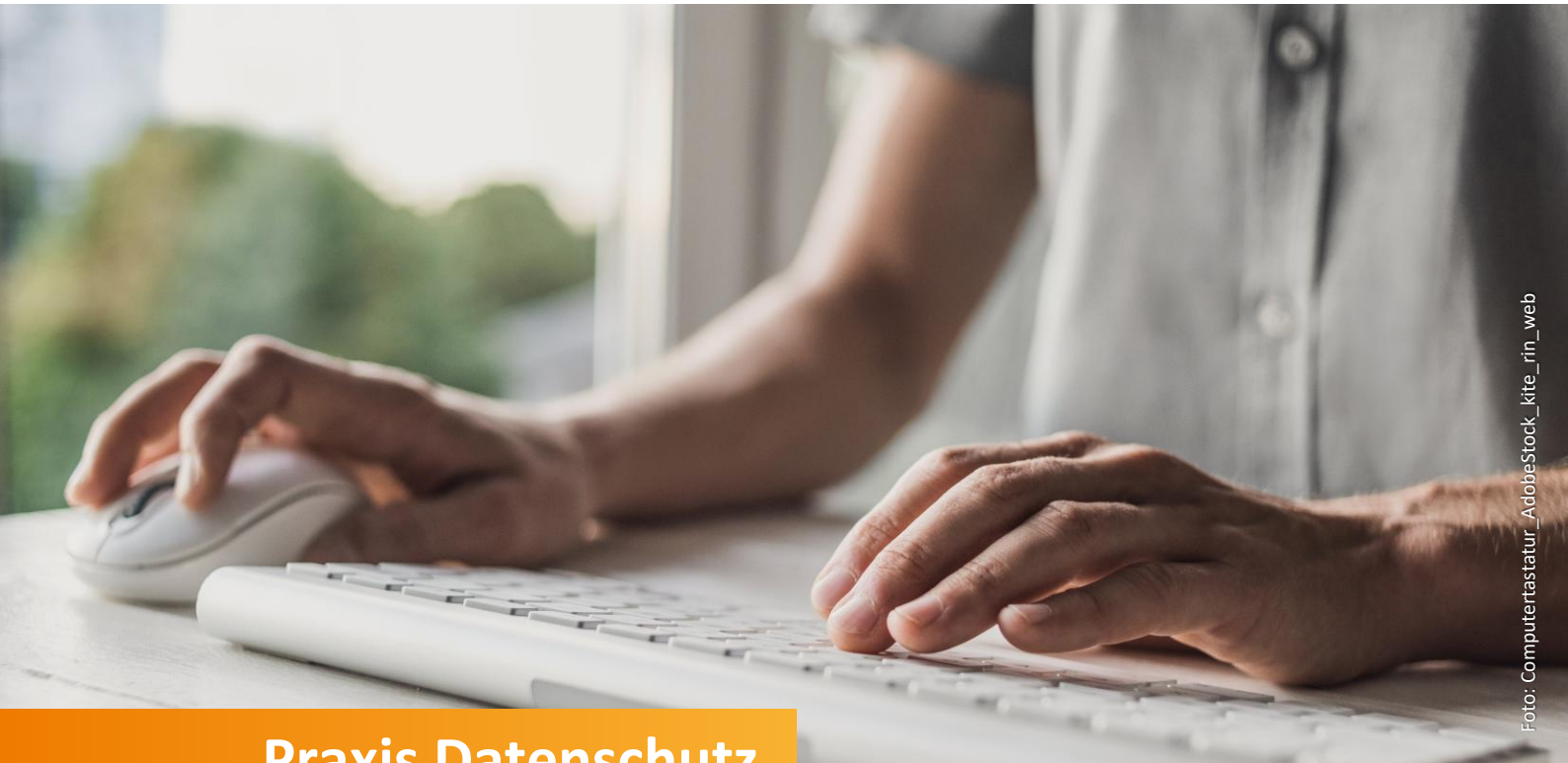


Foto: Computertastatur_AdobeStock_kite_rin_web

Praxis Datenschutz

Datenschutz bei künstlicher Intelligenz

Beim Einsatz künstlicher Intelligenz sind auch Aspekte des Datenschutzes zu berücksichtigen. Was konkret zu beachten ist, zeigen die aufbereiteten Praxisempfehlungen.

Berlin, August 2025

Datenschutz: Einer von vielen Aspekten bei der KI-Nutzung

Der Handlungsrahmen für den zulässigen Einsatz von KI-Anwendungen folgt aus zahlreichen Vorschriften unterschiedlichster Rechtsbereiche. So sind neben den maßgeblichen Regelungen der europäischen KI-Verordnung u.a. auch das Urheberrecht bei der Verwendung und Erstellung von Bildern und Texten oder der Datenschutz bei der Eingabe personenbezogener Daten zu beachten. Die nachfolgenden Ausführungen beschränken sich auf praxisrelevante Aspekte des Datenschutzes bei der Anwendung von KI-Tools und sind als spezifische Ergänzung bestehender KI-Handreichungen zu verstehen.

Wann ist Datenschutz beim Einsatz von KI zu beachten?

Die Nutzung von KI ist für sich genommen nicht datenschutzrelevant. Der Datenschutz ist jedoch dann zu beachten, wenn beim Einsatz von KI personenbezogene Daten verwendet werden. Personenbezogene Daten sind alle Informationen, die Rückschlüsse auf eine lebende Person zulassen (z.B. Name, körperliche Merkmale, finanzielle Verhältnisse, etc.). Solange solche personenbezogenen Daten nicht durch eine KI verarbeitet werden, findet der Datenschutz keine Anwendung.

➔ ***Es ist grundlegend zu empfehlen, bei der KI-Nutzung auf die Verwendung personenbezogener Daten zu verzichten.***

- Prüfen Sie, ob bei der Nutzung von KI-Tools die Eingabe personenbezogener Daten zwingend erforderlich ist. Häufig sind solche Daten nicht notwendig.
- Ansonsten ist eine vorherige Pseudonymisierung oder Anonymisierung der Daten angezeigt.

Checkliste: Datenschutzmaßnahmen

Ist es unerlässlich, personenbezogene Daten bei Nutzung einer KI zu verwenden, müssen bestimmte Datenschutzvorgaben beachtet werden. Vor der Einführung einer KI in die Arbeitsprozesse Ihrer Handwerksorganisation sollten Sie stets Ihren Datenschutzbeauftragten einbeziehen, um folgende Aspekte zu prüfen und sicherzustellen.

■ Verantwortlichkeit klären

Wenn Sie von einer KI personenbezogene Daten verarbeiten lassen wollen, gilt Ihre Handwerksorganisation als verantwortliche Stelle für den Datenschutz. Um Probleme bei der Verantwortungszuweisung zu vermeiden, ist zu raten, KI-Nutzungen für dienstliche Zwecke ausschließlich über dienstliche Geräte zu gestatten und die Verwendung privater Geräte von Beschäftigten ausdrücklich zu untersagen.

Wird ein KI-Tool eines Drittanbieters verwendet, muss ein sog. Datenschutz-Auftragsverarbeitungsvertrag (AV) geschlossen werden. Bei großen Anbietern (Microsoft, Apple, etc.) enthalten i.d.R. die Nutzungsbestimmungen bereits die erforderliche AV.

■ **Rechtsgrundlage bestimmen**

Die Verarbeitung personenbezogener Daten bedarf immer einer rechtlichen Befugnis. Das kann entweder eine gesetzliche Erlaubnis oder die Einwilligung der betroffenen Personen sein, deren Daten verarbeitet werden. Zu beachten ist, dass sämtliche Schritte der KI-Nutzung einer eigenen Rechtsgrundlage bedürfen. Soll z.B. ein Chatbot für Besucher der Webseite einer Handwerkskammer eingeführt werden, ist jeweils eine Rechtsgrundlage für die vorherige Datensammlung, das Training des Chatbots sowie für die Herausgabe der Chatbot-Antworten an die Webseite-Besucher erforderlich.

Einwilligungen können z.B. im Zusammenhang mit der Nutzung von Beschäftigtendaten durch den Arbeitgeber erforderlich sein und durch eine Betriebsvereinbarung eingeholt werden. Ebenso kann die Einwilligung von Antragstellern bei KI-unterstütztem Eintragungsverfahren in die Handwerksrolle eingeholt werden.

Kommt eine Einwilligung aus praktischen Gründen nicht in Betracht (z.B. zu hohe Anzahl betroffener Personen), braucht es eine gesetzliche Nutzungsermächtigung. Als Rechtsgrundlage kann Art. 6 Abs. 1 Buch. f) DSGVO herangezogen werden. Dies gilt auch für öffentlich-rechtliche Handwerksorganisationen, solange die Verwendung einer KI nicht für die Erfüllung gesetzlich-hoheitlicher Aufgaben genutzt wird.

■ **Daten minimieren**

Werden mithilfe von KI personenbezogene Daten verarbeitet, ist stets der Grundsatz der Datenminimierung konsequent anzuwenden und dementsprechend nur zwingend erforderliche Daten zu verwenden. So sind z.B. bei analytischen KI-Tools zur Betriebsberatung i.d.R. Finanz- und Wirtschaftsdaten erforderlich, die Firmenbezeichnung oder der Name des Inhabers sind dagegen für den Nutzungszweck irrelevant.

■ **Technische und organisatorische Maßnahmen (TOMs) ergreifen**

Bei jeder Datennutzung gilt es, durch geeignete TOMs sicherzustellen, Datenschutzvorfällen vorzubeugen und z.B. Datenlecks, den Zugriff Unbefugter oder eine zweckwidrige Datennutzung zu vermeiden. Im Zusammenhang mit KI-Tools sollte insbesondere darauf geachtet werden, dass die KI-Anwendung ausschließlich mit zulässigen (sog. kuratierten) Daten trainiert wurde oder neu eingegebene Daten nicht zum weiteren Training verwendet werden. Dies kann in der Regel mit kostenpflichtigen Pro-Tools gewährleistet werden.

Zudem empfiehlt sich die Nutzung von KI-Anwendungen, die ausschließlich in der EU und damit im Geltungsbereich der DSGVO gehostet werden. Hierdurch wird sichergestellt, dass der Hosting-Dienstleister die Anforderungen der DSGVO beachtet.

■ **Verbot automatisierter Entscheidungen beachten**

Die DSGVO verbietet in gleicher Weise wie die europäische KI-Verordnung, dass Entscheidungen, die gegenüber einer Person rechtliche Wirkung entfaltet, ausschließlich automatisiert erfolgt. So dürfen Verwaltungsentscheidungen der Handwerkskammern oder rechtlich relevante Empfehlungen der Betriebsberatungen nicht ausschließlich

auf einem Ergebnis einer KI-Anwendung erfolgen, sondern bedürfen zumindest einer menschlichen Mitentscheidung.

Interne Maßgaben zur KI-Nutzung

Der interne Umgang mit KI sollte in jeder Handwerksorganisation festgelegt werden. Hierzu gehören neben der Bestimmung, welche KI-Tools in welchem Handlungsrahmen und zu welchen Zwecken verwendet werden dürfen, auch Maßgaben zur Wahrung des Datenschutzes. Diese sollten entsprechend der vorherigen Ausführungen und Checkliste folgende Handlungshinweise zum Datenschutz enthalten.

- Vermeidung der Nutzung personenbezogener Daten
- Datenminimierung
- Keine automatisierten Entscheidungen zulassen

Ein Muster interner Leitlinien befindet sich im Anhang.

Herausgeber:

Zentralverband des Deutschen Handwerks e.V.
Haus des Deutschen Handwerks
Mohrenstraße 20/21 · 10117 Berlin
Postfach 110472 · 10834 Berlin

Lobbyregister: R002265
EU Transparency Register: 5189667783-94

Der Zentralverband des Deutschen Handwerks e. V. (ZDH) vertritt die Interessen von rund 1 Million Handwerksbetrieben in Deutschland mit rund 5,6 Millionen Beschäftigten. Als Spitzenorganisation der Wirtschaft mit Sitz in Berlin bündelt der ZDH die Arbeit von Handwerkskammern, Fachverbänden des Handwerks auf Bundesebene sowie bedeutenden wirtschaftlichen und sonstigen Einrichtungen des Handwerks in Deutschland. Mehr unter www.zdh.de

KI-Handlungsleitfaden bei dienstlicher Nutzung von KI-Tools

KI-Tools (Werkzeuge, die mit künstlicher statt menschlicher Intelligenz agieren) sind beispielsweise in der Lage, Texte oder Bilder zu generieren und menschliche Konversationen zu simulieren. Dabei greifen diese Tools auf umfangreiche Wissensbestände zurück, die auch wissenschaftliche Publikationen umfassen. KI kann dadurch u.a. komplexe und umfangreiche Texte unterschiedlicher Gattungen verfassen, Texte zusammenfassen und Antworten auf anspruchsvolle Fragen jeder Art geben.

Mittlerweile sind KI-Tools auch bereits als feste Bestandteile in Standard-Software integriert (z.B. Internet-Browser, Suchmaschinen und Office-Anwendungen).

Sollten diese Arbeitsmittel für die Erledigung Ihrer Aufgaben genutzt werden, sind folgende Hinweise dringend zu beachten, da ansonsten Datenschutz- und Urheberrechtsverstöße drohen, die auch zu einer persönlichen Haftung des Mitarbeiters führen können.

1. Allgemeines:

KI generierte Arbeitsergebnisse sind selten frei von Fehlern. KI neigt dazu, Tatsachen, Referenzen und Quellen zu erfinden oder zu vermengen (sog. „Datenhalluzination“). Selbst einfachste Berechnungen sind häufig falsch. Werden falsche Inhalte unkontrolliert und unkritisch übernommen, werden diese als eigene Fehler zugerechnet. Daher müssen KI-basierte Texte immer kritisch hinterfragt und auf Richtigkeit geprüft werden. Künstliche Intelligenz kann unterstützen, aber menschliche Intelligenz nicht ersetzen.

2. Datenschutz:

Onlinebasierte KI-Tools speichern neben der IP-Adresse des Nutzers auch Chatverläufe und nutzen diese Daten für diverse Zwecke, beispielsweise für Forschungs- und Verbesserungszwecke. Es ist untersagt, vertrauliche oder sensible Informationen (z.B. Geschäftsgeheimnisse, Geschäftsideen) im Chat eines KI-Tools einzugeben.

Personenbezogene Daten (z.B. Daten von Betrieben, Kollegen oder Geschäftspartnern) dürfen ausschließlich in solche KI-Tools eingegeben werden, die den Anforderungen der DSGVO genügen und ausdrücklich von der Geschäftsführung unter empfohlener Mitwirkung des Datenschutzbeauftragten freigegeben wurden. Wenn Sie personenbezogene Daten in ein KI-Tool eingeben, beschränken Sie sich auf zwingend erforderliche Daten. Alle Daten, die für Ihre Verwendung nicht notwendig sind, müssen außer Acht gelassen werden. Ansonsten ist eine vorherige Pseudonymisierung oder Anonymisierung der Daten angezeigt.

Sie dürfen Entscheidungen, die gegenüber einer Person rechtliche Wirkung entfaltet, nicht ausschließlich durch ein KI-Tool treffen lassen.

3. Urheberrecht:

Anbieter von KI-Tools übernehmen keine Verantwortung für die rechtliche Konformität der Nutzung ihres KI-Tools. Es liegt in der Verantwortung des Nutzers, sicherzustellen, dass alle anwendbaren Gesetze und Vorschriften eingehalten werden.

Zwar ist eine Verletzung von Urheberrechten des KI-Anbieters in der Regel ausgeschlossen, weil nur Werke einer natürlichen Person urheberrechtlich geschützt sind. Allerdings sind in den meisten Fällen die korrekten Quellen, die das KI-Tool für die Erstellung seiner Texte verwendet hat, unbekannt. Häufig fehlen Quellenangaben oder sind falsch. Somit drohen Urheberrechtsverstöße, wenn generierte Arbeitsergebnisse, wie Texte oder Bilder übernommen werden und damit fremdes geistiges Eigentum verletzt wird.

KI-generierte Arbeitsergebnisse sind als solche zu kennzeichnen und dürfen nur verwendet werden, wenn kein Urheberrechtsverstoß ersichtlich ist.

Es ist untersagt, urheberrechtlich geschütztes Material zur Bearbeitung oder Verwendung zur Verfügung zu stellen.

Diese Anweisungen treten am XX.XX.XXXX in Kraft