GDV Gesamtverband der Versicherer

POSITIONSPAPIER

Positionspapier

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
ID-Nummer 6437280268-55

zu Basismodellen und Generativer KI für die Trilogverhandlungen zum AI Act

Einleitung

Generative KI entwickelt sich rasant und ist in den vergangenen Monaten vor allem durch die leichte Verfügbarkeit von ChatGPT sehr stark in die mediale Wahrnehmung und gesellschaftspolitische Diskussion gelangt. Kaum ein Tag, an dem nicht offene Briefe, Forderungen nach einem Moratorium, Berichte über Chancen, Risiken und Ängste vor dieser Technologie die Debatten weiter befeuern. Während die Meinungen auseinandergehen, ob es sich bei generativer KI um einen Hype handelt oder sich ein wirklicher Paradigmenwechsel ankündigt, erarbeitet Europa die weltweit erste Regulierung der künstlichen Intelligenz.

Auch die Versicherungswirtschaft beschäftigt sich intensiv mit dem Thema Künstliche Intelligenz. Nicht erst seit dem Aufkommen von ChatGPT, sondern bereits seit einigen Jahren werden verschiedene KI-Systeme eingesetzt. Angefangen von Machine Learning Algorithmen für die Bilderkennung über Natural Language Processing beim Entwickeln von Sprachassistenten bis hin zu automatischer Bearbeitung von Schadenmeldungen, sind die Einsatzbereiche vielfältig. Während es sich

GDV

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, D-10002 Berlin
Telefon: +49 30 2020-5000 · Telefax: +49 30 2020-6000

Rue du Champ de Mars 23, B-1050 Brüssel
Telefon: +32 2 28247-30 · Telefax: +49 30 2020-6140
ID-Nummer 6437280268-55
www.gdv.de

Ansprechpartner
Koordinierungsstelle Digitalisierung

E-Mail
digitalisierung@gdv.de

hierbei zum Großteil um Modelle handelte, die einen vorher festgelegten Zweck verfolgten, steigt nun auch bei vielen Versicherern das Interesse an der Nutzung von generativer KI, die für breite Zwecke eingesetzt werden kann. Das Profitieren von generativen KI-Modellen wird für die europäischen Versicherer im internationalen Wettbewerb um innovative Produkte und Lösungen sowie exzellentem Kundenservice entscheidend sein. Generative KI hat das Potenzial, in nahezu jeder Branche Anwendung zu finden, in der große Datenmengen verarbeitet werden und komplexe Entscheidungen getroffen werden müssen. Wird es Unternehmen schwer gemacht, generative KI-Systeme und Basismodelle einzusetzen, werden diese einen erheblichen Wettbewerbsnachteil gegenüber außereuropäischen Unternehmen und Märkten erleiden.

Versicherer in der KI-Wertschöpfungskette und das Ökosystem der Basismodelle

Bisher existieren auf dem Markt einzelne große Basismodelle, wie zbsp. GPT-3.5 von OpenAI (das bekannte ChatGPT), LLaMA von Meta oder PaLM 2 von Google. Die Entwicklung dieser Modelle ist sehr anspruchsvoll und ressourcenintensiv: es werden enorme Mengen an Daten, Rechenleistung, Zeit, Energie und finanzielle Mittel benötigt.

Somit ist es einerseits wahrscheinlich, dass es mittel- bis langfristig einige wenige, große Basismodelle geben wird, die sich als systemisch relevant im KI-Ökosystem in dem Sinne etablieren, als dass unendlich viele weitere KI-Anwendungen branchenübergreifend auf ihnen basieren werden. Andererseits wird vermutlich kein Versicherungsunternehmen ursprünglicher Entwickler (so genannter „Upstream-Provider“) eines Basismodells werden. Dennoch können Versicherer laut EP-Vorschlag rechtlich zum Anbieter eines Basismodells in der Rolle des „Downstream-Providers“[1] werden, z. B., wenn sie ein vorhandenes Modell in hochriskanten Kontexten einsetzen. Dies wird auf zwei Arten erfolgen: entweder über eine Programmierschnittstelle (API) oder durch die Nutzung und Weiterentwicklung von Open Source Geschäftsmodellen (siehe auch Erwägungsgrund 60 des EP-Vorschlags). Das wird davon abhängen, welches Erlösmodell der jeweilige Anbieter vorsieht, und ist mit verschieden großen Gestaltungsmöglichkeiten durch den Nutzer bzw. Downstream-Provider verbunden. Der entscheidende Punkt ist:

Versicherer können zum Anbieter von Basismodellen werden

Und damit könnten die Regelungen für die Anbieter von Basismodellen, die vom EP und Rat vorgeschlagen werden, durchaus auch auf

[1] Im EP-Vorschlag werden die Entwickler (Anbieter) von Basismodellen als „Upstream-Provider“, und die Akteure (Nutzer) in der Wertschöpfungskette, die das Modell weiterverwenden, als „Downstream-Provider“ bezeichnet.

Versicherungsunternehmen anwendbar sein, die generative KI-Modelle und Basismodelle komplett oder als Teil ihrer KI-Landschaft verwenden möchten.

Regulatorische Herausforderungen

Die deutsche Versicherungswirtschaft begrüßt den grundsätzlichen Ansatz des europäischen Gesetzgebers, eine Regelung für diesen wichtigen Bereich von Künstlicher Intelligenz zu erlassen. Diese gibt Unternehmen einen verbindlichen Rechtsrahmen für den Einsatz dieser Systeme und somit Rechtssicherheit und schafft gleichzeitig Vertrauen für die Verbraucher, sie darf jedoch nicht zu Wettbewerbsnachteilen oder einem weiteren Bürokratieoverhead führen.

Während die Kommission in ihrem Vorschlag noch keine gesonderten Regelungen für generative KI-Systeme bzw. Basismodelle vorgesehen hat, schlagen das Europäische Parlament (EP) und der Rat entsprechende Vorschriften vor. Diese zusätzliche Ebene ist zu begrüßen, da sie auf die Besonderheiten von Basismodellen und generativer KI eingeht. Der Kommissionsvorschlag von 2021 verfolgt noch einen Use Case bezogenen Ansatz, der annimmt, dass KI-Systeme nur nach einem vorher festgelegten Zweck eingesetzt werden. Die Vorschläge von Rat und EP berücksichtigen hingegen die neuen technologischen Entwicklungen und setzen an der Wertschöpfungskette von KI-Systemen an. Die Verantwortlichkeiten werden hierbei gleichmäßig unter den Akteuren verteilt. Sie wählten jedoch unterschiedliche Schwerpunkte in ihren Ansätzen:

Der Rat spricht in seinem Vorschlag von „KI-Systemen mit allgemeinem Verwendungszweck“ und definiert diese als „KI-System, das (…) vom Anbieter dazu vorgesehen ist, allgemein anwendbare Funktionen wie Bild- oder Spracherkennung, Audio- und Videogenerierung, Mustererkennung, Beantwortung von Fragen, Übersetzung und Sonstiges auszuführen“ (Art. 3(1b) KI-VO). Das EP setzt hier grundlegender an und bezieht sich in seinem Vorschlag auf Basismodelle („Foundation Models“). In diesem Verständnis ist ein Basismodell ein „KI-Systemmodell, das auf einer breiten Datenbasis trainiert wurde, auf eine allgemeine Ausgabe ausgelegt ist und an eine breite Palette unterschiedlicher Aufgaben angepasst werden kann“ (Art. 3(1c) KI-VO).

Beide Vorschläge ordnen generative KI-Systeme bzw. Basismodelle nicht per se als hochriskant nach Annex III ein, was zu begrüßen ist. Jedoch sind die vorgeschlagenen Anforderungen an Compliance zu umfangreich - besonders im neuen EP-Artikel 28 b, durch z.B. Maßnahmen zur Datenverwaltung, Vorgaben für die Energienutzung, Anforderungen an die technische Dokumentation und die Einhaltung bestimmter Transparenzanforderungen, die in Artikel 52 Abs. 1 des EP-Vorschlags konkretisiert werden. **Bei strenger Auslegung unterliegt der Einsatz dieser Modelle damit so hohen Anforderungen, dass man den Eindruck**

gewinnt, der risiko-basierte Ansatz der KI-VO wird hier außer Acht gelassen und die hochriskante Einordnung von Basismodellen erfolgt durch die Hintertür.

Gerade bei der Regulierung dieses speziellen Teilbereichs von KI, die einen sehr breiten Anwendungsbereich und großen wirtschaftlichen Einfluss haben wird, ist es umso wichtiger, dass die Nutzung und der Zugang zu dieser Technologie Unternehmen aller Größen ermöglicht wird und auch die zukünftige Entwicklung von neuen innovativen Modellen in Europa nicht verhindert wird – sondern gefördert.

Im Einzelnen sollte die künftige Regulierung folgende Punkte berücksichtigen:

Regulierung mit Augenmaß und Fairness

Auch wenn generative KI-Anwendungen, Large Language Models und ChatGPT große mediale Aufmerksamkeit erlangt haben, sollte der Gesetzgeber diesen wichtigen Bereich mit der erforderlichen Ruhe und der nötigen Zeit regeln.

Wichtig ist es, die Folgen der zukünftigen Regelung genau abschätzen zu können. **Eine Folgenabschätzung wäre an dieser Stelle ein wichtiges Instrument gewesen, um die Auswirkungen der künftigen Regelung verlässlich beurteilen zu können.** Eine übereilte Regulierung nutzt niemanden, weder den Verbrauchern noch den Unternehmen.

Ebenfalls problematisch ist der Anwendungsbereich des Art. 28 b des EP-Vorschlags zu sehen, der jedes KI-Systemmodell, das auf einer breiten Datenbasis trainiert wurde, und eine breite Anzahl an Aufgaben ausführen kann, erfasst. Der Artikel 28 b in seiner jetzigen Form wendet alle enthaltenen Anforderungen proportional auf jedes KI-Systemmodell an, das dieser Definition entspricht, egal wie groß oder klein oder welchen Reifegrad es hat. Dies kann Innovationen behindern, indem es kleine Unternehmen oder Startups benachteiligt. Art. 55a Abs. 3 des Ratsvorschlags greift diesen Punkt bereits auf, und geht damit in die richtige Richtung. Dieser Ansatz sollte ausgeweitet werden. **Wir empfehlen daher einen proportionalen Ansatz, der die unterschiedlichen Voraussetzungen und Reifegrade der Systeme verschiedener Akteure berücksichtigt.** Sehr große Basismodelle würden somit besonders streng beaufsichtigt, wobei Benchmarks und Metriken für die Einordnung der Modelle noch entwickelt werden müssten. Vorstellbar wäre eine analoge Anlehnung an die „Gatekeeper“-Regelung des Digital Services Acts.

Gerechte Verteilung der Verantwortlichkeiten zwischen Anbieter und Nutzer bei Einsatz von generativen KI-Modellen in als hochriskant eingestuften Anwendungsfällen

Entscheidend wird die Verteilung der Verantwortlichkeiten zwischen Anbieter („Upstream-Provider“) und Nutzer (z. b. ein Versicherer als „Downstream-Provider“) beim Einsatz von Basismodellen bzw. KI-Systemen mit allgemeinem Verwendungszweck in hochriskanten Kontexten sein. Hier ist der Ansatz des EP-Vorschlags zu begrüßen, der die Rechte und Pflichten der Akteure auf den Bereich ihrer Verantwortlichkeit innerhalb der Wertschöpfungskette eingrenzt, und in Artikel 28 Abs. 2a vorgibt, welche Dokumentationen und Einblicke vom Upstream- an den Downstream-Provider weitergegeben werden müssen, um mit der KI-VO konform zu sein.

Ebenso sollte die Frage geklärt werden, ob Anbieter von Basismodellen die Zweckbestimmung ihrer Modelle durch den Nutzer grundsätzlich einschränken können, wie es der Rat in Art. 4c vorsieht.

Laut Art. 28 Abs. 1 (b a) des EP-Vorschlags wird ein Nutzer zum Anbieter von Basismodellen, wenn er es derart verändert, dass es unter den hochriskanten Anwendungsbereich nach Art. 6 fällt. In den Fällen, in denen der Nutzer zum Anbieter wird, ist es erforderlich, dass er seine sich daraus ergebenden Verpflichtungen erfüllen kann. **Eine entsprechende Regelung sieht Art. 4 b Abs. 5 der Allgemeinen Ausrichtung des Rates sowie Art. 28 Abs. 2e des EP-Vorschlags bereits vor. Dies ist zu begrüßen, da beide Vorschläge dafür sorgen, dass der Nutzer seine Anforderungen erfüllen kann. Eine Regelung in diesem Sinne sollte in jedem Fall im Gesetzestext enthalten sein.**

Anforderungen an die Data-Governance müssen umsetzbar sein (Art. 28b Abs. 2 lit. b)

Der Vorschlag des EP sieht in Art. 28 b Abs. 2b vor, dass der Anbieter eines Basismodells nur Datensätze verarbeiten und einbeziehen darf, die angemessenen Data-Governance-Maßnahmen für Basismodelle unterliegen, „insbesondere Maßnahmen zur Prüfung der Eignung der Datenquellen, möglicher Verzerrungen und geeigneter Abhilfemaßnahmen“. Um Verzerrungen zuverlässig aufzudecken, muss auch die Überprüfung anhand von Echtdaten zulässig sein. Insoweit sollte Art. 10 Abs. 5, der die Verwendung von Echtdaten zur Vermeidung von Verzerrungen erlaubt, mindestens in der Fassung des Kommissionsentwurfs und des Vorschlags des Rates beibehalten werden.

Damit der gesetzgeberische Zweck des Art. 28b Abs 2b des EP-Vorschlags erfüllt werden kann, sollte darüber hinaus Art. 10 Abs. 5 des Kommissionsentwurfs in zweifacher Hinsicht ausgeweitet werden: Erstens sollte die Überprüfung anhand

von Echtdaten nicht nur zum Aufdecken von Verzerrungen, sondern auch zur Prüfung der generellen Eignung der Datenquellen möglich sein. Zweitens sollte die Erlaubnis zum Einsatz von Echtdaten nicht auf hochriskante KI-Systeme beschränkt sein, da generative KI nach dem EP-Vorschlag nicht per se als hochriskant eingestuft wird.

Zudem sollte Art. 28b (2b) die Besonderheiten der Entwicklung von Basismodellen berücksichtigen. Für das so genannte „pre-training" von Basismodellen werden sehr große Datenmengen benötigt. Allein für das Training von GPT-3 des Anbieters OpenAI wurden 570 Gigabyte an reinen Textdateien verarbeitet. Diese Daten alle vorab auf angemessene Data Governance zu prüfen ist nahezu unmöglich und kann bei strenger Auslegung einem Verbot von Basismodellen gleichkommen. Es gibt aktuell viele Bestrebungen, die Datenqualität und Transparenz für Basismodelle zu verbessern, allerdings noch keinen einheitlichen etablierten Standard. Besser wäre es hier auf so genannte „Embeddings" zu setzen, welche, einfach ausgedrückt, der Ausgabe einen Korridor vorgeben, in dem sie sich bewegen darf. Das Basismodell könnte mit einem großen Datensatz trainiert werden und so seine umfassenden Fähigkeiten erwerben, wie z.B. Text- oder Bilderzeugung, und in einem zweiten Schritt wird der Ausgabekontext, der z.B. die Einhaltung der Anforderungen zur Vermeidung von Vorurteilen oder Diskriminierung sicherstellt, durch Einbettungen bereitgestellt. **Daher sollte die Anforderung so formuliert werden, dass sie sich nicht nur auf die Datensätze beim Training bezieht, sondern eine gewisse Flexibilität enthalten, um die Einhaltung der Data Governance Vorgaben bei der Ausgabe gewährleisten zu können.**

Einbeziehung von unabhängigen Experten als Vorschlag des EP

Es wird sich wohl erst in Zukunft klären, ab welchem Reifegrad bzw. welcher systemischen Relevanz ein Basismodell durch internes Qualitätsmanagement ausreichen kontrolliert ist, oder wann externe Experten hinzugezogen werden sollten.

Das EP schlägt vor, dass der Anbieter bei der Erfüllung der Anforderungen nach Art. 28 b Abs. 2 a und c einen unabhängigen Experten hinzuziehen kann. Dies sollte in keinem Fall verpflichtend vorgeschrieben werden. Es sollten vielmehr Kriterien festgelegt werden, ab welcher Größe die Prüfung eines Basismodell durch externe, unabhängige Experten notwendig ist. Hierbei ist zu befürchten, dass es zu Engpässen und Kostenexplosionen kommt, da der Bedarf an Experten nicht schnell genug vom Markt gedeckt werden kann. Zudem entsteht auch ein Risiko bei der Wahrung von Geschäftsgeheimnissen, sollten unabhängige Experten bei verschiedenen Firmen tiefe Einblicke in die Funktionsweise der Modelle erhalten.

Zudem hat sich die Kommission grundsätzlich dafür entschieden, dass die Anbieter in eigener Verantwortung prüfen können, ob die von Ihnen auf den Markt zu bringenden KI-Systeme den regulatorischen Anforderungen genügen. Die nun

vom EP vorgesehene Hinzuziehung von externen Experten steht diesem Ansatz entgegen. Auch wenn die Hinzuziehung von externem Sachverstand zurzeit noch nicht obligatorisch ist, könnte man es so verstehen, dass den Unternehmen nicht genügend eigener Sachverstand zugetraut wird. Das ist ein falsches Signal. **Daher sollte der Bezug auf externe Sachverständige nur für sehr große Basismodelle empfohlen werden.**

Berücksichtigung der Besonderheiten von Open-Source-Software

Eine weitere dringende Frage ist, wie die Nutzung von Open-Source-Modellen reguliert wird, die keinen kommerziellen Anbieter haben. Das EP macht in seinem Vorschlag keinen Unterschied zwischen kommerziell angebotenen Basismodellen oder solchen, die unter einer Open-Source-Lizenz zur Verfügung gestellt werden. Daher stellt sich die Frage, ob bzw. ab welchem Reifegrad quelloffene Basismodelle der KI-Verordnung unterliegen.

Wie oben beschrieben, sollte bei der Anwendung der Verordnung auf Relevanz und Reifegrad des Modells geachtet werden. Auch in der Versicherungswirtschaft wird, wie in allen anderen Branchen auch, mit Open Source Anwendungen gearbeitet. Besonders im KI-Bereich hat die Open Source Community durch die Weiterentwicklung freier Modelle einige Innovationen, wie z. B. Low Rank Adaptation (LoRA), hervorgebracht. Vor diesem Hintergrund sollte die künftige Regulierung keine unnötigen Hürden für die Open Source Entwickler in Europa enthalten.

Aus unserer Sicht ist beim Anwendungsbereich der Verordnung eine klare Unterscheidung zwischen Entwicklern von Open-Source-Basismodellen und Anbietern, die Open-Source- Basismodelle kommerziell verfügbar machen, zu treffen. Für KI-Komponenten, die frei und quelloffen verfügbar sind, sollte auch im Fall einer kommerziellen Nutzung der Entwickler nicht verantwortlich sein. Der Vorschlag des EP in Art. 2 Abs. 5e ist daher zu begrüßen, allerdings sollte er auch auf Basismodelle ausgeweitet werden.