Stellungnahme des Deutschen Caritasverbands

zu den Verordnungsvorschlägen der EU-Kommission für ein Digital-Omnibus-Paket zu Daten (2025/0360) und Künstlicher Intelligenz (2025/0359)

EU-Vertretung des Deutschen Caritasverbandes
Rue de Pascale 4-6
B-1040 Brüssel
Telefon-Zentrale +32 2 230 45 00
Telefon-Zentrale +49 761 200 700
www.caritas.de

Ihr Ansprechpartner
Tobias Kutschka
Referent für EU-Förderpolitik
und Digitalpolitik
Telefon: +49 761 200 702
tobias.kutschka@caritas.de

Datum 25.02.2026

Der Deutsche Caritasverband e.V. (DCV) begrüßt das Ziel der EU-Kommission, Digitalgesetze zu vereinfachen und Organisationen damit die Einhaltung der Gesetze zu erleichtern. Die Verbände der Caritas sind wichtige Säulen der sozialen Infrastruktur in Deutschland und unterstützen den Ansatz des Draghi-Berichts, Produktivitätswachstum mit starker sozialer Inklusion zu verbinden[1].

Der DCV vertritt die Belange von deutschlandweit rund 25.000 Einrichtungen und Diensten mit 740.000 Beschäftigten und mehreren hunderttausend ehrenamtlich Engagierten. Zudem setzt sich der DCV für Anliegen der rund 12 Millionen Menschen ein, die jährlich als Klient:innen in den Einrichtungen und Diensten u.a. Unterstützung, Betreuung und Pflege erhalten.

Für den Deutschen Caritasverband sind in der Bewertung der Verordnungsvorschläge zwei Leitfragen entscheidend:

- Werden die vorgeschlagenen Änderungen den gemeinnützigen, mehrheitlich kleinen und mittelgroßen Organisationen der Caritas die digitalisierte Arbeit erleichtern?
- Werden die vorgeschlagenen Änderungen einen hohen Datenschutz und Schutz vor Diskriminierung für benachteiligte und vulnerable Personengruppen (die die Caritasverbände mit ihrer Arbeit unterstützen) gewährleisten?

[1] Siehe Draghi (2024): Die Zukunft der europäischen Wettbewerbsfähigkeit. Teil A. Eine Strategie für die Wettbewerbsfähigkeit Europas, S. 23.

Aufbau des Papiers:

Im ersten Teil werden die Kernforderungen des Deutschen Caritasverbands für den Digitalomnibus zu Daten und KI vorgestellt. Anschließend, in Teil II, zeigt das Papier ausführlich Forderungen des DCVs für den Datenschutz und die Datennutzung auf: Artikel des Kommissionsvorschlags, die wir befürworten, konkrete Änderungsvorschläge für andere Artikel, sowie Forderungen, die über den Omnibusvorschlag der EU-Kommission hinausgehen. Teil III des Papiers beinhaltet Caritas-Forderungen für KI-Nutzung und -Schutz, ebenfalls mit Artikeln, die der DCV unterstützt, sowie mit Änderungsvorschlägen für einzelne Artikel des Kommissionvorschlags zur Änderung der KI VO.

Teil I

Die Kernforderungen des DCVs für den Digital-Omnibus zu Daten (2025/0360) sind:

(unten finden Sie die konkreten Änderungsvorschläge für die Gesetzestexte)

1. **Klare Vorgaben, Bündelung der Regeln und Zuständigkeiten.**

   Verschiedene EU-Gesetze (wie die Open-Data-Richtlinie oder die Daten-Governance-Verordnung), in dem Datengesetz passend zusammenzuführen wäre eine Vereinfachung für Träger. Die Einrichtung der ENISA als zentrale Meldestelle für Cybersicherheitsvorfälle ist hilfreich. An vielen Stellen würde der Verordnungsvorschlag der EU-Kommission allerdings vor allem durch neue subjektivere Formulierungen für Unsicherheiten sorgen. Es gilt aber: Je übersichtlicher und klarer anwendbar die Gesetze sind, desto mehr profitieren kleinere Organisationen. Die Co-Gesetzgeber müssen daher an jeglichen Stellen der Verordnungen sicherstellen, dass die Formulierungen und Vorgaben klar sind, und sich zudem nicht mit anderen Gesetzen aus dem Digitalgesetzbesitzstand der EU widersprechen.

   (siehe Art. 6 Nr. 1 Digital-Omnibus-VO-Vorschlag/ Art. 23a NIS-2-RL)

2. **Personenbezogene Daten und Privatsphäre schützen, Art. 3 Nr. 1a entfernen.**

   Das Niveau des Datenschutzes und des Schutzes der Privatsphäre muss hoch bleiben. Der Vorschlag, bestimmte (pseudonymisierte) personenbezogene Daten nicht mehr als

personenbezogene Daten zu behandeln, sofern eine Rückidentifizierung unwahrscheinlich ist, führt für viele Träger zu großer Unsicherheit, was die einfache Datennutzung verhindert. Wir fürchten deswegen, dass dieser relative Personenbezug kleinen, gemeinnützigen Trägern nicht entscheidend hilft, sondern nur mehr Unklarheit schafft. Auch für Klient:innen als Datensubjekte, deren sensiblen personenbezogenen Daten verarbeitet werden, entstünden keine nennenswerten Vorteile. Im Gegenteil, sie müssten darauf vertrauen, dass alle verantwortlichen Akteur:innen ihre personenbezogenen Daten besonders in den Datenwertschöpfungsketten online schlicht nicht rückidentifizieren können. Art. 3 Nr. 1a des Digital-Omnibus-VO-Vorschlag sollte gelöscht werden.

(siehe Art. 3 Nr. 1 Digital-Omnibus-VO-Vorschlag/ Art. 4 Nr. 1 DSGVO; Art. 3 Nr. 10 Digital-Omnibus-VO-Vorschlag / Art. 41a DSGVO)

3. Mehr (Rechts)Sicherheit über Pflichten durch „Umsetzungslisten".

Ein hilfreicher Vorschlag sind die Durchführungsrechtsakte auf Grundlage von Listen des Europäischen Datenschutzausschusses über Verarbeitungstätigkeiten, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, oder nicht durchzuführen ist. Sofern die EU-Kommission die Expertise des Ausschusses berücksichtigt und diese Listen regelmäßig erneuert werden, kann dies eine enorme Arbeitserleichterung für kleine und mittelgroße Träger der Caritas darstellen. Diese Form der Unterstützung sollte auch auf andere Anforderungen der DSGVO erweitert werden, z.B. welche Pseudonymisierungsverfahren dem aktuellen Stand entsprechen, oder welche Anonymisierungsverfahren best-practice entsprechen.

(siehe Art. 3 Nr. 9 Digital-Omnibus-VO-Vorschlag/ Art. 35 DSGVO)

4. Ein freiwilliges Zertifizierungssystem für DSGVO-konforme Produkte und Dienste.

Ähnlich dem Zertifizierungssystem der ENISA für die Cybersicherheit, sollten der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftrage den Auftrag erhalten, IKT-Produkte und Dienste update-sicher, kostenfrei und für Anbieter freiwillig auf ihre DSGVO-Vereinbarkeit hin zu prüfen und zu zertifizieren. Nicht nur die Organisationen der Caritas, auch alle KMUs könnten von dieser Zertifizierung bei der Auswahl der von ihnen genutzten Produkte und Dienste sowie der erhöhten Rechtssicherheit

profitieren – sie müssten nicht länger aufwendig selbst prüfen, wie z.B. im Fall von Auftragsdatenverarbeitungen.

(siehe Art. 42 und 43 DSGVO und Titel III des Cybersicherheitsgesetzes)

Die Kernforderungen des DCVs für den Digital-Omnibus zu KI (2025/0359) sind:

(unten finden Sie die konkreten Änderungsvorschläge für die Gesetzestexte)

1. **Fristverschiebungen verhindern.**

   Die Regeln der KI-Verordnung für Hochrisiko-KI-Systeme sind sowohl für Träger als auch zum Schutz der oftmals benachteiligten und vulnerablen Klient:innengruppen wichtig. Die Einhaltung der Umsetzungsfristen muss oberste politische Priorität sein, d.h. die nötigen Standards und Normen müssen schnellstmöglich erarbeitet werden. Wenn eine Fristverlängerung unter keinen Umständen abgewendet werden kann, sollte für alle Hochrisiko-KI-Systeme spätestens mit dem 2. Oktober 2027 dieselbe, feste neue Frist gelten.

   (siehe Art. 1 Nr. 31 Digital-Omnibus-KI-VO-Vorschlag/ Art. 113 Abs. 3 KI VO)

2. **Genaue Vorgaben für die Verarbeitung sensibler Daten zur Erkennung und Korrektur von Verzerrungen.**

   Die Minimierung von Verzerrungen und Diskriminierungen durch KI-Systeme ist eines der Hauptanliegen der Caritas, insbesondere bei Hochrisiko-KI-Systemen. Dass Anbieter solcher Systeme in Ausnahmen besondere Kategorien personenbezogener Daten verarbeiten dürfen, um Verzerrungen zu verhindern, ist sinnvoll. Die außerdem von der EU-Kommission vorgeschlagenen Bedingungen und die darin enthaltenden Schutzvorkehrungen für die Verarbeitung besonderer Kategorien personenbezogener Daten zur Erkennung und Korrektur von Verzerrungen müssen in den Verhandlungen des Gesetzgebungsprozesses beibehalten werden. Der Artikelvorschlag scheint von einmaligen Maßnahmen zur Korrektur auszugehen. Maßnahmen zur Minimierung von Verzerrungen sollten allerdings – wenn nötig – kontinuierlich erfolgen und die Daten jeweils wieder gelöscht werden.

   (siehe Art. 1 Nr. 5 Digital-Omnibus-KI-VO-Vorschlag / Art 4a KI VO)

3. KI-Kompetenzen wirksam stärken.

Organisationen mit der Weiterbildung ihrer Beschäftigten und ehrenamtlich Engagierten nicht alleine zu lassen ist richtig – die EU-Kommission und nationale staatliche Stellen einzubinden ist daher ein guter Vorschlag. Die Formulierungen müssen aber klarer sein und allen Akteur:innen eindeutige Vorschriften machen, Mitgliedstaaten z.B. verpflichten kostenlos zugängliche Angebote anzubieten, mit denen Grundkenntnisse über KI vermittelt werden. Arbeitgeber:innen können darauf aufbauend organisationsspezifische weitere Kompetenzen vermitteln.

(siehe Art. 1 Nr. 4 Digital-Omnibus-KI-VO-Vorschlag / Art. 4 KI VO)

Teil II

Forderungen des Deutschen Caritasverbands für eine bessere und sichere Datennutzung in der sozialen Daseinsvorsorge

Die Verbände möchten in ihren Tätigkeitsfeldern zum Wohl der Klient:innen stärker datenbasiert arbeiten und so ihre Angebote zu verbessern. In den 25.000 Einrichtungen und Diensten werden täglich große Mengen Daten verarbeitet.[2] Die Millionen Klient:innendaten z.B. in der Gesundheitshilfe, Familien-, Kinder- und Jugendhilfe, Altenhilfe, oder auch Schuldnerberatung zählen dabei oftmals zu der besonderen Kategorie personenbezogener Daten im Sinne der Datenschutzgrundverordnung (DSGVO) und sind daher zu Recht besonders schützenswert.

Die Verbände der Caritas in Deutschland sind gemeinnützig sowie größtenteils dezentral und in unabhängigen kleinen bis mittelgroßen Organisationen organisiert. Diese Strukturen ermöglichen es der Caritas überall in Deutschland gezielt die sozialen und gesundheitlichen Dienste anzubieten, die vor Ort benötigt werden. Daten im großen Stil zu aggregieren und zu nutzen ist aufgrund dieser Strukturen und der verschiedenen Tätigkeitsbereiche der einzelnen Einrichtungen und Dienste jedoch schwierig. Darüber hinaus ist es für die vielen kleinen, gemeinnützige Träger eine große Herausforderung, die Einhaltung der zahlreichen Digitalgesetze sicherzustellen. Meist verfügen die Träger über keine eigene Rechtsabteilung und nur über begrenztes Budget für externe juristische Expertise. Wichtig sind daher einheitliche gemeinsame Standards und Schnittstellen, klare rechtliche Vorgaben und Fristen, sowie umfassende, sektorspezifische Unterstützungsangebote der Behörden zur Einhaltung der Gesetze.

Wie eingangs bereits erwähnt, ist muss zeitgleich ein hohes Maß an Datenschutz und Schutz vor Diskriminierung für benachteiligte und vulnerable Personengruppen (die die Caritasverbände mit ihrer Arbeit unterstützen) gewährleisten sein.

[2] Zu beachten ist, dass der Datenschutz bei dem Deutschen Caritasverband entsprechend Art. 91 DSGVO auf der Grundlage kirchlicher Datenschutzgesetze erfolgt. Für die Caritas gilt das Gesetz über den Kirchlichen Datenschutz (KDG).

1) **Folgende Vorschläge des Digital-Omnibusses für Daten unterstützen wir:**

ENISA als zentrale Meldestelle für Cybersicherheitsvorfälle	
Omnibusvorschlag (Art. 6 Nr. 1 Digital-Omnibus-VO-Vorschlag/ Art. 23a NIS-2-Richtlinie)	**Empfehlung: beibehalten und zeitnahe Umsetzung sicherstellen**
Begründung: Meldeanforderungen zu verschlanken und die Agentur der Europäischen Union für Cybersicherheit (ENISA) zur zentralen Meldestelle für Cybersicherheitsvorfälle auszubauen unterstützen wir. Für betroffene Träger reduziert sich der bürokratische Aufwand für Meldungen, wenn die ENISA die vorgeschlagene Rolle zeitnah übernehmen kann und für Schnittstellen zu nationalen Behörden gesorgt wird.	

Durchsetzungsrechtsakte mit Listen über Verarbeitungsvorgänge, für die Datenschutzfolgeabschätzungen erforderlich oder nicht erforderlich sind	
Omnibusvorschlag (Art. 3 Nr. 9 und 10 Digital-Omnibus-VO-Vorschlag/ Art. 35 Abs. 4, 5, 6 DSGVO)	**Empfehlung: beibehalten, EDSA berücksichtigen und auf andere Vorgaben ausweiten**
Begründung: Sofern die EU-Kommission die Expertise des Europäischen Datenschutzausschusses berücksichtigt und die Listen regelmäßig erneuert werden, kann dies eine enorme Arbeitserleichterung für kleine und mittelgroße Träger der Caritas darstellen und die Rechtssicherheit wie auch den allgemeinen Datenschutz in der EU stark verbessern. Gerade aufgrund der dezentralen Organisation der Verbände müsste so nicht jeder der tausenden Träger eigenständig prüfen, wofür eine Datenschutzfolgeabschätzung durchzuführen ist. Diese Form der Unterstützung sollte auch auf andere Anforderungen der DSGVO erweitert werden. Denkbar sind z.B. ähnliche Unterstützungen, welche Pseudonymisierungsverfahren dem aktuellen Stand entsprechen oder welche Anonymisierungsverfahren genügen.	

Automatisierte und maschinenlesbare Angaben zu den Wahlentscheidungen für die Verarbeitung personenbezogener Daten	
Omnibusvorschlag (Art. 3 Nr. 15 Digital-Omnibus-VO-Vorschlag/ Art. 88b DSGVO)	**Empfehlung: beibehalten und auf Umsetzung innerhalb von 12 Monaten nach Inkrafttreten der VO hinwirken**
Begründung: Die allseits bekannte Cookie-Müdigkeit zu adressieren, ist ein guter und wichtiger Schritt. Cookie-Banner, insbesondere mit manipulativen Methoden, sind die eine Auswirkung der DSGVO, die viele Menschen täglich sehen. Sie tragen maßgeblich zum oft schlechten Ruf der DSGVO bei. Der Vorschlag in Art. 88b scheint eine geeignete Maßnahme zu sein, um Cookie-Banner überflüssig zu machen und die Datensouveränität der Nutzer:innen zu gewährleisten. Die Maßnahme muss verpflichtend sein, um wirksam zu werden. Die Ausnahme für Mediendienstanbieter wird vermutlich ein Schlupfloch für Online-Werbeanbieter, auch wenn die Absicht der EU-Kommission verständlich ist, nicht das Geschäftsmodell von (Online-)Journalismus zu gefährden. Die Erschleichung der Einwilligung in die Weiterverwendung (aller) Daten via Cookie-Banner durch viele Webseiten- und App-Betreiber:innen ist schließlich nicht nur oft lästig, sie müssen aus Sicht des DCVs auch deswegen beendet werden, da insbesondere Menschen mit geringen digitalen Kompetenzen, darunter viele Klient:innengruppen der Caritas, ausgenutzt werden. Nutzer:innen sollten die Wahl haben, ob sie der Datenverarbeitung zustimmen oder nicht. Wichtig ist daher eine zeitnahe Umsetzung des Artikels 12 Monate nach Inkrafttreten der Verordnung, nicht erst nach 24 oder 48 Monaten (siehe Abs. 5 und 7).	

2) Folgende Vereinfachungen fordern wir über die Omnibus-Vorschläge hinaus:

Die oben genannten Vorschläge in dem Digital-Omnibus-Vorschlag der EU-Kommission zu Daten würden aus Sicht des Deutschen Caritasverbands zu Vereinfachungen für die Einrichtungen und Dienste führen und haben das Potential zudem das Datenschutzniveau der Klient:innen zu erhöhen. Darüber hinaus sieht der DCV allerdings weiteren Handlungsbedarf, um gemeinnützigen Trägern (sowie KMUs und mittelgroßen Unternehmen) die Arbeit mit Daten zu erleichtern und ihre Dienste im Sinne der Klient:innen zu verbessern.

Ein freiwilliges Zertifizierungssystem für DSGVO-konforme Produkte und Dienste
Vorschlag zur Änderung der Art. 42 und 43 DSGVO
Es müssen europäische Schemata für eine Datenschutzzertifizierung geschaffen werden, nach denen offizielle Prüfungsstellen bescheinigen, dass die Datenverarbeitung der entsprechend bewerteten IKT-Produkte, -Dienste und -Prozesse im Einklang mit den Anforderungen der DSGVO erfolgt. Anbieter können ihre Produkte und Dienste freiwillig zertifizieren lassen. Die Zertifikate müssen kostenfrei EU-weit gültig sein und bei Updates aktualisiert werden. Die Rolle der Prüfstelle könnte eine Untergruppe des Europäische Datenschutzausschusses (EDSA) übernehmen. Vorbild sollte Titel III des Cybersicherheitsgesetzes (2019/881) bzw. des Kommissionsvorschlags für ein Cybersicherheitsgesetz II (2026/0011) sein, Art. 42 und 43 der DSGVO sind entsprechend zu ändern. Die Prüfungen für diese europäischen Datenschutzsiegel sollten idealerweise erfolgen, bevor die Software in den Verkehr gebracht wird (privacy by design), aber auch während des Betriebs möglich sein und bei eventuellen Updates erneuert werden. Ein solches Zertifizierungssystem böte datenverarbeitenden Organisationen eine vielfach stärkere Rechtssicherheit und eine wesentliche Vereinfachung bei der Auswahl der verwendeten IKT-Anwendungen, sowohl im eigenen Gebrauch als bei Auftragsdatenverarbeitungen nach Art. 28 DSGVO. Gleichzeitig würde der Fragmentierung der DSGVO-Umsetzung entgegengewirkt und das Funktionieren des Binnenmarkts verbessert. Profitieren würden schließlich nicht nur Organisationen der Caritas, sondern u.a. auch alle KMUs. In der Folge würde das Datenschutzniveau aller verbessert.
Begründung: Bisher entfalten die Verhaltensregeln nach Art. 40 und die Zertifizierungen im Sinne von Art. 42 und 43 DSGVO kaum entlastende Wirkung für die Träger der Caritas. Zwar bietet bspw. Art. 28 Abs. 5 DSGVO die Möglichkeit, Verhaltensregeln oder Zertifizierungen durch einen Auftragsverarbeiter für eine Auftragsdatenverarbeitung zu nutzen, um hinreichende Garantien nachzuweisen, dass „geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet“ (Art. 28 Abs. 1 DSGVO) ist.

Realität sind jedoch komplizierte Verträge, ein hoher zeitlicher Aufwand für die einzelnen Träger, große Unsicherheit und die Angst, für Fehler zu haften. Viele gemeinnützige (not-for-profit) Träger haben keine finanziellen Ressourcen für eigene Rechtsabteilungen oder umfassende externe rechtliche Unterstützung. Verlässliche Zertifikate wären eine große Vereinfachung, insbesondere zusammen mit umfassenden Unterstützungsangeboten durch die nationalen Datenschutzbehörden.

Einrichtung einer EU-Data-Servicestelle
Vorschlag für einen ergänzenden Abschnitt der DSGVO / eine Erweiterung der EHDS
Die Einrichtung einer EU-Data-Servicestelle, die vorhandene (auch nationale) Gesundheits- und Sozialdatensätze auf Anfrage anonymisiert und sie mit passenden Analysetools Organisationen und Unternehmen zur Verfügung stellt. Vorbilder für eine solche Servicestelle können Findata, die finnische Social and Health Data Permit Authority, oder EuroDaT sein.
Begründung: Die Servicestelle böte insbesondere kleineren und mittelgroßen Organisationen sowie Unternehmen wertvolle neue Möglichkeiten, datengestützte Angebote zu entwickeln, zu denen sie mit ihren eigenen Datensätzen und Tools bisher nicht in der Lage sind. Eine EU-Data-Servicestelle für Gesundheits- und Sozialdaten würde die EU zudem in ihrem Ziel einer Datenunion unterstützen, den Europäischen Gesundheitsdatenraum erweitern, sowie Wettbewerbsfähigkeit und Datensouveränität sicherzustellen.

3) Folgende Vorschläge des Digital-Omnibusses für Daten lehnen wir ab bzw. sollten geändert werden:

Personenbezogene Daten		
Bestehendes Gesetz **Datenschutzgrundverordnung (2016/679)**	**Omnibus-Vorschlag (2025/0360) Art. 3 Nr. 1a / Art. 4 Nr. 1 DSGVO**	**Änderungsvorschlag**

Begriffsbestimmungen **Art. 4 Nr. 1**		
Im Sinne dieser Verordnung bezeichnet der Ausdruck: „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;	Im Sinne dieser Verordnung bezeichnet der Ausdruck: „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann; **Angaben zu einer natürlichen Person sind nicht notwendigerweise personenbezogene Daten**	Art. 3 Nr. 1a sollte gelöscht werden.

	für jede andere Person oder Einrichtung, nur weil eine andere Einrichtung diese natürliche Person identifizieren kann; Angaben sind für eine bestimmte Einrichtung nicht personenbezogen, wenn diese Einrichtung die natürliche Person, auf die sich die Angaben beziehen, in Anbetracht der mit hinreichender Wahrscheinlichkeit von dieser Einrichtung genutzten Mittel, nicht identifizieren kann; derartige Angaben werden für diese Einrichtung nicht allein deshalb personenbezogen, weil ein potenzieller späterer Empfänger über Mittel verfügt, die mit hinreichender Wahrscheinlichkeit zur Identifizierung der natürlichen Person, auf die sich die Angaben beziehen, verwendet werden können;	

Begründung:

Mit dieser Änderung sollen bestimmte Kategorien pseudonymisierter personenbezogene Daten nicht mehr als besondere Kategorien personenbezogener Daten gelten, sofern eine Rückidentifizierung unwahrscheinlich ist. Die EU-Kommission scheint sich mit diesem Vorschlag auf das ein Urteil des EuGH zu beziehen (C-413/23P EDPS v SRB). Dieser Änderungsvorschlag jedoch führt nicht zu mehr Vereinfachung, sondern zu mehr Unsicherheit und Komplexität. Zudem würden bestimmte personenbezogene Daten von verschiedenen Akteur:innen (Verantwortliche) anders gehandhabt werden als von anderen Akteur:innen (andere Verantwortliche, Datensubjekte, Auftragsdatenverarbeiter), insbesondere auch bei einer Mehrfachverwendung der Daten (siehe auch die Analyse von noyb).

Mit Blick auf kleine und mittelgroße Organisationen der Caritas, die in großem Maß personenbezogene Daten verarbeiten, wären kleine potenzielle Vereinfachungen von vielen rechtlichen und technischen Fragen überlagert: Sind dieselben Daten für Träger A zukünftig nicht mehr personenbezogen, für Träger B aber doch? Müssten Träger nur ihre Möglichkeiten der Identifizierung berücksichtigen oder auch die Möglichkeiten und Mittel Dritter? Nach welchen Kriterien? Wir fürchten, dass dieser relative Personenbezug kleinen, gemeinnützigen Trägern nicht entscheidend hilft, sondern mehr Unklarheit schafft. Zumal was heute noch „mit hinreichender Wahrscheinlichkeit“ nicht identifiziert werden kann, morgen wieder identifiziert werden könnten, wenn Technologien weiterentwickelt werden oder sich die Verarbeitungszwecke ändern.

Auch für Klient:innen als Datensubjekte, deren sensiblen personenbezogenen Daten verarbeitet werden, entstünden keine nennenswerten Vorteile. Im Gegenteil, sie müssten darauf vertrauen, dass alle verantwortlichen Akteur:innen ihre personenbezogenen Daten besonders in den Datenwertschöpfungsketten online schlicht nicht rückidentifizieren können. Ob die Regelung im Einklang mit Art. 8 der EU Grundrechtecharta steht, ist ebenfalls fraglich. Der mögliche Nutzen durch die Änderung rechtfertigt diese Probleme nicht. Im Gegenteil, Datensubjekte und ihren personenbezogenen Daten droht eine starke Abschwächung des bisherigen Schutzes. Mit Blick auf die Klient:innen der FW, die oftmals marginalisierten und vulnerablen Personengruppen angehören, ist diese Reduzierung des Datenschutzes nicht vertretbar.

Verarbeitung personenbezogener Daten bei Entwicklung und Betrieb von KI		
Bestehendes Gesetz **Datenschutzgrundverordnung (2016/679)**	**Omnibus-Vorschlag (2025/0360)** **Art. 3 Nr. 15 / Art. 88c DSGVO**	**Änderungsvorschlag** **Omnibus-Vorschlag (2025/0360) Art. 3 Nr. 15 / Art. 88c DSGVO**
-	**Ist die Verarbeitung personenbezogener Daten im Zusammenhang mit der Entwicklung und dem Betrieb eines KI-Systems im Sinne des Artikels 3 Nummer 1 der Verordnung (EU) 2024/1689 oder eines KI-Modells im Interesse des Verantwortlichen erforderlich, so kann diese Verarbeitung gegebenenfalls aus berechtigtem Interesse im Sinne des Artikels 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 erfolgen, es sei denn, andere Rechtsvorschriften der Union oder der Mitgliedstaaten sehen ausdrücklich eine Einwilligung vor und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern,**	Ist die Verarbeitung personenbezogener Daten im Zusammenhang mit der Entwicklung und dem Betrieb eines KI-Systems im Sinne des Artikels 3 Nummer 1 der Verordnung (EU) 2024/1689 oder eines KI-Modells im Interesse des Verantwortlichen erforderlich, so kann diese Verarbeitung gegebenenfalls aus berechtigtem Interesse im Sinne des Artikels 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 erfolgen, es sei denn, andere Rechtsvorschriften der Union oder der Mitgliedstaaten sehen ausdrücklich eine Einwilligung vor und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere wenn es sich bei der

	überwiegen, insbesondere wenn es sich bei der betroffenen Person um ein Kind handelt. **Eine solche Verarbeitung unterliegt geeigneten organisatorischen, technischen Maßnahmen und Garantien für die Rechte und Freiheiten der betroffenen Person, zum Beispiel um in der Phase der Auswahl der Quellen und des Trainings und Testens von KI-Systemen oder KI-Modellen die Einhaltung der Datenminimierung sicherzustellen, im KI-System oder KI-Modell auf Vorrat gespeicherte Daten vor der Offenlegung zu schützen, für mehr Transparenz für die betroffenen Personen zu sorgen und den betroffenen Personen ein bedingungsloses Recht auf Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einzuräumen.**	betroffenen Person um ein Kind handelt. Eine solche Verarbeitung unterliegt ~~geeigneten~~ *strikten* organisatorischen, technischen Maßnahmen und Garantien für die Rechte und Freiheiten der betroffenen Person, ~~zum Beispiel um in der~~ *in allen Phasen der Verarbeitung, insbesondere in der Phase* der Auswahl der Quellen und des Trainings und Testens. *In der Entwicklung und im Betrieb von* KI-Systemen oder KI-Modellen ist die Einhaltung der Datenminimierung sicherzustellen, im KI-System oder KI-Modell auf Vorrat gespeicherte Daten vor der Offenlegung zu schützen, für mehr Transparenz für die betroffenen Personen zu sorgen und den betroffenen Personen ein bedingungsloses Recht auf Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einzuräumen. *Alle betroffenen Personen, deren personenbezogene Daten verarbeitet werden,*

		sind über den Verarbeitungsvorgang aus berechtigtem Interesse zu informieren und ihnen einen Widerspruch zu ermöglichen.

Begründung:

Der Vorschlag der EU-Kommission ist eine Klarstellung, dass personenbezogene Daten in der Entwicklung und im Betrieb von KI-Modellen und KI-Systemen auf der rechtlichen Grundlage des Artikels 6 Absatz 1 Buchstabe f der DSGVO erfolgen darf. Die daraus resultierende Bevorzugung von KI-Systemen und Modellen bei der Verarbeitung personenbezogener Daten gegenüber anderen Verarbeitungsformen/-technologien ist zu hinterfragen. Gleichzeitig würde die Änderung es auch Trägern der Caritas erleichtern, KI mit personenbezogenen Daten zu betreiben. Angesichts der Menge und Vielfalt personenbezogener Daten in der Arbeit der Verbände, kann so das Angebot der Einrichtungen und Dienste an die Klient:innen verbessert werden. Zudem scheinen große KI-Konzerne bereits jetzt ohne Probleme große Mengen personenbezogener Daten für ihre Systeme und Modelle nutzen, kleinere Organisationen könnten dies mit dieser Gesetzesänderung mit stärkerer Rechtssicherheit und im kleineren, sichereren und datensparsameren Rahmen auch. Trotz der ebenfalls von der EU-Kommission vorgeschlagenen Bedingungen für Schutzmaßnahmen ist anzunehmen, dass diese Änderung die Möglichkeiten von Individuen reduziert, selbstbestimmt zu entscheiden, wann wo und zu welchem Zweck ihre personenbezogenen Daten verarbeitet werden.

Daher fordert der Deutsche Caritasverband nachdrücklich striktere Schutzmaßnahmen sowie eine Pflicht betroffene Personen über die Verarbeitung ihrer personenbezogenen Daten für die Entwicklung und den Betrieb von KI zu informieren, und ihnen eine Opt-out-Möglichkeit zu geben.

Datenzugangsverlangen und Verletzungen von Geschäftsgeheimnissen durch Dritte		
Bestehendes Gesetz **Daten-Verordnung (2023/2854) Art. 5 Abs. 11**	**Omnibus-Vorschlag** **(2025/0360)** **Art. 1 Nr. 4**	**Änderungsvorschlag** **Daten-Verordnung (2023/2854) hinzufügen eines Art. 2 Nr. 5a**
Wenn unter außergewöhnlichen Umständen der Dateninhaber, der Inhaber eines Geschäftsgeheimnisses ist, nachweisen kann, dass er trotz der vom Dritten gemäß Absatz 9 des vorliegenden Artikels getroffenen technischen und organisatorischen Maßnahmen mit hoher Wahrscheinlichkeit einen schweren wirtschaftlichen Schaden durch eine Offenlegung von Geschäftsgeheimnissen erleiden wird, kann er das Datenzugangsverlangen für die betreffenden speziellen Daten im Einzelfall ablehnen. Dieser Nachweis ist auf der Grundlage objektiver Fakten, insbesondere der Durchsetzbarkeit des Schutzes von Geschäftsgeheimnissen in Drittländern, der Art und des Grads der Vertraulichkeit	Wenn unter außergewöhnlichen Umständen der Dateninhaber, der Inhaber eines Geschäftsgeheimnisses ist, nachweisen kann, dass er trotz der vom Dritten gemäß Absatz 9 des vorliegenden Artikels getroffenen technischen und organisatorischen Maßnahmen mit hoher Wahrscheinlichkeit einen schweren wirtschaftlichen Schaden durch eine Offenlegung von Geschäftsgeheimnissen erleiden wird, **oder dass die Offenlegung von Geschäftsgeheimnissen gegenüber dem Nutzer ein hohes Risiko des rechtswidrigen Erwerbs oder der rechtswidrigen Nutzung oder Offenlegung gegenüber Einrichtungen aus Drittländern oder in der Union niedergelassenen Einrichtungen, die**	*‚einzigartiges vernetztes Produkt‘ bezeichnet ein Produkt, dessen Kernfunktionalität ohne wesentliche, ausschließlich für einen einzelnen Kunden entwickelte Softwarebestandteile nicht nutzbar wäre, wobei der Anteil dieser kundenindividuellen Komponenten mindestens 30 % der implementierten Funktionalität ausmacht; bloße Konfigurationen, Parametrisierungen oder Kunden-Onboarding begründen keine Einzigartigkeit;*

der verlangten Daten sowie der Einzigartigkeit und Neuartigkeit des vernetzten Produkts hinreichend zu begründen und Dritten unverzüglich schriftlich vorzulegen. Verweigert der Dateninhaber die Weitergabe von Daten gemäß diesem Absatz, so teilt er dies der gemäß Artikel 37 benannten zuständigen Behörde mit.	**unter der direkten oder indirekten Kontrolle solcher Einrichtungen stehen und Rechtsordnungen unterliegen, die einen schwächeren oder nicht gleichwertigen Schutz im Vergleich zu dem nach Unionsrecht bieten, birgt,** kann er das Datenzugangsverlangen für die betreffenden speziellen Daten im Einzelfall ablehnen. Dieser Nachweis ist auf der Grundlage objektiver Fakten, wie der Durchsetzbarkeit des Schutzes von Geschäftsgeheimnissen in Drittländern, der Art und des Vertraulichkeitsgrads der verlangten Daten sowie der Einzigartigkeit und Neuartigkeit des vernetzten Produkts hinreichend zu begründen. Er ist dem Dritten unverzüglich schriftlich vorzulegen. Verweigert der Dateninhaber die Weitergabe von Daten gemäß diesem Absatz, so teilt er dies der gemäß Artikel 37 benannten zuständigen Behörde mit.	

Begründung:

Die Gefahr von Schäden durch die Offenlegung von Geschäftsgeheimnissen von Dateninhabern möchte der DCV nicht beurteilen. Es muss aber sichergestellt werden, dass Dateninhaber eine angebliche Einzigartigkeit eines Produkts nicht ausnutzen, um Datenzugangsverlangen abzulehnen. Daher schlagen wir zum Schutz der Nutzer:innen eine ergänzende Definition in der Datenverordnung vor, was ein einzigartiges vernetztes Produkt ausmacht.

Definition wissenschaftliche Forschung		
Bestehendes Gesetz **Datenschutzgrundverordnung** **(2016/679)** **Begriffsbestimmungen** **Art. 4 Nr. 1**	**Omnibus-Vorschlag** **(2025/0360)** **Art. 3 Nr. 1b**	**Änderungsvorschlag** **(2025/0360)** **Art. 3 Nr. 1b**
-	Im Sinne dieser Verordnung bezeichnet der Ausdruck: **‚wissenschaftliche Forschung' jede Forschungstätigkeit, die auch Innovationen, wie etwa technologische Entwicklung und Demonstration, unterstützen kann. Mit diesen Tätigkeiten werden Beiträge zu den vorhandenen wissenschaftlichen Erkenntnissen geleistet oder vorhandene Erkenntnisse auf neuartige Weise**	Im Sinne dieser Verordnung bezeichnet der Ausdruck: ‚wissenschaftliche Forschung' ~~jede~~ Forschungstätigkeit, die auch Innovationen, wie etwa technologische Entwicklung und Demonstration, unterstützen kann. Mit diesen Tätigkeiten werden Beiträge zu den vorhandenen wissenschaftlichen Erkenntnissen geleistet ~~oder vorhandene Erkenntnisse auf neuartige Weise angewendet~~; ~~sie~~

	angewendet; sie werden mit dem Ziel durchgeführt, zur Entwicklung des allgemeinen Wissens und des Wohlergehens der Gesellschaft beizutragen, wobei in dem betreffenden Forschungsbereich ethische Standards eingehalten werden. Dabei ist es nicht ausgeschlossen, dass die Forschung auch der Förderung eines gewerblichen Interesses dienen kann.	~~werden mit dem Ziel durchgeführt, zur Entwicklung des allgemeinen Wissens und des Wohlergehens der Gesellschaft beizutragen,~~ *sie trägt zu dem Erreichen der Forschungsziele der EU entsprechend Anhang I der Verordnung 2021/695 [Horizont Europa] bei*, wobei in dem betreffenden Forschungsbereich ethische Standards eingehalten werden. Dabei ist es nicht ausgeschlossen, dass die Forschung auch der Förderung eines gewerblichen Interesses dienen kann.

Begründung:

Wissenschaftliche Forschung muss gefördert werden, die Nutzung von Daten für Forschung ist zweifellos notwendig. Auch die Verbände der Caritas arbeiten täglich an sozialen Innovationen. Allerdings ist die von der EU-Kommission vorgeschlagene Definition für wissenschaftliche Forschung viel zu weit gefasst. Der vorgeschlagene Text eröffnet die Möglichkeit zahllose Tätigkeit als wissenschaftliche Forschung zu deklarieren, solange eine vage formulierte neue Erkenntnis entsteht, zum ebenfalls vagen „Wohlergehen der Gesellschaft“ beigetragen wird und bereichsspezifische ethische Standards eingehalten werden. Dies birgt die Gefahr, dass Datenschutz unter dem Vorwand wissenschaftlicher Forschung abgeschwächt wird, vor allem von großen Unternehmen, die große Mengen Daten verarbeiten. Auch hier ist zu befürchten, dass die Nutzung personenbezogener Daten für eine derart weit definierte Forschung marginalisierten und vulnerablen Personengruppen den Individuen schadet.

Teil III

Forderungen des DCVs für eine bessere KI-Nutzung in der sozialen Daseinsvorsorge

Viele Tätigkeitsbereiche der Caritas in Deutschland fallen in die Kategorie der Anwendungsbereiche für Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2 und Anhang III KI VO, darunter die Bereiche Bildung; Beschäftigung; grundlegende private und grundlegende öffentliche Dienste und Leistungen; Strafverfolgung und Rechtspflege; Migration und Asyl. Teilweise sind die Verbände als Anbieter und Betreiber von KI-Systemen selbst tätig, teilweise setzen sie sich für Klient:innengruppen ein, die in den genannten Bereichen vom Output von KI-Systemen betroffene Personen sind.

Daher ist der Caritas ein möglichst hohes Maß an Sicherheit wichtig, wenn Hochrisiko-KI-Systeme genutzt werden. Die Einrichtungen und Dienste wollen ihrer Verantwortung gegenüber Klient:innen, Mitarbeitenden und Engagierten nachkommen und potenzielle Schäden soweit möglich ausschließen, wenn sie selbst KI entwickeln, oder wenn sie KI-Systeme betreiben. Zudem gehören die Menschen, die sich als Klient:innen an die Einrichtungen und Dienste der Caritas wenden, oftmals zu benachteiligten und vulnerablen Personengruppen. Diese Personengruppen haben ein höheres Risiko durch Datenverarbeitungen durch KI-Systeme diskriminiert zu werden.

Der risikobasierte Ansatz der KI-Verordnung ist daher zu begrüßen. Allerdings muss auch sichergestellt werden, dass die beschlossenen Regeln gelten und dass Träger die notwendige Unterstützung bekommen, KI-Systeme nutzen zu können.

1) Folgende Vorschläge des Digital-Omnibusses für KI unterstützen wir:

Verarbeitung besonderer Kategorien personenbezogener Daten zur Erkennung und Korrektur von Verzerrungen	
Omnibusvorschlag (2025/0359) **Art. 1 Nr. 5 / Art. 4a KI VO**	**Empfehlung: beibehalten und wiederkehrende Erkennung und Korrektur berücksichtigen**
Begründung: Die Minimierung von Verzerrungen und Diskriminierungen durch KI-Systeme ist eines der Hauptanliegen des DCVs, insbesondere bei Hochrisiko-KI-Systemen. Dass Anbieter	

solcher Systeme in Ausnahmen besondere Kategorien personenbezogener Daten verarbeiten dürfen, um Verzerrungen zu verhindern, ist sinnvoll. Die außerdem von der EU-Kommission vorgeschlagenen Bedingungen und die darin enthaltenden Schutzvorkehrungen für die Verarbeitung besonderer Kategorien personenbezogener Daten zur Erkennung und Korrektur von Verzerrungen müssen in den Verhandlungen des Gesetzgebungsprozesses beibehalten werden. Der Artikelvorschlag scheint von einmaligen Maßnahmen zur Korrektur auszugehen. Maßnahmen zur Minimierung von Verzerrungen sollten allerdings – wenn nötig – kontinuierlich erfolgen und die Daten jeweils wieder gelöscht werden.

2) **Folgende Vorschläge des Digital-Omnibusses für KI lehnen wir ab bzw. sollten geändert werden:**

Verschiebung der Umsetzungsfristen für Hochrisiko-KI-Systeme		
Bestehendes Gesetz **KI-Verordnung** **(2024/1689)** **Art. 113** **Inkrafttreten und Geltungsbeginn**	**Omnibus-Vorschlag** **(2025/0359)** **Art. 1 Nr. 31 / Art. 113 Abs. 3 KI VO**	**Änderungsvorschlag** **Omnibus-Vorschlag** **(2025/0359)** **Art. 1 Nr. 31 / Art. 113 Abs. 3 KI VO**
Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft. Sie gilt ab dem 2. August 2026. Jedoch: a) Die Kapitel I und II gelten ab dem 2. Februar 2025;	**In Absatz 3 wird folgender Buchstabe d angefügt:** **„d) Kapitel III Abschnitte 1, 2 und 3 gelten nach Annahme eines Beschlusses der Kommission, in dem bestätigt wird, dass geeignete Maßnahmen zur Unterstützung der Einhaltung des Kapitels III**	Der Deutsche Caritasverband fordert höchste politische Anstrengungen, die erforderlichen Normen und Standards für die Umsetzung des Kapitel III Abschnitte 1, 2 und 3 so schnell wie möglich zu entwickeln und die Frist für den Geltungsbeginn nicht zu verschieben.

b) Kapitel III Abschnitt 4, Kapitel V, Kapitel VII und Kapitel XII sowie Artikel 78 gelten ab dem 2. August 2025, mit Ausnahme des Artikels 101; c) Artikel 6 Absatz 1 und die entsprechenden Pflichten gemäß dieser Verordnung gelten ab dem 2. August 2027.	**bestehen, ab den folgenden Zeitpunkten:** **i) sechs Monate nach Annahme des Beschlusses in Bezug auf KI-Systeme, die gemäß Artikel 6 Absatz 2 und Anhang III als hochriskant eingestuft sind, und** **ii) zwölf Monate nach Annahme des Beschlusses in Bezug auf KI-Systeme, die gemäß Artikel 6 Absatz 1 und Anhang I als hochriskant eingestuft sind.** **Wird kein Beschluss im Sinne des Unterabsatzes 1 angenommen oder liegen die nachstehend festgelegten Daten vor der Annahme dieses Beschlusses, so gelten Kapitel III Abschnitte 1, 2 und 3 ab dem** **i) 2. Dezember 2027 in Bezug auf KI-Systeme, die gemäß Artikel 6 Absatz 2 und Anhang III als hochriskant eingestuft sind, und** **ii) 2. August 2028 in Bezug auf KI-Systeme, die**	Sollte dies unter keinen Umständen möglich sein, fordert der DCV: *In Absatz 3 wird folgender Buchstabe d angefügt:* *Kapitel III Abschnitte 1, 2 und 3 gelten in Bezug auf KI-Systeme, die gemäß Artikel 6 Absatz 2 und Anhang III als hochriskant eingestuft sind, und in Bezug auf KI-Systeme, die gemäß Artikel 6 Absatz 1 und Anhang I als hochriskant eingestuft sind, ab dem 2. Oktober 2027.*

	gemäß Artikel 6 Absatz 1 und Anhang I als hochriskant eingestuft sind.“ **b) In Absatz 3 wird folgender Buchstabe e angefügt: „e) Artikel 102 bis 110 gelten ab dem [Datum des Geltungsbeginns dieser Verordnung].“**	
Begründung: Die Regeln der KI-Verordnung für Hochrisiko-KI-Systeme sind sowohl für Träger als auch zum Schutz der oftmals benachteiligten und vulnerablen Klient:innengruppen wichtig, wie oben beschrieben. Die Einhaltung der Umsetzungsfristen muss oberste politische Priorität sein, d.h. die nötigen Standards und Normen müssen schnellstmöglich erarbeitet werden. Zudem haben sich viele Träger in ihren Planungen bereits an den bestehenden Fristen und den Vorgaben für Hochrisiko-KI-Systeme ausgerichtet. Wie an anderer Stelle bereits erwähnt, verfügen die vielen gemeinnützigen kleinen und mittelgroßen Träger über keine großen Rechtsabteilungen oder Gelder für umfassende juristische Expertise. Wenn eine Fristverlängerung unter keinen Umständen abgewendet werden kann, sollte für alle Hochrisiko-KI-Systeme dieselbe, feste neue Frist gelten. Innerhalb dieser Frist müssen dann mit allen nötigen Ressourcen die erforderlichen Standards ausgearbeitet werden. Die von der EU-Kommission vorgeschlagene differenzierte und relative Frist würde nur zu weiterer rechtlicher und organisatorischer Komplexität führen.		

Unterstützung für Träger der Caritas und zivilgesellschaftliche Organisationen bei der Durchführung der KI-Verordnung		
Bestehendes Gesetz **KI-Verordnung** **(2024/1689)** **Art. 70 Abs. 8**	**Omnibus-Vorschlag** **(2025/0359)** **Art. 1 Nr. 23 / Art. 70 Abs. 8 KI VO**	**Änderungsvorschlag** **Omnibus-Vorschlag** **(2025/0359)**

Benennung von zuständigen nationalen Behörden und zentrale Anlaufstelle		**Art. 1 Nr. 23 / Art. Art. 70 Abs. 8 KI VO**
Die zuständigen nationalen Behörden können gegebenenfalls insbesondere KMU, einschließlich Start-up-Unternehmen, unter Berücksichtigung der Anleitung und Beratung durch das KI-Gremium oder der Kommission mit Anleitung und Beratung bei der Durchführung dieser Verordnung zur Seite stehen. Wenn zuständige nationale Behörden beabsichtigen, Anleitung und Beratung in Bezug auf ein KI-System in Bereichen anzubieten, die unter das Unionrecht fallen, so sind gegebenenfalls die nach jenen Unionsrecht zuständigen nationalen Behörden zu konsultieren.	Die zuständigen nationalen Behörden können gegebenenfalls insbesondere **kleinen Midcaps und** KMU, einschließlich Start-up-Unternehmen, unter Berücksichtigung der Anleitung und Beratung durch das KI-Gremium oder **die** Kommission mit Anleitung und Beratung bei der Durchführung dieser Verordnung zur Seite stehen. Wenn zuständige nationale Behörden beabsichtigen, Anleitung und Beratung in Bezug auf ein KI-System in Bereichen anzubieten, die unter das Unionsrecht fallen, so sind gegebenenfalls die nach jenem Unionsrecht zuständigen nationalen Behörden zu konsultieren.	Die zuständigen nationalen Behörden können gegebenenfalls insbesondere kleinen Midcaps und KMU, einschließlich Start-up-Unternehmen, *und zivilgesellschaftliche Organisationen* unter Berücksichtigung der Anleitung und Beratung durch das KI-Gremium oder die Kommission mit *sektorspezifischer* Anleitung und Beratung bei der Durchführung dieser Verordnung zur Seite stehen. Wenn zuständige nationale Behörden beabsichtigen, Anleitung und Beratung in Bezug auf ein KI-System in Bereichen anzubieten, die unter das Unionsrecht fallen, so sind gegebenenfalls die nach jenem Unionsrecht zuständigen nationalen Behörden zu konsultieren.
Begründung: Die Caritasverbände sind ein wichtiger Teil der sozialen Infrastruktur Deutschlands und zivilgesellschaftliche Organisationen. Sie sollten daher bei sektorspezifischen Anleitungen und Beratungen ebenfalls berücksichtigt werden.		

Registrierung von KI-Systemen, die nicht als hochriskant eingestuft werden		
Bestehendes Gesetz **KI-Verordnung** **(2024/1689)** **Art. 6 Abs. 4**	**Omnibus-Vorschlag** **(2025/0359)** **Art. 1 Nr. 6/ Art. 6 Abs. 4 KI VO**	**Änderungsvorschlag Omnibus-Vorschlag** **(2025/0359)** **Art. 1 Nr. 6/ Art. 6 Abs. 4 KI VO**
Ein Anbieter, der der Auffassung ist, dass ein in Anhang III aufgeführtes KI-System nicht hochriskant ist, dokumentiert seine Bewertung, bevor dieses System in Verkehr gebracht oder in Betrieb genommen wird. Dieser Anbieter unterliegt der Registrierungspflicht gemäß Artikel 49 Absatz 2. Auf Verlangen der zuständigen nationalen Behörden legt der Anbieter die Dokumentation der Bewertung vor.	**Ein Anbieter, der der Auffassung ist, dass ein in Anhang III aufgeführtes KI-System nicht hochriskant ist, dokumentiert seine Bewertung, bevor dieses System in Verkehr gebracht oder in Betrieb genommen wird. Auf Verlangen der zuständigen nationalen Behörden legt der Anbieter die Dokumentation der Bewertung vor.**	Ein Anbieter, der der Auffassung ist, dass ein in Anhang III aufgeführtes KI-System nicht hochriskant ist, dokumentiert seine Bewertung, bevor dieses System in Verkehr gebracht oder in Betrieb genommen wird. Dieser Anbieter unterliegt *einer vereinfachten* Registrierungspflicht *(Name des Systems, Anwendungsbereich und Kontaktdaten des Anbieters)* gemäß Artikel 49 Absatz 2. Auf Verlangen der zuständigen nationalen Behörden legt der Anbieter die Dokumentation der Bewertung vor.
Begründung: Eine Registrierung von KI-Systemen, die nicht als hochriskant eingestuft wurden, ist ein zusätzlicher Bürokratieaufwand für Anbieter. Da die Einstufung jedoch vom Anbieter selbst vorgenommen wird und eine Einstufung eines Systems als Hochrisiko-KI-System einen erheblichen Zusatz an Vorgaben und damit Aufwand zur Folge hat, besteht die Gefahr, dass viele Anbieter einen Anreiz haben, ihre Systeme als nicht hochriskant einzustufen.		

Daher fordert der DCV eine Beibehaltung der Registrierungspflicht auch für KI-Systeme, die nicht hochriskant sind bzw. sein sollen. Allerdings in einem vereinfachten Verfahren, um Anbieter von nicht hochriskanten KI-Systemen zu entlasten.

KI-Kompetenzen		
Bestehendes Gesetz **KI-Verordnung** **(2024/1689)** **Art. 4**	**Omnibus-Vorschlag** **(2025/0359)** **Art. 1 Nr. 4/ Art. 4 KI VO**	**Änderungsvorschlag** **Omnibus-Vorschlag** **(2025/0359)** **Art. 1 Nr. 4/ Art. 4 KI VO**
Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind.	**Die Kommission und die Mitgliedstaaten halten die Anbieter und Betreiber von KI-Systemen dazu an, Maßnahmen zu ergreifen, die sicherstellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihr Ausbildungs- und Schulungsniveau und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-**	Die Kommission und die Mitgliedstaaten *stellen sicher, dass* Anbieter und Betreiber von KI-Systemen ~~dazu an,~~ Maßnahmen ~~zu~~ ergreifen, die sicherstellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihr Ausbildungs- und Schulungsniveau und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt

	Systeme eingesetzt werden sollen, zu berücksichtigen sind.	werden sollen, zu berücksichtigen sind. *Die Mitgliedstaaten stellen Anbietern, Betreibern und Bürgern kostenlose Lerninhalte über KI-Grundkenntnisse zur Verfügung.*
Begründung: Organisationen mit der Weiterbildung ihrer Beschäftigten und ehrenamtlich Engagierten nicht alleine zulassen ist richtig – die EU-Kommission und nationale staatliche Stellen einzubinden ist daher ein guter Vorschlag. Die Formulierungen müssen aber klarer sein und allen Akteur:innen eindeutige Vorschriften machen, Mitgliedstaaten z.B. verpflichten kostenlos zugängliche Angebote anzubieten, mit denen Grundkenntnisse über KI vermittelt werden. Arbeitgeber:innen können darauf aufbauend organisationsspezifische weitere Kompetenzen vermitteln.		