Attention Is All You Need

Christoph Krönke 2023-04-14T17:12:03

Allseits beschlagen wieder die Brillengläser. Die italienische Datenschutzbehörde, der *Garante per la protezione dei dati personali*, hat mit seiner Maßnahme vom 30. März 2023 die vorübergehende Beschränkung der Verarbeitung personenbezogener Daten von im italienischen Hoheitsgebiet ansässigen Personen durch das KI-basierte, für Endkunden bestimmte Chatbot-Programm ChatGPT gemäß Art. 58 Abs. 2 lit. f) DSGVO angeordnet. Damit und mit der daraufhin vom Anbieter OpenAI veranlassten Sperrung des Dienstes für italienische Nutzer bot sich für Medien, Politik und Wissenschaft rasch die Gelegenheit, einen Klassiker neu aufzulegen: Eine bahnbrechende, von einem Unternehmen aus San Francisco entwickelte Technologie, (zu Recht) gefeiert als Meilenstein der neueren Technikgeschichte, zerschellt am harten Beton des Brüsseler Datenschutzregimes. Während einige technikkritische Stimmen – auch schon auf dem Verfassungsblog – laut applaudieren („ChatGPT has a big privacy problem“), prügeln andere hitzig auf das vermeintlich innovationsfeindliche Datenschutzrecht ein. Doch gibt ChatGPT – bzw. vorsichtiger formuliert: was bislang öffentlich über ChatGPT bekannt ist – tatsächlich Anlass für derart fundamentale datenschutzrechtliche Bedenken im Hinblick auf generative KIs?

Eine nüchterne Betrachtung der vom italienischen *Garante* angegebenen Begründung seiner Maßnahme aus datenschutzrechtlicher Perspektive zeigt: Bei verständiger Interpretation steht das Datenschutzrecht den modernen Anwendungen generativer KI für Endkunden – einerseits – keineswegs in unvereinbarer Weise entgegen und blockiert damit auch nicht den technologischen Fortschritt. Andererseits müssen Anbieter derartiger Anwendungen durchaus Sensibilität für datenschutzrechtliche Vorgaben und Belange beweisen – sowohl beim Betrieb als auch bei der Entwicklung der Programme. Bei der Sensibilität für datenschutzrechtliche Fragen besteht speziell für ChatGPT wohl in der Tat noch ein wenig Luft nach oben.

Datenschutzrechtliche Gründe für die Maßnahme gegen ChatGPT

Im Einzelnen sind es vier (mögliche) datenschutzrechtliche Verstöße, die der *Garante* zur Begründung seiner schneidigen Maßnahme angeführt hat:

- Weder den Benutzern noch den betroffenen Personen, deren Daten von OpenAI gesammelt und über den ChatGPT-Dienst verarbeitet wurden, würden Informationen zur Verfügung gestellt.
- Es gebe keine geeignete Rechtsgrundlage für die Erhebung personenbezogener Daten und deren Verarbeitung zum Zwecke des Trainings der dem Betrieb von ChatGPT zugrunde liegenden Algorithmen.

- Die Verarbeitung personenbezogener Daten der betroffenen Personen sei insofern ungenau, als die von ChatGPT bereitgestellten Informationen nicht immer mit den tatsächlichen Daten übereinstimmen.
- Es fehle an einer Überprüfung des Alters der Nutzer des ChatGPT-Dienstes, der gemäß den von OpenAI veröffentlichten Bedingungen Personen vorbehalten ist, die mindestens 13 Jahre alt sind.

Während die letztgenannte Frage eines angemessenen Jugendschutzes nicht datenschutzspezifisch ist und daher im Folgenden ausgeblendet wird, berühren das Fehlen einer Rechtsgrundlage sowie die mangelnde Richtigkeit und Transparenz der Verarbeitung geradezu die Grundfesten des Datenschutzrechts. Alle drei datenschutzbezogenen Gründe, die der *Garante* für seine Maßnahme angeführt hat, erweisen sich bei näherer Betrachtung allerdings nicht als unüberwindbares Hindernis, das die Grundlage für eine dauerhafte Beschränkung oder gar ein Verbot des Dienstes bilden könnte – jedenfalls auf der Basis der Informationen, die zu ChatGPT bislang öffentlich verfügbar sind. Im Einzelnen ist indes durchaus differenzierte Kritik an der Ausgestaltung des Dienstes angebracht.

Funktionsweise einer generativen KI wie ChatGPT

Wichtig für die datenschutzrechtliche Beurteilung ist zunächst, sich die Funktionsweise einer generativen KI wie ChatGPT – ein Akronym für „Generative Pre-trained Transformer“, ausgestaltet als „Chat“-Programm – zumindest in groben Zügen bewusst zu machen. Die grundlegende Idee, auf der insbesondere ChatGPT beruht, ist denkbar einfach. Das Programm erzeugt („Generative“) auf der Grundlage eines Inputs (zum Beispiel einer Frage, die der Nutzer eingibt) einen Text, indem es das zu dem Input wahrscheinlich am besten passende (erste) Wort findet. Auf der Basis des Inputs und des gefundenen Wortes sucht das Programm sodann erneut nach dem nächsten (zweiten) Wort, das wahrscheinlich am besten zu dem vorherigen Text passt. Dieser Vorgang wird so lange wiederholt, bis das Programm genügend Antworttext erzeugt hat. Das jeweils am besten passende Wort bestimmt das Programm anhand der auf Datenbasis (dazu sogleich) ermittelten Wahrscheinlichkeit, mit der ein Wort auf eine bestimmte Wortfolge hin verwendet wird. Derartige Sprachmodelle funktionieren daher, in den treffenden Worten der schleswig-holsteinischen Datenschutzbeauftragten Marit Hansen, wie ein (sehr leistungsfähiger) „stochastischer Papagei“. ChatGPT ist dabei, wie der Name sagt, ein „Transformer“, folgt also einer besonders wirksamen Methode, mit der das Programm die eingegebenen Zeichenfolgen in Antworttexte übertragen kann. Konkret lenkt ein solcher Transformer die Aufmerksamkeit („attention“) bei der Verarbeitung jedes einzelnen Wortes auf bestimmte andere Ausdrücke im Text, um die verschiedenen Kontexte, in denen ein bestimmtes Wort verwendet werden kann, möglichst differenziert zu erfassen. Um die Wahrscheinlichkeiten mit Hilfe des spezifischen Aufmerksamkeitsmechanismus von ChatGPT bestimmen zu können, wurde das Sprachmodell der gegenwärtig öffentlich zugänglichen Variante in zahlreichen Schritten mittels künstlicher neuronaler Netze und mit menschlichem Feedback trainiert, auf der Grundlage eines „Pre-trainings“ mit Texten, bestehend aus rund 400 bis 500 Milliarden Wörtern, die aus online verfügbaren Quellen wie etwa Wikipedia oder digitalisierten Büchern aus dem Gutenberg-Projekt stammen.

Unterscheidung von Trainingsdaten und Betriebsdaten

Berücksichtigt man diese Funktionsweise von GPT, muss bei der datenschutzrechtlichen Bewertung des Programms ganz grundsätzlich unterschieden werden zwischen den bei den verschiedenen Trainingsschritten verarbeiteten Daten (im Folgenden: Trainingsdaten) und den diversen Inhalts- und Nutzungsdaten, die beim Betrieb des Programms von den Benutzern eingegeben bzw. erzeugt werden (im Folgenden: Betriebsdaten). Beide Datenmengen können zu ganz erheblichem Anteil auch personenbezogene Daten enthalten. So wurden beim Trainieren der KI mit öffentlich zugänglichen Daten aus dem Internet sicherlich auch vielfältige personenbezogene Daten herangezogen. Und auch bei der Nutzung von ChatGPT durch ein Unternehmen oder Einzelpersonen werden diverse Daten generiert oder erhoben, die sich bestimmten oder bestimmbaren Personen zuordnen lassen – man denke etwa an die Inhalte der Anfragen, die ein Nutzer bei der Verwendung von ChatGPT in die Eingabemaske eingibt, und an die Metadaten, die bei der Nutzung des Programms anfallen (Zeit, Ort, Häufigkeit der Nutzung usw.). Beide Datentypen – Trainings- und Betriebsdaten – werden in verschiedenen Kontexten und für unterschiedliche Zwecke erhoben und verarbeitet. Für sie gelten daher auch jeweils unterschiedliche datenschutzrechtliche Anforderungen.

Rechtsgrundlage für die Verarbeitung

Mit Blick auf die Erhebung und Verarbeitung personenbezogener Trainingsdaten bemängelte die italienische Datenschutzbehörde bereits das Fehlen einer geeigneten Rechtsgrundlage (*„RILEVATA l'assenza di idonea base giuridica in relazione alla raccolta dei dati personali e al loro trattamento per scopo di addestramento degli algoritmi sottesi al funzionamento di ChatGPT"*). Diese – gewiss entscheidungsstilbedingt – lapidare Feststellung verwundert einigermaßen, denn als Rechtsgrundlage kommt naheliegend zunächst Art. 6 Abs. 1 lit. f) DSGVO in Betracht. Dass es den berechtigten, konkret: durch die unternehmerische Freiheit (Art. 16 GRC) gedeckten Interessen eines Unternehmens entsprechen kann, Informationen zu verarbeiten, die über Veröffentlichungen im Internet gleichsam allverfügbar sind, ist im Schrifttum und in der Rechtsprechung (insbesondere des EuGH, spätestens seit der Rechtssache Google Spain aus 2014, aber auch des BGH, etwa in seinem Delisting-Urteil aus 2020) bereits seit dem Aufkommen und der Verbreitung von Suchmaschinen weitgehend anerkannt und wird nicht mehr ernstlich bestritten. Letztlich ist dies auch Ausdruck einer sich immer weiter entwickelnden Informationsgesellschaft – der EuGH hat daher in der Sache Google Spain zu Recht auch die Informationsfreiheit (Art. 11 Abs. 1 Satz 2 GRC) als legitimes Verarbeitungsinteresse in Stellung gebracht (ebenso wie 2020 der BGH). Es sollte deswegen auch mit Blick auf die Entwicklung generativer KIs durch private Unternehmen nicht mehr unter Verweis auf eine vermeintliche Allmacht informationskapitalistischer Akteure infrage gestellt werden, dass eine Verarbeitung öffentlich im Internet zugänglicher Informationen im Grundsatz der Wahrnehmung berechtigter privater und öffentlicher Interessen dienen kann. Vor

diesem Hintergrund dürfte es – im Einklang mit der Einschätzung etwa des früheren baden-württembergischen Datenschutzbeauftragten Stefan Brink – prinzipiell zulässig sein, für das Trainieren auch einer kommerziell angebotenen generativen KI auf online verfügbare Informationen mit Personenbezug zuzugreifen und diese zu verarbeiten.

Dies bedeutet nicht, dass eine Verarbeitung frei verfügbarer Daten zu Trainingszwecken in unbegrenztem Maße gestattet ist. Eine Berufung auf Art. 6 Abs. 1 lit. f) DSGVO setzt eine Abwägung der einander gegenüberstehenden Rechte und Interessen voraus, in deren Rahmen auch die Rechte der betroffenen Personen aus Art. 7 und 8 GRC berücksichtigt werden müssen. Deren Interessen sind durch Programme wie ChatGPT vor allem dann berührt, wenn die KI in Beantwortung von Nutzeranfragen im Internet vorfindliche personenbezogene Informationen zusammenträgt, miteinander verknüpft und mit der Nutzeranfrage kontextualisiert. Analog zur Rechtsprechung betreffend der Ausgabe von Suchergebnissen in Online-Suchmaschinen kann sich zwar nicht regelmäßig, wohl aber im Einzelfall durchaus ein Anspruch auf Löschung der betreffenden Daten ergeben, zumal wenn eine betroffene Person von ihrem Widerspruchsrecht nach Art. 21 Abs. 1 DSGVO Gebrauch macht und damit die Darlegungslast für das Vorliegen zwingender schutzwürdiger Gründe für die Verarbeitung dem verantwortlichen Betreiber der KI auferlegt. Eine besondere Bedeutung wurde in der Rechtsprechung zu den Suchmaschinen in diesem Zusammenhang neben der Sensibilität der Daten auch der Richtigkeit der verarbeiteten Informationen beigemessen. Ein individueller Anspruch auf Richtigstellung bzw. Löschung unrichtiger Informationen wird insbesondere dann bestehen, wenn die KI im Einzelfall falsche Darstellungen zu Personen ausgibt (dazu sogleich). Pauschal und unter Verweis auf das Fehlen einer geeigneten Rechtsgrundlage verneinen lässt sich die Zulässigkeit der Datenverarbeitung allerdings nicht.

Anders zu beurteilen ist das Trainieren der dem Betrieb von ChatGPT zugrunde liegenden Algorithmen freilich, wenn dabei nicht nur frei verfügbare Informationen benutzt werden, sondern auch Betriebsdaten, insbesondere Nutzereingaben. So wurde etwa schon vor der Maßnahme des italienischen *Garante* berichtet, dass „Textbeispiele von ChatGPT“ mitunter Ähnlichkeiten zu „vertraulichen Unternehmensdaten“ hätten. Eine Verarbeitung von Betriebsdaten zu Trainingszwecken lässt sich in vertretbarer Weise kaum mehr auf Art. 6 Abs. 1 lit. f) DSGVO stützen – insbesondere kann die kollektive Informationsfreiheit der Nutzer nicht mehr unmittelbar bemüht werden –, sondern bedarf einer anderen, robusteren Rechtsgrundlage. Vor allem eine Einwilligung der betroffenen Nutzer gemäß Art. 6 Abs. 1 lit. a) DSGVO kommt dafür in Betracht. In der Tat sind in der Privacy Policy von OpenAI (Stand: 7. April 2023), auf die in den Terms of use (Stand: 14. März 2023) verwiesen wird, unter Ziffer 2 u.a. folgende Verarbeitungszwecke vorgesehen:

> „We may use Personal Information for the following purposes: To provide, administer, maintain, improve and/or analyze the Services; (…). We may aggregate or de-identify Personal Information and use the aggregated information to analyze the effectiveness of our Services, to improve and

> add features to our Services, to conduct research and for other similar purposes."

Ob diese Angaben und Formulierungen genügen, um eine i.S.v. Art. 4 Nr. 11 DSGVO informierte Einwilligung der betroffenen Nutzer nicht nur in die zur Erbringung der Dienste erforderliche Verarbeitung („To provide … services"), sondern auch in Verarbeitungen zur Verbesserung und Fortentwicklung („improve and add features") zu tragen, mag hier noch dahinstehen (dazu unten die Überlegungen zur Transparenz). Ganz grundsätzlich kann eine Einwilligungserklärung nach Art. 6 Abs. 1 lit. a) DSGVO aber richtigerweise durchaus die Grundlage für Datenverarbeitungen zum Zwecke des kontinuierlichen Trainings einer generativen KI wie ChatGPT bilden. Voraussetzung dafür ist dann unter dem Gesichtspunkt der Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO) und der Vertraulichkeit und Integrität (Art. 5 Abs. 1 lit. f) DSGVO) sicherlich, dass geeignete, beim Trainieren einer KI ohne Zweifel anspruchsvolle technische und organisatorische Maßnahmen (insbesondere effektive Anonymisierungstechniken, die im Sinne der Breyer-Entscheidung des EuGH eine Re-Identifizierung zwar nicht objektiv unmöglich, aber doch „praktisch nicht durchführbar" und damit wirtschaftlich unmöglich machen) getroffen werden, um die Risiken für die betroffenen Personen zu begrenzen. Eine geeignete Rechtsgrundlage ist mit der Einwilligungsmöglichkeit nach Art. 6 Abs. 1 lit. a) DSGVO jedoch prinzipiell vorhanden.

Weitergehende, hier nicht weiter thematisierbare Rechtsfragen zur Verarbeitungsgrundlage stellen sich schließlich dann, wenn ein (unternehmerisch handelnder) Nutzer die API von OpenAI im Rahmen einer Auftragsverarbeitung verwenden möchte, um selbst als Verantwortlicher personenbezogene Daten (weiter) zu verarbeiten (z.B. um Kundenbewertungen auf Bewertungsportalen automatisiert beantworten zu lassen). Für diesen Fall hält OpenAI ein gesondertes Data Processing Addendum vor.

Richtigkeit der Daten

Soweit die Richtigkeit der verarbeiteten Daten die Zulässigkeit des „Ob" der Verarbeitung betrifft, überschneiden sich die Maßstäbe teilweise mit dem Grundsatz der Datenrichtigkeit gemäß Art. 5 Abs. 1 lit. d) DSGVO, der von der italienischen Datenschutzbehörde ebenfalls gesondert gerügt wurde („RILEVATO che il trattamento di dati personali degli interessati risulta inesatto in quanto le informazioni fornite da ChatGPT non sempre corrispondono al dato reale"). Die Beanstandung von ChatGPT erscheint insoweit zunächst intuitiv plausibel und nahbereichsempirisch gestützt. Den Verfasser dieser Zeilen etwa gibt ChatGPT (Stand: April 2023) zwar schmeichelhaft, aber unzutreffend als Professor an der Ludwig-Maximilians-Universität München aus, wo er angeblich Experte im Bereich des Zivilrechts sei, mit Schwerpunkten im Schuldrecht, Sachenrecht und Erbrecht.

In der Tat verpflichtet der Grundsatz der Datenrichtigkeit den Verantwortlichen – hier: OpenAI – prinzipiell dazu, sicherzustellen, dass die von ChatGPT generierten Ausgaben nicht auf ungeeigneten Trainingsmethoden beruhen und in der Folge falsche Mitteilungen über Tatsachen oder unrichtige Einschätzungen in Bezug auf

eine betroffene Person enthalten. Der Betreiber der Software muss dabei nicht nur dann tätig werden, wenn die betroffene Person einen Anspruch auf Berichtigung (Art. 16 Abs. 1 DSGVO) erhebt. Jedenfalls dann, wenn es um einen wirkmächtigen Dienst geht, der mit derart weitreichenden Verarbeitungen wie im Falle von Suchmaschinen oder allgemeinen generativen KIs einhergeht, muss der Betreiber – wie der EuGH mit Blick auf die Datenpflege im Ausländerzentralregister bereits im Jahr 2008 festgestellt hatte – ähnlich wie ein hoheitlich handelnder Akteur auch von sich aus tätig werden, um unrichtige Informationen unverzüglich zu löschen oder zu berichtigen. Den Verantwortlichen trifft insoweit, wie sich heute auch aus Art. 24 und Art. 25 Abs. 1 DSGVO ergibt, prinzipiell eine Organisationspflicht in Bezug auf die Gewährleistung der Richtigkeit und Aktualität verarbeiteter personenbezogener Informationen.

Könnte und müsste man die Ausgabe und Verbreitung unrichtiger personenbezogener Angaben durch einen Anbieter digitaler Dienste indes ohne Weiteres zum Anlass nehmen, den betreffenden Dienst dauerhaft zu beschränken oder zu verbieten, müsste man praktisch sämtliche Online-Plattformen und insbesondere wiederum die großen Suchmaschinen unverzüglich vom Netz nehmen. Dass dies weder zweckmäßig noch rechtlich geboten ist, liegt auf der Hand. Ein angemessener datenschutzrechtlicher Umgang mit der Verbreitung unrichtiger personenbezogener Daten durch digitale Dienste verlangt vielmehr nach der Entwicklung maßvoller Organisationspflichten der Betreiber zur Gewährleistung der Richtigkeit verarbeiteter personenbezogener Informationen, wie sie beispielsweise der BGH bereits 2013 in seinem (inhaltlich mittlerweile gewiss fortgeschriebenen) Autocomplete-Urteil geleistet hatte. In jener Entscheidung machte der BGH eine Haftung des Suchmaschinenbetreibers Google für persönlichkeitsrechtsverletzende Suchergänzungsvorschläge (die sog. „Autocomplete“-Funktion) von der Verletzung einer Überwachungspflicht abhängig, deren Inhalt und Reichweite er grundrechtsgeleitet nach Maßgabe von Zumutbarkeitsgesichtspunkten bestimmte. Dieser Grundgedanke der BGH-Entscheidung lässt sich auch auf die Beurteilung von innovativen generativen KIs wie ChatGPT übertragen, die auch technisch durchaus Parallelen zu der Autocomplete-Funktion aufweisen („Autocomplete reloaded“). Von vornherein ausschließen lassen sich Unrichtigkeiten bei der Wiedergabe personenbezogener Informationen mittels generativer KI demnach vernünftigerweise nicht, zumal es sich ganz überwiegend um ersichtlich experimentelle Anwendungen handelt. Anders als die Betreiber von klar auf informationelle Verlässlichkeit ausgelegten Suchmaschinen kommuniziert OpenAI dies auch nicht, sondern hebt sehr deutlich als die „Limitations“ von ChatGPT hervor:

> „May occasionally generate incorrect information – May occasionally produce harmful instructions or biased content – Limited knowledge of world and events after 2021“.

Dem Empfänger der verarbeiteten Daten muss damit klar sein: Die ausgegebenen Informationen erheben keinen unbedingten Richtigkeitsanspruch, sondern sollten stets gesondert auf ihre Richtigkeit und Aktualität überprüft werden. Wenn und soweit der Betreiber daneben auch ein System vorhält, das im Einklang mit Art.

16 Abs. 1 DSGVO eine hinreichend effektive Bearbeitung von Meldungen und die zeitnahe Korrektur von Unrichtigkeiten ermöglicht, ist der Grundsatz der Datenrichtigkeit kein unüberwindbares Hindernis für Dienste wie ChatGPT. Allein vor diesem Hintergrund erscheint der Verweis des italienischen *Garante* auf Art. 5 Abs. 1 lit. d) DSGVO deutlich überzogen.

Informationspflichten

Es bleibt als dritter Grund für die angeordnete Beschränkung der Datenverarbeitung die mangelnde Bereitstellung hinreichender Informationen sowohl für die Nutzer von ChatGPT – in Bezug auf die Verarbeitung der Betriebsdaten – als auch für die sonst betroffenen Nicht-Nutzer – in Bezug auf die Erhebung und Weiterverarbeitung von Trainingsdaten (*„RILEVATO, da una verifica effettuata in merito, che non viene fornita alcuna informativa agli utenti, né agli interessati i cui dati sono stati raccolti da OpenAI, L.L.C. e trattati tramite il servizio di ChatGPT“*). In dieser Hinsicht geben speziell die Dienste von OpenAI gegenwärtig in der Tat noch Anlass zu datenschutzrechtlicher Kritik.

Zu differenzieren ist hier erneut zwischen der Verarbeitung von Trainingsdaten und der Verarbeitung von Betriebsdaten. Für die Verarbeitung frei verfügbarer personenbezogener Informationen zu Trainingszwecken dürften regelmäßig Art. 12 und Art. 14 DSGVO maßgeblich sein. Der Verantwortliche muss demnach i.S.v. Art. 12 Abs. 1 DSGVO „geeignete Maßnahmen“ treffen, um den Betroffenen Informationen u.a. bezüglich der Verarbeitungszwecke mitzuteilen, Art. 14 Abs. 1 DSGVO. Dabei genügen in digitalen Umgebungen – wie etwa die Artikel-29-Datenschutzgruppe in ihrem WP 160 zu Transparenz herausgearbeitet hat – prinzipiell auch abstrakt-generelle Darstellungen in leicht auffindbaren Datenschutz- oder Transparenzrichtlinien, ggfs. in angemessen abgeschichteter Form. Eine individualisierte oder gar aktiv vom Betreiber eines digitalen Dienstes an den einzelnen betroffenen Nicht-Nutzer gerichtete Kommunikation ist nicht erforderlich (und wäre praktisch auch kaum durchführbar).

Selbst in Anbetracht dieser vergleichsweise großzügigen Maßstäbe erscheinen die Informationen, die OpenAI als der Anbieter von ChatGPT zur Verfügung stellt, gegenwärtig nicht zureichend. Die zitierte Privacy Policy betrifft lediglich die Verarbeitung von Betriebsdaten, nicht die online frei verfügbaren personenbezogenen Daten. An einer entsprechend ausdifferenzierten Datenschutzerklärung, wie sie beispielsweise Google auch mit Blick auf die Verarbeitung von Informationen in Bezug auf Nicht-Nutzer bereitstellt, fehlt es derzeit. Leistbar ist die Bereitstellung der erforderlichen Informationen natürlich allemal – sofern Wille und Sorgfalt vorhanden sind.

Strenger zu beurteilen sind demgegenüber richtigerweise die Informationen, die den Nutzern generativer KIs gemäß Art. 13 DSGVO in Bezug auf die Verarbeitung ihrer Inhalts- und Nutzungsdaten bereitgestellt werden müssen, wenn und soweit auf ihrer Basis eine Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO erteilt werden soll. Speziell bei einwilligungsbasierten Verarbeitungen ist zu berücksichtigen, dass die bereitgestellten Informationen essenzielle Bedeutung für die Willensbildung seitens

des Betroffenen haben und ein allzu großzügiger Maßstab bei der Beurteilung der Informationsbasis im Ergebnis dazu führen kann, dass mit der daraufhin erteilten Einwilligung praktisch jede Datenverarbeitung legalisiert werden kann. Die Informationspflichten des Verantwortlichen im Kontext einer Einwilligung sollten daher grundsätzlich anspruchsvoll interpretiert werden; überdies sollte die Bereitstellung nur unzureichender Informationen auf Rechtsfolgenseite den Wegfall einer tragfähigen Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO zur Konsequenz haben – mithin also besonders einschneidend für den Verantwortlichen sein.

Vor diesem Hintergrund erscheinen auch die oben zitierten Informationen, die den Nutzern von ChatGPT in der Privacy Policy (Stand: 7. April 2023) von OpenAI zur Verfügung gestellt werden, als gegenwärtig wohl noch zu weit gefasst, um eine ausreichende Basis für eine informierte Einwilligung in die Verarbeitung zu bilden. Die deutschen Zivilgerichte haben in den vergangenen Jahren vor allem zu weit gefasste Zweckbestimmungen in Bezug auf umfassende Datenverarbeitungen mehrfach für unwirksam erklärt. Passend zu den von OpenAI in der Privacy Policy verwendeten Formulierungen wurden in der Rechtsprechung etwa Einwilligungsklauseln für unzulässig erachtet, wonach erhobene Daten dazu verwendet würden, die „Produkte, Dienste, Inhalte und Werbung zu entwickeln, anzubieten und zu verbessern“, ohne dabei anzugeben, „welche der vom Verbraucher erhobenen Daten genutzt werden und wie dies im Einzelnen erfolgen soll“ (so etwa das LG Berlin mit Blick auf Bestimmungen in den AGB der irischen Apple-Tochter). Aufgrund dieser Maßgaben ist bei einer beabsichtigten Verarbeitung von personenbezogenen Daten durch generative KI-Systeme, die typischerweise auf eine möglichst umfassende Verwertung möglichst vieler Informationen abzielt, sorgfältig auf eine möglichst präzise Zweckbestimmung zu achten. Eine datenschutzrechtssichere Formulierung entsprechender Einwilligungserklärungen ist zwar sicherlich anspruchsvoll, mit entsprechender Mühe und Rücksicht auf die Architektur des Sprachmodells aber zweifelsohne leistbar. In dieser Hinsicht dürfte OpenAI noch nachbessern müssen – aber auch können.

Bei der Entwicklung der Maßstäbe für hinreichend transparent und verständlich gestaltete Informationen für Betroffene muss im Einzelnen freilich bedacht werden: Die Gewährleistung transparent generierter, zumindest erklärbarer Outputs von KI-Systemen und die Herleitung darauf bezogener konkreter Transparenz- und Informationsanforderungen übersteigt den Regelungsanspruch des Datenschutzrechts letztlich sehr deutlich. Auf sie zielen andere, spezifischere Regulierungsinstrumente ab – etwa der Digital Services Act (DSA), der für Vermittlungsdienste mit komplexen Sortier- und Moderationsalgorithmen u.a. Transparenzberichtspflichten statuiert, und der ins Werk gesetzte AI Act, der die Grundlagen für ein allgemeines KI-Produktsicherheitsrecht legen soll. Die Herstellung umfassender KI-Transparenz qua Datenschutzrechts erscheint daher von vornherein als überambitioniert und überdehnt damit auch das Mandat der Datenschutzbehörden.

“Attention is all you need”

Zusammenfassend wird man festhalten dürfen: Der *Garante per la protezione dei dati personali* hat mit seiner Maßnahme zwar auf kritische Punkte hingewiesen, die bei der datenschutzrechtskonformen Ausgestaltung generativer KI-Dienste für Endkunden wie ChatGPT beachtet werden müssen – und von OpenAI zum Teil tatsächlich vernachlässigt wurden. Insgesamt ist er mit der ansatzlosen und rigorosen Anordnung der vorübergehenden Beschränkung der Verarbeitung aber über das Ziel hinausgeschossen, da aus datenschutzrechtlicher Sicht keine unüberwindbaren Hindernisse für einen rechtskonformen Betrieb bestehen, die nicht auch durch mildere, deutlich grundrechtsschonendere Aufsichtsmaßnahmen (z.B. im Wege der informellen Beratung oder einer Warnung, Art. 58 Abs. 2 lit. a) DSGVO) hätten ausgeräumt werden können – auch unter Berücksichtigung der Interessen betroffener Personen. Es bleibt zu hoffen, dass andere Aufsichtsbehörden diesem Beispiel nicht folgen.

Für die Anbieter von Programmen wie ChatGPT gilt in der Gesamtschau: Datenschutzrechtliche Sorgfalt und Aufmerksamkeit lohnen sich. Die Ansprüche des europäischen Datenschutzrechts sind durchweg erfüllbar, verlangen aber sowohl beim Betrieb als auch bereits bei der Entwicklung innovativer KI-Produkte entsprechende Anstrengungen. Es gilt damit, in Anlehnung an den von den Schöpfern des Transformer-Modells ausgegebenen Leitsatz, auch in datenschutzrechtlicher Hinsicht: „Attention is all you need“.
