Gesellschaft für Datenschutz
und Datensicherheit e.V.

ChatGPT im Unternehmen

Generative Künstliche Intelligenz (KI) kann, wie jede andere Technologie, auch **Risiken** für den Datenschutz **bergen**, wenn sie nicht verantwortungsvoll eingesetzt wird. Und es braucht nicht viel Fantasie, um zu erkennen, wie schnell ein Unternehmen eine hart erarbeitete Beziehung zu seinen Kunden durch eine schlechte Nutzung generativer KI beschädigen kann. Doch auch wenn die Technologie neu ist, bleiben die Grundsätze des Datenschutzrechts die gleichen und es gibt einen klaren Fahrplan für Unternehmen, um Innovationen so zu gestalten, dass die Privatsphäre der Menschen gewahrt bleibt.

Organisationen, die generative KI entwickeln oder einsetzen, sollten ihre Datenschutzverpflichtungen von Anfang an berücksichtigen und einen Ansatz des Datenschutzes durch Design und durch Voreinstellung verfolgen (Art. 25 DS-GVO). Dies ist nicht optional, wenn Sie personenbezogene Daten verarbeiten, dies ist gesetzlich vorgeschrieben.

Das Datenschutzrecht gilt auch dann, wenn die personenbezogenen Daten, die Sie verarbeiten, aus öffentlich zugänglichen Quellen stammen. Wenn Sie generative KI entwickeln oder verwenden, die personenbezogene Daten verarbeitet, müssen Sie sich die folgenden Fragen stellen:

1. **Auf welcher Rechtsgrundlage verarbeiten Sie personenbezogene Daten?** Wenn Sie personenbezogene Daten verarbeiten, müssen Sie eine geeignete Rechtsgrundlage angeben, z.B. die Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO) oder berechtigte Interessen (Art. 6 Abs. 1 lit. f DS-GVO).
2. **Haben Sie einen Vertrag mit einem Anbieter generativer KI wie ChatGPT?** Wenn Sie ein Auftragsverarbeiter oder gemeinsam mit anderen für die Verarbeitung Verantwortlicher (Joint Controller) sind, muss es einen rechtsverbindlichen Vertrag geben, in dem diese Beziehung zum Ausdruck kommt.
3. **Haben Sie eine Datenschutz-Folgenabschätzung (DSFA) vorbereitet?** Bevor Sie mit der Verarbeitung personenbezogener Daten beginnen, müssen Sie alle Datenschutzrisiken mit Hilfe der Datenschutz-Folgenabschätzung bewerten und abmildern. Ihre Datenschutz-Folgenabschätzung sollte auf dem neuesten Stand gehalten werden, wenn sich die Verarbeitung und ihre Auswirkungen weiterentwickeln.
4. **Sind Sie ein für die Verarbeitung Verantwortlicher, ein Mitverantwortlicher oder ein Auftragsverarbeiter?** Wenn Sie generative KI unter Verwendung personenbezogener Daten entwickeln, sind Sie als für die Datenverarbeitung Verantwortlicher verpflichtet. Wenn Sie von Anderen entwickelte Modelle verwenden oder anpassen, können Sie ein für die Verarbeitung Verantwortlicher, ein Mitverantwortlicher oder ein Auftragsverarbeiter sein.
5. **Wie sorgen Sie für Transparenz?** Sie müssen Informationen über die Verarbeitung öffentlich zugänglich machen, es sei denn, es gilt eine Ausnahmeregelung. Wenn dies nicht mit unverhältnismäßigem Aufwand verbunden ist, müssen Sie diese Informationen direkt an die Personen weitergeben, auf die sich die Daten beziehen.

6. **Wie werden Sie die Sicherheitsrisiken abschwächen?** Zusätzlich zu den Risiken der Weitergabe personenbezogener Daten sollten Sie auch die Risiken der Modellinversion und der Ableitung von Zugehörigkeiten, des Data Poisoning[1] und anderer Formen von Angriffen durch Angreifer berücksichtigen und abschwächen.
7. **Wie werden Sie unnötige Verarbeitungen einschränken?** Sie dürfen nur die Daten erheben, die zur Erfüllung des angegebenen Zwecks erforderlich sind. Die Daten sollten relevant und auf das Notwendige beschränkt sein (Datenminimierung).
8. **Haben Sie festgestellt, ob Daten in ein Drittland übermittelt werden?** Wenn eine Übermittlung in ein Drittland stattfindet, müssen Sie sicherstellen, dass das Schutzniveau für personenbezogene Daten in den Ländern der EU und der EWG entspricht. Gibt es Standardvertragsklauseln?
9. **Wie werden Sie Anfragen zu den Rechten des Einzelnen nachkommen?** Sie müssen in der Lage sein, den Anträgen von Personen auf Auskunft, Berichtigung, Löschung oder andere Rechte an Informationen (Rechte des Betroffenen) zu entsprechen.
10. **Werden Sie generative KI verwenden, um ausschließlich automatisierte Entscheidungen zu treffen?** Wenn ja - und diese haben rechtliche oder ähnlich bedeutsame Auswirkungen (z.B. wichtige Gesundheitsdiagnosen) - haben Einzelpersonen weitere Rechte (Rechte in Bezug auf automatisierte Entscheidungen und Profiling) gemäß Art. 22 DS-GVO.

Bonn, den 27.04.2023

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. tritt als gemeinnütziger Verein für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen - insbesondere auch die Datenschutzbeauftragten - bei der Lösung und Umsetzung der vielfältigen mit Datenschutz und Datensicherheit verbundenen rechtlichen, technischen und organisatorischen Anforderungen zu unterstützen.

Gesellschaft für Datenschutz und Datensicherheit e.V.
Heinrich-Böll-Ring 10, 53119 Bonn
info@gdd.de | www.gdd.de

[1] Beim Data Poisoning schleusen Angreifer absichtlich manipulierte Daten in ein KI-System ein, um die Aussagen des Modells zu kompromittieren.