Stellungnahme zum Einsatz von ChatGPT

Stand: Juli 2023

Eine Datenschutzfolgeabschätzung ist zum jetzigen Zeitpunkt mangels ausreichender Informationen nicht möglich. Da ChatGPT sich aber sehr schnell verbreitet nachfolgend eine Stellungnahme nicht nur aus datenschutzrechtlicher Sicht, sondern auch zur Frage ob es für Konzepte, Planungen etc. einsetzbar ist: ChatGPT gehört dem ursprünglich als Non-Profit Organisation gegründeten Forschungsunternehmen OpenAI LP, das mittlerweile gewinnorientiert arbeitet und unter anderem von Microsoft, Amazon Web Services und Infosys Technologies, einem weltweit tätigen IT Unternehmen mit Hauptsitz in Indien, unterstützt wird.

ChatGPT steht für Chatbot Generative Pre-trained Transformer und ist ein Sprachmodell, das mit Benutzereingaben und frei im Internet verfügbaren Informationen trainiert wird, um bessere Antworten zu liefern. Hinter ChatGPT steckt, sehr vereinfacht ausgedrückt, ein künstliches neuronales Netz (KI), das ähnlich wie das menschliche Gehirn funktioniert. Es sammelt und verarbeitet große Mengen an Daten. Dazu zählen Informationen zum Nutzerkonto wie Name und Kontaktdaten, aber auch alle Eingaben in das Chatfenster, samt hochgeladenen Dateien und Feedback ebenso das Nutzungsverhalten. Open AI räumt sich selbst und einer nicht näher benannten Zahl anderer Firmen weitgehende Nutzungsrechte an diesen Daten ein. ChatGPT kann nicht beurteilen ob es sich um sensible oder personenbezogene Daten handelt. Genau daraus entstehen Probleme hinsichtlich des Datenschutzes (I.) aber auch des Schutzes von Betriebs- und Geschäftsgeheimnissen (II.) sowie des Urheberrechts und anderer Rechtsgebiete (III.).

I. Problembereiche im Datenschutz bei Verarbeitung personenbezogener Daten

1. Rechtsgrundlage:

Das Datenschutzrecht ist so konstruiert, dass es sich um ein Verbot mit Erlaubnisvorbehalt handelt, was bedeutet, dass personenbezogene Daten nur dann rechtmäßig verarbeitet werden, wenn eine Rechtsgrundlage gem. Art. 6 Abs. 1 DS-GVO / § 6 Abs. 1 KDG vorliegt. Anders als z.B. in einem Forschungslabor, ist in einer Bildungseinrichtung der Einsatz von ChatGPT zur Vertragserfüllung nicht zwingend erforderlich. Liegt keine andere Rechtsgrundlage gem. Art. 6 Abs. 1 DS-GVO vor, so kommt nur eine Einwilligung der Betroffenen in Betracht. Dazu müssen die

Betroffenen allerdings über die Art der Datenverarbeitung informiert werden. Da eine KI wie ChatGPT als Blackbox gilt kann in der Regel keine detaillierte Auskunft über die Datenverarbeitung geben werden. Eine wirksame Einwilligung ist deshalb unmöglich. Ohne Rechtsgrundlage ist die Verarbeitung personenbezogener Daten rechtswidrig.

2. Betroffenenrechte:

Betroffene Personen müssen über ihre Rechte aufgeklärt und verarbeitete Daten auf Anfrage gelöscht werden. Das ist bei ChatGPT faktisch nicht möglich, da die Daten nach Eingabe in der Algorithmus-Blackbox „verschwinden“ und Bestandteil des Wissens von ChatGPT werden und bleiben. Dementsprechend verstößt die Nutzung von ChatGPT mit personenbezogenen Daten gegen die Betroffenenrechte aus Art. 15 ff DS-GVO/ § 17 ff KDG.

3. Transparenz:

Die Intransparenz des ChatGPT Algorithmus widerspricht zudem dem Grundsatz der Transparenz, wonach personenbezogene Daten in einer für die Betroffenen nachvollziehbaren Form verarbeitet werden sollen. Zudem kann ein Unternehmen so auch keine ausreichenden Informationen über den Umfang der Datenverarbeitung, die Rechtsgrundlage und die Empfänger:innen geben und verstößt damit gegen die Informationspflichten aus Art. 13 und 14 DS-GVO / §§ 15 und 16 KDG.

4. Datenübermittlung in ein Drittland:

ChatGPT gehört dem US-amerikanischen Unternehmen Open-AI das die Daten auch an Server außerhalb Europas überträgt. Da gemäß Art. 44 ff DS-GVO ein angemessenes Schutzniveau sichergestellt sein muss und es momentan noch immer kein Datenschutzabkommen zwischen der EU und den USA gibt, ist der Einsatz von ChatGPT nur dann zulässig, wenn strenge Anforderungen für den Schutz der Daten eingehalten werden, die vorab einzeln geprüft werden müssen. Hierzu liegen aber im Moment noch nicht genug Informationen vor.

5. Auftragsverarbeitungsvertrag oder gemeinsame Verantwortlichkeit:

Nutzt ein Unternehmen zur Verarbeitung von Daten einen Dienstleister, sehen europäische wie kirchliche Datenschutzgesetze vor, dass ein Auftragsverarbeitungsvertrag (AV-Vertrag) geschlossen wird. Ob aufgrund der Art und des Umfangs der Datenverarbeitung durch ChatGPT aus datenschutzrechtlicher Sicht eine Auftragsverarbeitung i.S.d. Art. 28 DSGVO, oder möglicherweise eine sog. gemeinsame Verantwortlichkeit des Anbieters von ChatGPT und des nutzenden Unternehmens vorliegt, ist bislang unklar. Sollte es sich um eine gemeinsame Verantwortlichkeit handeln würde die DSGVO weitere Voraussetzungen wie z.B. den Abschluss einer besonderen Vereinbarung über die gemeinsame Verantwortlichkeit vorsehen, die ChatGPT aktuell nicht erfüllen kann.

Bei Buchung der kostenpflichtigen Variante zu ChatGPT wird der Abschluss eines Auftragsdatenverarbeitungsvertrags angeboten. Ob dies wirklich die passende Variante ist und ob der AV-Vertrag dann auch den datenschutzrechtlichen Vorgaben genügt ist noch nicht geklärt. Bei der kostenlosen Variante von ChatGPT ist weder ein AV-Vertrag noch eine gemeinsame Verantwortlichkeit vorgesehen und daher der Betrieb datenschutzkonform mit Sicherheit nicht möglich.

Fazit: Der Einsatz von ChatGPT zur Verarbeitung personenbezogener Daten ist aus datenschutzrechtlicher Sicht rechtskonform nicht möglich.
Kann ChatGPT rechtskonform an Stellen eingesetzt werden, an denen keine persönlichen Daten verarbeitet werden?

II. Betriebs- und Geschäftsgeheimnisse

Werden keine personenbezogenen Daten verarbeitet müssen zwar keine datenschutzrechtlichen Vorschriften berücksichtigt werden, der Einsatz von ChatGPT kann aber den Schutz von Betriebs- und Geschäftsgeheimnissen gefährden. Geschäftsgeheimnisse sind vereinfacht gesagt nicht allgemein bekannte Informationen von wirtschaftlichem Wert bei dem der Inhaber ein Interesse an der Geheimhaltung hat. Bei Bildungseinrichtungen dürfte sich dies z.B. um konkrete Angebote auf Ausschreibungen handeln, jedenfalls dann, wenn man sich im Wettbewerb mit anderen Anbietern befindet.

ChatGPT nutzt nach eigenen Angaben sämtliche Eingaben zur Verbesserung seiner Dienste. Wenn Arbeitnehmende Angaben machen die auf einem Geschäftsgeheimnis basieren, kann ChatGPT diese Angaben nutzen um seine Dienste zu verbessern. So können dann andere Chat GPT-Nutzer die Angaben als Output erhalten. (Samsung hat die Verwendung von ChatGPT untersagt nachdem ein Mitarbeitender einen sensiblen Code verwendete der dann über die Datenbank von ChatGPT der Öffentlichkeit zugänglich wurde.)

III.) Urheberrecht / Kontrolle der Ergebnisse

1. Urheberrecht:

ChatGPT ist nach eigenen Angaben sehr darum bemüht die Urheberrechte anderer zu wahren, wobei aufgrund der unterschiedlichen Urheberrechte in Europa und den USA auch hier nicht von Sicherheit ausgegangen werden kann. Lässt man das beiseite, kommt allerdings im Bildungsbereich eine andere Situation in Betracht. Fordern Mitarbeitende ChatGPT auf einen bestehenden Text zu verändern liegt nach überwiegender Auffassung eine menschlich gesteuerte, durch die KI lediglich ausgeführte Bearbeitung nach § 23 Abs. 1 Satz 1 UrhG vor, die – wenn der Text urheberrechtlich geschützt ist und keine freie Benutzung vorliegt – Urheberrechte verletzt. Dies ist nur dann nicht der Fall, wenn der neue Text einen hinreichenden Abstand zum benutzten Werk hat. Hinreichender Abstand ist dann gegeben, wenn der neue Text absolut dominiert und das ursprüngliche Werk völlig hinter dem neuen Text zurücktritt.

2. Ergebniskontrolle:

Nutzer:innen sollten die durch die KI generierten Texte sorgfältig darauf überprüfen, ob personenbezogene Daten Dritter darin vorkommen. Ist der Ursprung der personenbezogenen Daten nicht bekannt – und das dürfte die Regel sein – sollte der Text jedenfalls nicht mit den personenbezogenen Daten genutzt werden. Denn die Bildungseinrichtung die den Text verwendet ist dafür zuständig nachzuweisen, dass diese Person mit der Nennung ihres Namens einverstanden ist.

Die KI nimmt ihr Wissen aus dem Netz und den Chats. Dabei wird nicht immer die politisch korrekte Sprache verwendet. Die Texte sind also auch dahingehend zu

überprüfen, ob sie dem korrekten Sprachgebrauch entsprechen und nicht etwa abwertende Sprache nutzen.

D) Ausblick / Mögliches Vorgehen / Technische Möglichkeiten:

Die Taskforce der deutschen Datenschutzbehörden prüft momentan die Datenschutzkonformität von ChatGPT. Wie schnell hier mit einer raschen Entscheidung zu rechnen ist, kann nicht abgesehen werden.

Die EU arbeitet mit Hochdruck an einer KI Verordnung die voraussichtlich noch in diesem Jahr fertig sein wird. Selbst wenn sie erst in 2025 in Kraft treten sollte, dürfte diese Verordnung eine gute Basis für einen einheitlichen Umgang mit ChatGPT sein.

Es sollten betriebsinterne Richtlinien für den Einsatz generativer KI (also aller KI basierender Programme) erstellt werden. Diese Richtlinien sollten die zulässigen Einsatzzwecke benennen und Vorgaben sowohl für den Umgang mit personenbezogenen Daten als auch mit Geschäftsgeheimnissen machen.

Technisch kann an den Einstellungen gearbeitet und so der Datenschutz erhöht werden. Standardmäßig lässt sich OpenAI genehmigen, alle Daten der ChatGPT-Nutzer:innen zur Erweiterung des Wissens der KI zu verarbeiten. Unter chat.openai.com lässt sich der Datenschutz nachträglich modifizieren. OpenAI behauptet, dass darüber zumindest eine Einschränkung der Nutzung der eingegebenen Daten möglich ist.

Die US-amerikanischen IT-Riesen haben in der Vergangenheit hinreichend Anlass gegeben nicht allen Angaben immer glauben zu schenken. Deshalb sollte man sich um eine eigene technische Lösung des Problems bemühen. Nachfolgend ein Vorschlag meines Kollegen F. Schwanitz:

Schutz vor Ausspähung und Datensammlung

<u>1. Hochsicherheitsbetriebssysteme:</u>

Der sicherste technische Schutz vor Ausspähung und Datensammlung auf ChatGPT ist die temporäre, spurlose Verwendung eines Hochsicherheitsbetriebssystems auf dem PC. Es gibt extreme Lösungen wie das Whonix-Anonymous Operating System, die nur mit großem fachlichen Aufwand betrieben werden können. Für Laie gibt es jedoch ebenfalls Lösungen, die von einer DVD oder einem USB-Stick anstelle des auf dem PC installierten Betriebssystems direkt gestartet werden, wenn der

Computer hochgefahren wird. Diese Hochsicherheitsbetriebssysteme sind ausgestattet mit zertifiziert sicherer Software und lassen den Betrieb weiterer Software nicht zu. Sie geben keine privaten Daten an ChatGPT von sich aus preis. Sie verwischen alle Spuren, die Nutzer:innen und deren PCs hinterlassen könnten. Diese Hochsicherheitsbetriebssysteme sind **Tails, Discreete Linux** und **Qubes OS**:

- **Tails:** Mit der kostenlosen Live-DVD bzw. dem kostenlosen Live-USB-Stick „Tails“ (Tails steht für „The Amnesic Incognito Live System“), erhalten Anwender:innen eine hochsichere Surf-Umgebung auf Linux-Basis, die auch Edward Snowden lange Zeit genutzt hat. Für die Kommunikation mit dem Internet nutzt Tails das sichere TOR-Netzwerk. Neben Internet-Programmen und Systemtools steht auch die vollständige Opensource-Office-Lösung Libre Office zur Verfügung. Da Tails als Live-System arbeitet, ist das System beim Start von DVD schon davor geschützt, ChatGPT Daten preiszugeben. Anwender:innen können in der Live-Umgebung den „Windows-Tarnmodus“ aktivieren. In diesem Fall sieht die Umgebung wie ein Windows-System aus, sodass der Blick über die Schulter des Anwenders nicht verrät, dass er ein Hochsicherheitsbetriebssystem verwendet.

- **Qubes OS:** Bei Qubes OS handelt es sich um eine Linux-Distribution, die ebenfalls für das sichere Arbeiten im Internet ausgelegt und derzeit der Favorit von Edward Snowden ist. Qubes OS arbeitet mit einem isolierten Netzwerk und kann die verschiedenen Arbeitsbereiche voneinander trennen. Dazu können verschiedene sogenannte virtuelle Maschinen betrieben werden, die es Angreifer:innen wegen ihrer Verkapselung unmöglich machen, das ganze System zu übernehmen. ChatGPT hat damit keinerlei Möglichkeit, Daten zu sammeln. Dieses System ist nahezu übertrieben sicher, und es benötigt eine gewisse Einarbeitungszeit.

- **Discreete Linux:** Discreete Linux wird ebenfalls als Live-DVD bzw. Live-USB-Stick betrieben. Im Fokus der Distribution steht vor allem die anonyme Verwendung des Internets. Die Live-Distribution schützt Anwender:innen nicht nur vor Trojanern und anderen Angreifer:innen aus dem Internet, sondern verhindert ebenso, dass ChatGPT an Daten kommt. Dazu sind auch

Verschlüsselungstechnologien integriert sowie die Möglichkeit ein isoliertes Netzwerk aufzubauen. Es verhindert zudem Bedienungsfehler, indem es den Mitarbeitenden gar nicht erst die Möglichkeit einräumt während der Arbeit mit ChatGPT auf ein Laufwerk oder ein Intranet zuzugreifen. Dieses Hochsicherheitsbetriebssystem ist moderner als Tails und einfacher als Qubes OS, weshalb es besonders empfohlen wird, auch wenn es als Betaversion noch nicht für den produktiven Einsatz freigegeben ist. Mit dem produktiven Einsatz ist die Verwendung als Haupt-Betriebssystem für den gesamten Arbeitszeitraum gemeint.

2. Verwendung von Discreete Linux oder Tails

- Herunterladen des ISO-Abbildes unter https://www.privacy-cd.org/howto.html#get_pre bzw. https://tails.boum.org/index.de.html
- ISO-Abbild auf DVD oder USB-Stick speichern
- PC mit dieser DVD oder dem USB-Stick starten

Das Vorgehen im Detail sprengt den Umfang dieser Zusammenfassung und kann den zuständigen IT-Mitarbeitenden überlassen werden. **Für die normalen Anwender:innen ist es nur wichtig, dass sie die ihnen überlassene DVD oder den USB-Stick, der das Hochsicherheitsbetriebssystem enthält, verwenden, sobald sie planen ChatGPT zu nutzen.**

Fazit: Die Nutzung von ChatGPT mit personenbezogenen Daten ist datenschutzkonform zum jetzigen Zeitpunkt nicht möglich. Werden entsprechende technische und organisatorische Maßnahmen getroffen, ist die Nutzung von ChatGPT für andere Zwecke – ohne Nutzung personenbezogener Daten – rechtssicher möglich.