Schriftenreihe

Deutsches Kinderhilfswerk

RECHTSWISSENSCHAFTLICHE GUTACHTERLICHE STELLUNGNAHME

Gesetzeskonforme Nutzbarkeit biometrischer Kinderdaten als KI-Trainingsdaten und in KI-gesteuerten Entscheidungsprozessen

Das Deutsche Kinderhilfswerk e.V. setzt sich seit mehr als 50 Jahren für die Rechte von Kindern in Deutschland ein. Die Überwindung von Kinderarmut und die Beteiligung von Kindern und Jugendlichen an allen sie betreffenden Angelegenheiten stehen im Mittelpunkt der Arbeit als Kinderrechtsorganisation. Das Deutsche Kinderhilfswerk initiiert und unterstützt Maßnahmen und Projekte, die die Teilhabe von Kindern und Jugendlichen, unabhängig von deren Herkunft oder Aufenthaltsstatus, fördern. Die politische Lobbyarbeit wirkt auf die vollständige Umsetzung der UN-Kinderrechtskonvention in Deutschland hin, insbesondere im Bereich der Mitbestimmung von Kindern, bei ihren Interessen bei Gesetzgebungs- und Verwaltungsmaßnahmen und der Überwindung von Kinderarmut. Ziel ist insgesamt die gleichberechtigte gesellschaftliche Teilhabe aller Kinder in Deutschland.

Die Publikation wurde im Rahmen des Projektes Koordinierungsstelle Kinderrechte in der digitalen Welt erstellt. Das Deutsche Kinderhilfswerk erhält dafür eine Förderung des Bundesministeriums für Bildung, Familie, Senioren, Frauen und Jugend.

Die Veröffentlichung stellt keine Meinungsäußerung des Deutschen Kinderhilfswerkes oder des Bundesministeriums für Bildung, Familie, Senioren, Frauen und Jugend dar. Für inhaltliche Aussagen trägt der Autor die Verantwortung.

Das vorliegende Gutachten wird durch eine kinderrechtliche Einordnung des Deutschen Kinderhilfswerkes kommentiert. Diese dient dazu, das Thema zusätzlich aus der Perspektive der Kinderrechte zu verorten, Risiken und Chancen der Nutzung biometrischer Kinderdaten im Kontext von KI zu bewerten und politische sowie praktische Handlungsmöglichkeiten für eine kinderrechtskonforme Ausgestaltung aufzuzeigen. Die kinderrechtliche Einordnung ist abrufbar unter: www.dkhw.de/kinderrechtliche-einordnung-biometrische-kinderdaten-ki-training.

Herausgegeben von:

Deutsches Kinderhilfswerk

Verfasst von:

wida
wissenschaftliches institut für die digitalisierung der arbeitswelt

Gefördert vom:

Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend

Im Rahmen von:

KJP Kinder- und Jugendplan des Bundes

GAmM Gutes Aufwachsen mit Medien

IMPRESSUM

Schriftenreihe des Deutschen Kinderhilfswerkes e. V.

Deutsches Kinderhilfswerk e. V.
Leipziger Straße 116-118
10117 Berlin
Fon: +49 30 308693-0
Fax: +49 30 308693-93
E-Mail: dkhw@dkhw.de
www.dkhw.de

Autor: Dr. Stefan Brink

Redaktion: Martin Fischer, Lukas Glaser und Frauke Rummler

Layout: DAS KOMMUNIKATIONSHAUS
c/o SCHOSSMANN CONSULTING & PRODUKTION
Anna Salari

© 2025 Deutsches Kinderhilfswerk e.V.

Zielsetzung des Herausgebers

Biometrische Daten sind physische Merkmale, an denen eine Personen eindeutig identifiziert werden kann. Meist wird dabei von Gesichtserkennung gesprochen, es können aber auch ein Fingerabdruck, ein Stimmprofil, ein spezifisches Fuß- und Laufprofil einer Person, bestimmte Handlungsmuster oder eine Verbindung solcher Merkmale sein. Das Verständnis biometrischer Daten ist weit, im Kern steht dabei die eindeutige Identifizierbarkeit des Subjekts. Dies hat technologisch weitreichende Einsatzgebiete im öffentlichen sowie im persönlichen Raum. Daher werden diese Daten häufig als Trainingsdaten für das Training von KI-Systemen in Betracht gezogen. Damit bewegt sich die Erhebung biometrischer Daten im rechtlichen Spannungsfeld der Datenschutzgrundverordnung, des Digital Services Acts und der KI-Verordnung. Diese Verordnungen setzen Grenzen, welche Daten verarbeitet werden dürfen, und unterstreichen das erhöhte Schutzbedürfnis von Kindern. Insbesondere die KI-Verordnung formuliert besondere Risikobereiche, in welchen der Einsatz von KI untersagt ist, und für welche Ausnahmen bestehen sollen.

Dabei muss beachtet werden, dass die Nutzung biometrischer Daten für KI-Training längst stattfindet. Sind diese erstmal erlernt und somit Teil der algorithmischen Entscheidungsprozesse geworden, könnten die einzelnen Daten nicht einfach wieder extrapoliert werden. Hinzu kommt: Gerade bei Kindern sind biometrische Daten noch im Wandel. Gesichtszüge ändern sich, die Stimme unterliegt Veränderungen und so ist insbesondere bei dieser Zielgruppe die eindeutige Identifikation auf Dauer kaum zu gewährleisten. Gleichzeitig verbleiben diese Daten Teil der algorithmischen Entscheidungsgrundlage. Die langfristigen Konsequenzen dieser Situation sind heute kaum abschätzbar.

Vor diesem Hintergrund möchte das Deutsche Kinderhilfswerk zu einer besseren Entscheidungsgrundlage beitragen, in welchen Bereichen biometrische Kinderdaten KI-gestützt zum Einsatz kommen können und dürfen. Dazu soll zunächst eine funktionale Arbeitsdefinition von biometrischen Daten herausgearbeitet werden und in die Rechtsgrundlagen eingebettet werden. Daraus soll abgeleitet werden, unter welchen Umständen biometrische Daten von Kindern gesetzeskonform für automatisierte, KI-gesteuerte Entscheidungsprozesse eingesetzt werden dürfen. Dies soll über abgesteckte mögliche Einsatzfelder geschehen, in welchen eine legale Nutzung der biometrischen Kinderdaten stattfinden dürfte.

In weiteren Schritten sollen durch das Kinderhilfswerk die Einsatzfelder aus kinderrechtlicher Perspektive bewertet werden. Die Ergebnisse sollen in den politischen Diskurs einfließen und damit eine weitere informierte politische Auseinandersetzung ermöglichen. Darüber hinaus ist es das Ziel, die Ergebnisse des Gutachtens in nationalen und internationalen Kinderrechte-Netzwerken zu verbreiten, um auch hier das Verständnis für die Problematik und den Umgang mit biometrischen Kinder-Daten zu erhöhen.

Inhalt

I. Arbeitsdefinition zur Abgrenzung biometrischer Daten 5

I.1. Allgemeine Definition biometrischer Daten 5

I.2. Biometrische Daten gemäß DS-GVO 7

I.3. Definitionen biometrischer Daten in KI-VO und DSA 10

I.4. Abweichende Begriffsverständnisse 10

I.5. Biometrische Daten von Kindern 10

II. Persönliche Daten: besondere Schutzbedürfnisse bei den Daten von Kindern DS-GVO) 12

II.1. Personenbezogene Daten 12

II.2. Verhältnis personenbezogener zu biometrischen Daten 12

II.3. Schutz der Daten von Kindern durch die DS-GVO 13

III. Einordnung biometrischer Daten in den Kontext von DS-GVO, DSA, KI-Verordnung und weiteren relevanten Gesetzgebungen 19

III.1. Digital Services Act 19

III.2. KI-Verordnung 21

Zwischenfazit 25

IV. Entwicklung zulässiger Einsatzfelder für biometrische Kinderdaten in KI-Anwendungen 26

IV.1. Datenverarbeitung zum Training von Basismodellen 26

IV.2. Datenverarbeitung im Rahmen der Nutzung von KI-Systemen 28

IV.3. Art. 22 DS-GVO als Unikat 28

IV.4. Drei Beispiele aus der Praxis 29

Fazit 36

Zusammenfassung der wesentlichen Ergebnisse 37

Literaturverzeichnis 40

Leitlinien und Guidelines 42

I. Arbeitsdefinition zur Abgrenzung biometrischer Daten

I.1. Allgemeine Definition biometrischer Daten

Eine einheitliche oder gar allgemein verbindliche Definition von „biometrischen Daten“ existiert (noch) nicht, der Begriff „Biometrie“ ist griechischen Ursprungs und leitet sich aus den Worten bios (= Leben) und metrein (= messen) her. Unter Biometrie wird ganz allgemein die automatisierte Erkennung von Personen anhand ihrer körperlichen Merkmale verstanden. Die „Wissenschaft der Körpermessung am Lebewesen“[1] macht sich zunutze, dass die körperlichen Eigenschaften im Gegensatz zu Wissens- und Besitzelementen nicht nur mittelbar personenbezogen, sondern unmittelbar personengebunden und nicht beliebig veränderbar sind.[2] „Biometrische Verfahren“ nutzen daher physiologische Charakteristka (Fingerabdruck, Gesichtszüge, Gang [gait recognition], Irismuster etc.) oder verhaltensbedingte Merkmale (Schreibverhalten, Lippenbewegung, Stimme) **zum Zweck der Identifikation einer Person**.

Für biometrische Daten ist es charakteristisch, dass sie Informationen über objektiv unverwechselbare Merkmale natürlicher Personen enthalten und besonders geeignet sind, sie zumeist lebenslang eindeutig zu identifizieren oder ihre Identität zu bestätigen (Identifizierungs- und Authentifizierungsfunktion).[3]

aa) Als Erkennungsverfahren entwickelte Alphonse Bertillon 1879 ein später Bertillonage genanntes System zur Identitätsfeststellung, das auf elf Körperlängenmaßen basierte (Anthropometrie). 1892 legte Francis Galton den wissenschaftlichen Grundstein für die Nutzung des Fingerabdrucks (Daktyloskopie).[4] Inzwischen sind weitere biometrische Merkmale bekannt, die zur Identifikation eines Menschen herangezogen werden können:

- DNA (genetischer Fingerabdruck)
- Fingerabdruck (Fingerlinienbild)
- Gangerkennung
- Gesichtsgeometrie
- Handgeometrie
- Handlinienstruktur
- Handvenenstruktur
- Iris (Regenbogenhaut)
- Retina (Augenhintergrund)
- Körpergeruch
- Lippenbewegung
- Stimmerkennung (Klangfarbe)
- Nagelbettmuster
- Ohrform
- Tippverhalten auf Tastaturen (keystroke dynamics)
- Unterschrift (statisch, dynamisch, ggf. auch Handschrift)
- Zahnabdruck[5]

bb) Bei erstmaliger Aufnahme in ein biometrisches Verfahren (so genanntes Einlernen oder Enrolment) werden ausgewählte Merkmale der betroffenen Person vermessen und mittels eines Algorithmus in einen Datensatz (ein so genanntes **Template**) umgewandelt.[6] Dieses Vermessen, das in der Wissenschaftsgeschichte ursprünglich analog erfolgte,

---

1 Vgl. https://www.lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/biometrie/biometrie-und-datenschutz-55984.html, abgerufen am 18.01.2025.

2 Paal/Pauly/Ernst, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 99.

3 Simitis/Hornung/Spiecker gen. Döhmann/Petri, Datenschutzrecht, 1. Auflage 2019, Art. 4 Nr. 14 Rn. 2.

4 https://de.wikipedia.org/wiki/Biometrie, abgerufen am 18.01.2025.

5 Nachweise bei https://de.wikipedia.org/wiki/Biometrie#cite_note-JTC001-SC37-N-1480-3, abgerufen am 18.01.2025.

6 https://www.lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/biometrie/biometrie-und-datenschutz-55984.html, abgerufen am 18.01.2025.

geschieht zunehmend mit digitalen Verfahren, teilweise vollautomatisiert und unter Einsatz teilweise komplexer Algorithmen.[7] Im Rahmen von Kontrollen werden Merkmale erhoben und daraus Messwerte errechnet, die dann mit dem gespeicherten Datensatz verglichen werden.

Vor diesem Hintergrund definiert man Biometrie im Bereich der Personenerkennung heute als automatisierte Erkennung von Individuen, basierend auf ihren Verhaltens- und biologischen Charakteristika.[8]

cc) Es werden zwei Arten der biometrischen Erkennung unterschieden[9], die jeweils einen anderen Zweck verfolgen: zum einen die **Personenverifikation** und zum anderen die **Personenidentifikation**.[10] Bei der Verifikation wird lediglich die Identität einer Person bestätigt, also geprüft, ob es sich bei einer Person um diejenige handelt, für die sie sich ausgibt oder für die sie aufgrund anderer Faktoren gehalten wird. Dafür ist es zunächst erforderlich, dass sich die zu überprüfende Person gegenüber dem Verfahren zu erkennen gibt, etwa durch eine Benutzerkennung, ein Passwort oder einen Ausweis. Der Abgleich der Daten geschieht mittels 1:1-Abgleich zwischen den aktuell errechneten Messwerten und dem zuvor im System zentral oder auf einem Speichermedium abgelegten Datensatz, z. B. durch einen Blick auf einen biometrischen Ausweis und das Gesicht des zu Verifizierenden.[11] Das Ergebnis dieses Vergleichs kann entweder die Bestätigung der Identität oder aber deren Nichtbestätigung sein.

Bei der Identifikation wird demgegenüber die Frage geklärt, um welche bestimmte Person es sich handelt. Die aktuell errechneten Daten der sich identifizierenden Person werden dabei mit allen im System gespeicherten Messwerten abgeglichen. Die überprüfte Person wird dann als dasjenige Individuum identifiziert, dessen Referenzdatensatz mit den aktuellen Messwerten übereinstimmt. Es erfolgt daher ein 1:n-Abgleich[12], der zwingend voraussetzt, dass die Daten aller Nutzer*innen zuvor gleichförmig erfasst und in einer zentralen Datenbank gespeichert werden. Das Ergebnis der Überprüfung ist die Ausgabe identifizierender Faktoren, also etwa des Namens, der Nutzerkennung o. Ä. der betroffenen Person.

Mögliche Anwendungsfälle der Biometrie sind die Zugangssicherung von Räumen, Rechenzentren, Haustüren, Bankautomaten etc. bzw. die Zugriffsberechtigung zu einer digitalen Anwendung, einem PC oder etwa zum Internetbanking. Aktuell wird das Thema beherrscht von der Debatte um die Einführung biometrischer Ausweisdokumente (Reisepass und Personalausweis).[13]

dd) Auch die moderne Biometrie bietet (natürlich) keine absolute Erkennungssicherheit. Messfehler können nicht nur durch technische Unzulänglichkeiten, sondern auch durch alterungsbedingte Veränderung der körperlichen Merkmale oder durch äußere Einflüsse wie Verletzung, Krankheit oder auch nur die Änderung der äußeren Merkmale einer Person (Frisur, Bart, Styling) auftreten. Dabei kann es zu zwei verschiedenen Fehlerereignissen kommen. Die „False Rejection Rate“ (FRR – auch false negative) bezeichnet prozentual

---

7 Kühling/Buchner/Weichert, 4. Aufl. 2024, DS-GVO Art. 4 Nr. 14 Rn. 1.

8 http://www.3dface.org/media/vocabulary.html, zuletzt abgerufen am 13.02.2025, archiviert unter: https://archive.is/z77Kh.

9 Gola/Heckmann/Gola, 3. Aufl. 2022, DS-GVO Art. 4 Rn. 119.

10 Grundlegend dazu https://www.lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/biometrie/biometrie-und-datenschutz-55984.html, abgerufen am 18.01.2025.

11 Kühling/Buchner/Weichert, 4. Aufl. 2024, DS-GVO Art. 4 Nr. 14 Rn. 7.

12 Gola/Heckmann/Gola, 3. Aufl. 2022, DS-GVO Art. 4 Rn. 119.

13 https://www.lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/biometrie/biometrie-und-datenschutz-55984.html, abgerufen am 18.01.2025.

die Anzahl der Personen, die vom System fälschlicherweise zurückgewiesen werden, obwohl sie die Merkmale für eine Identifikation aufweisen. Die „False Acceptance Rate" (FAR – auch false positive) dagegen gibt Aufschluss über die Prozentzahl der Personen, die das System fälschlicherweise als eine andere erkennt (und zulässt).[14]

Zudem kommt es vor, dass Personen das in einem biometrischen Identifikationsverfahren verwendete Merkmal nicht besitzen (z.B. aufgrund von Erkrankungen oder Behinderungen) bzw. dass das Merkmal so gering ausgeprägt ist, dass das System es nicht mathematisch erfassen kann. Diese als „failure to enrol rate" (FER) bezeichnete Messfehlerrate zeigt daher an, welcher Prozentsatz an Personen nicht in das System „eingelernt" werden kann. Die verschiedenen biometrischen Verfahren wie Gesichtserkennung, Fingerabdruck, Handgeometrie oder Iriserkennung haben dabei jeweils ihre spezifischen Vor- und Nachteile bezogen auf Erkennungsleistung, Praxistauglichkeit, Fehleranfälligkeit, Überwindungssicherheit und Bedieungsfreundlichkeit.[15]

Bleibt demnach die Definition von „biometrischen Daten" und das Verständnis „biometrischer Verfahren" entwicklungsbedingt noch fluide, so steht doch im Kern ihr Nutzungskontext fest: Es geht um die eindeutige Verifikation bzw. Identifikation menschlicher Subjekte.

I.2. Biometrische Daten gemäß DS-GVO

aa) Biometrische Daten sind in Art. 4 Nr. 14 der Datenschutzgrundverordnung (VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG–DS-GVO) legal definiert. Danach sind biometrische Daten „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten" (vgl. dazu auch Erwägungsgrund[16] 51 der DS-GVO). Diese eigene Schutzkategorie der eindeutig identifizierenden Biometriedaten hat einen spezifisch datenschutzrechtlichen Hintergrund[17]: Damit soll das Erstellen umfassender Persönlichkeitsprofile durch systematische Zusammenführung von Daten mithilfe dieser mit modernen technischen Mitteln einfach zu erlangenden und vom Betroffenen nicht beeinflussbaren Daten verhindert werden.[18]

In Identitätspapiere (Personalausweis, Reisepass, Führerschein, Aufenthaltstitel) inte grierte, maschinenlesbare Gesichtsbilder zählen unzweifelhaft zu biometrischen Daten i.S.d. Art. 4 Nr. 14 DS-GVO.[19]

Biometrische Daten sind sowohl die sog. Rohdaten, also die direkt mit einem Sensor erfassten Merkmale, als auch sog. Templates, das heißt aus den Rohdaten gewonnene und

14 https://www.lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/biometrie/biometrie-und-datenschutz-55984.html, abgerufen am 18.01.2025.

15 https://www.lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/biometrie/biometrie-und-datenschutz-55984.html, abgerufen am 18.01.2025.

16 Erwägungsgründe sind als Teil des Rechtsakts den Artikeln der DS-GVO vorangestellt und dienen ihrer Auslegung; sie können jedoch den Wortlaut von Artikeln nicht einschränken.

17 Kühling/Buchner/Weichert, 4. Aufl. 2024, DS-GVO Art. 9 Rn. 32.

18 Kühling/Buchner/Weichert, 4. Aufl. 2024, DS-GVO Art. 9 Rn. 32.

19 Kühling/Buchner/Weichert, 4. Aufl. 2024, DS-GVO Art. 4 Nr. 14 Rn. 3; Simitis/Hornung/Spiecker gen. Döhmann/Petri, Datenschutzrecht, 1. Auflage 2019, Art. 4 Nr. 14, Rn. 8.

typisierte Merkmals-Vektoren, die auf der Grundlage eines mathematischen Modells standardisiert erfasst und regelmäßig zum Identitätsabgleich herangezogen werden. Biometrische Daten sind zur eindeutigen Identifizierung von Menschen geeignet, wenn die gemessenen Merkmale einzigartig sind. Nicht notwendig ist, dass die Angaben weltweit eindeutig sind.[20] Typische Beispiele für biometrische Daten sind neben Fingerabdrücken[21] oder der Stimmerkennung[22] auch die von automatisierten Gesichtserkennungsverfahren erfassten Daten, z. B. die Herstellung von Templates durch die Verarbeitung der Bilddaten, deren Speicherung in einer Referenzdatei, und die mit ihnen erzeugten personenbezogenen Daten.[23] Werden Daten, die für sich allein eine eindeutige Identifizierung nicht ermöglichen, zu einem die Identifizierung ermöglichenden Datensatz zusammengefügt, so ist der gesamte Datensatz als biometrisches Datum anzusehen.[24]

bb) Die Legaldefinition biometrischer Daten in Art. 4 Nr. 14 DS-GVO erschließt sich allerdings erst vor dem Hintergrund der **Regelungskonzeption der Datenschutz-Grundverordnung** vollständig:

aaa) Die DS-GVO reguliert den Umgang mit personenbezogenen Daten i.S.v. Art. 4 Nr. 1 DS-GVO. Unter „personenbezogenen Daten" versteht die DS-GVO (vgl. Art. 4 Nr. 1) „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".[25]

Diese Legaldefinition deutet darauf hin, dass das wesentliche Problem des Datenschutzes als rechtlicher Gewährleistung der informationellen Selbstbestimmung in der **Identifizierbarkeit** einer Person gesehen wird.[26] Eine solche Identifizierung kann sich simpel gestalten, wenn beispielsweise bestimmte Angaben unmittelbar mit Identifikatoren wie dem Namen verknüpft werden, der unter normalen Umständen und unter Einsatz allgemein verfügbarer Informationsquellen (Internet, Telefonbuch etc.)[27] mit hoher Verlässlichkeit jeden zu der Bezugsperson führt.[28]

bbb) Die DS-GVO reguliert den Umgang mit personenbezogenen Daten i.S.v. Art. 4 Nr. 1 DS-GVO, sobald sie „verarbeitet" werden: Unter **Verarbeitung** versteht die DS-GVO „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung" (Art. 4 Nr. 2 DS-GVO). Diese Verarbeitungen unterliegen den Grundsätzen für Datenverarbeitungen nach Art. 5 DS-GVO und bedürfen, sollen sie rechtmäßig sein, einer Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO. Dies umfasst somit alle KI-Systeme und KI-Modelle und unterfällt der DS-GVO, soweit dort personenbezogene Daten verarbeitet werden.

---

20 Kühling/Buchner/Weichert, 4. Aufl. 2024, DS-GVO Art. 4 Nr. 14 Rn. 2.

21 Gola/Heckmann/Gola, 3. Aufl. 2022, DS-GVO Art. 4 Rn. 117.

22 EDSA, Guidelines 2/2021 v. 7.7.2021, Rn. 128; Gola/Heckmann, 3. Aufl. 2022, DS-GVO Art. 4 Rn. 117.

23 Wolff/Brink/v. Ungern-Sternberg, BeckOK DatenschutzR/Veit, 46. Ed. 01.08.2023, DS-GVO Art. 9 Rn. 44.

24 Kühling/Buchner/Weichert, 4. Aufl. 2024, DS-GVO Art. 4 Nr. 14 Rn. 2.

25 Dazu insgesamt instruktiv Wolff/Brink/v. Ungern-Sternberg, BeckOK DatenschutzR/Albers/Veit, 46. Ed. 01.08.2023, DS-GVO Art. 9 Rn. 16.

26 Vgl. auch Erwägungsgrund 26 der DS-GVO.

27 EuGH BeckRS 2011, 81685 Rn. 88; BeckRS 2016, 82520 Rn. 32 ff.; BeckRS 2014, 82595 Rn. 22 f.

28 Für Passagierdaten im Rahmen des PNR-Abkommens EuGH, Gutachten v. 26.07.2017, 1/15, Rn. 121 f.

ccc) Allerdings definiert die DS-GVO besondere Kategorien personenbezogener Daten, welche gar nicht oder nur unter erheblich erschwerten Bedingungen verarbeitet werden dürfen. Nach Art. 9 Abs. 1 DS-GVO ist insbesondere die „Verarbeitung von [...] biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person [...] untersagt". Damit soll der besonderen Anfälligkeit bestimmter Datenkategorien für Diskriminierung, Stigmatisierung oder gar Verfolgung Rechnung getragen werden.

Zu prüfen sind im Rahmen von Art. 9 DS-GVO daher immer drei Kriterien (s. auch EDSA, Leitlinien 3/2019 vom 29.01.2020 Rn. 76): die Art der Daten (Daten „zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person"), Mittel und Wege der Verarbeitung („mit speziellen technischen Verfahren gewonnene" Daten) und der Zweck der Verarbeitung („zur eindeutigen Identifizierung einer natürlichen Person").[29] Das mit Art. 9 DS-GVO verfolgte Konzept der Typisierung von Risiken und Schutzerfordernissen, die an eine allgemeine Kategorisirung von Daten anknüpft, führt zu erheblichen Anwendungsproblemen.[30] Um diese zu mildern, wird Art. 9 DS-GVO unter bestimmten Voraussetzungen schutzbedarfsgerecht eingeschränkt (teleologisch reduziert).[31]

Eine teleologische Reduktion des Anwendungsbereichs kommt etwa in Fällen in Betracht, in denen die Verarbeitung genetischer, biometrischer oder Gesundheitsdaten unter jedem Aspekt erkennbar „belanglos" ist. Hierhin gehört das Beispiel des Fotos eines Brillenträgers in belanglosen Zusammenhängen.[32] Für die Anwendbarkeit von Art. 9 DS-GVO ist danach eine kontextabhängige Betrachtung[33] erforderlich, die in der Praxis ganz maßgeblich durch die Auswertungsabsicht des Verantwortlichen geprägt ist.[34]

Diesem schutzorientierten Anwendungsbereich folgend unterliegen auch nicht alle biometrischen Daten dem Verarbeitungsverbot des Art. 9 Abs. 1 DS-GVO, sondern nur solche „zur eindeutigen Identifizierung einer natürlichen Person".[35] Dass biometrische Daten die „eindeutige Identifizierung" einer bestimmten natürlichen Person ermöglichen oder bestätigen können, ergibt sich bereits aus der Legaldefinition dieser Daten in Art. 4 Nr. 14 DS-GVO. Unter Art. 9 Abs. 1 DS-GVO fallen diese Daten daher nicht wegen ihrer Fähigkeit zur Identifizierung, sondern nur dann, wenn der Verantwortliche sie zu diesem Zweck auch zielgerichtet einsetzt.[36]

Demnach muss also eine Auswertungsabsicht bestehen.[37] Der Gesetzgeber hat nämlich die besondere Sensibilität biometrischer Daten nicht pauschal, sondern nur für solche Daten festgestellt, die mit einer als für die informationelle Selbstbestimmung besonders problematischen Zweckbestimmung verwendet werden, nämlich zu Zwecken der Identifizierung. Die Verarbeitung biometrischer Daten zu anderen Zwecken fällt demnach nicht unter das grundsätzliche Verarbeitungsverbot.[38] Soweit in der Literatur teilweise die Auffassung vertreten wird, die Auswerteabsicht spiele ebenso wenig eine Rolle wie der

---

29 Wolff/Brink/v. Ungern-Sternberg, BeckOK DatenschutzR/Veit, 46. Ed. 01.08.2023, DS-GVO Art. 9 Rn. 44.

30 Wolff/Brink/v. Ungern-Sternberg, BeckOK DatenschutzR/Veit, 46. Ed. 01.08.2023, DS-GVO Art. 9 Rn. 21.

31 Wolff/Brink/v. Ungern-Sternberg, BeckOK DatenschutzR/Albers/Veit, 46. Ed. 01.08.2023, DS-GVO Art. 9 Rn. 21.

32 Wolff/Brink/v. Ungern-Sternberg, BeckOK DatenschutzR/Albers/Veit, 46. Ed. 01.08.2023, DS-GVO Art. 9 Rn. 46.

33 Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 9 Rn. 13.

34 Taeger/Gabel/Mester DS-GVO Art. 9 Rn. 10; auch der EDSA scheint diese Position zu vertreten, vgl. EDSA, Leitlinien 03/2019, Version 2.0 v. 29.01.2020 Rn. 63 f.; a.A., Simitis/Hornung/Spiecker gen. Döhmann/Petri DS-GVO Art. 9 Rn. 12; Reuter, ZD 2018, 564 (565).

35 Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 9 Rn. 19.

36 a.A Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 9 Rn. 14, der meint, der Konkretisierung der biometrischen Daten „zur eindeutigen Identifizierung einer natürlichen Person" hätte es angesichts der Legaldefinition nicht bedurft.

37 Also nicht bereits das schlichte Passbild eines Brillenträgers oder die Aufnahme eines Fotos mit einem biometriefähigen Endgerät (z. B. Smartphone), Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 9 Rn. 19.

38 Simitis/Hornung/Spiecker gen. Döhmann/Petri, Datenschutzrecht, 1. Auflage 2019, Art. 9 Rn. 14.

konkrete Verwendungszusammenhang von mittelbar sensiblen Daten,[39] steht dies im Widerspruch zum eindeutigen Gesetzeswortlaut.

I.3. Definitionen biometrischer Daten in KI-VO und DSA

Vergleichbare Definitionen weisen weder die VERORDNUNG (EU) 2024/1689 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz – KI-Verordnung bzw. KI-VO) noch die VERORDNUNG (EU) 2022/2065 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG – Gesetz über digitale Dienste bzw. DSA) auf. Sie sind eigenständige Rechtsquellen, deren Tatbestandsmerkmale eigenständig zu interpretieren sind. Dennoch kann davon ausgegangen werden, dass die DS-GVO insoweit als wesentlicher Orientierungspunkt fungiert.

I.4. Abweichende Begriffsverständnisse

Dennoch kann die DS-GVO das Verständnis biometrischer Daten natürlich nicht monopolisieren. Andere begriffliche oder definitorische Ansätze bleiben möglich, sind aber zur Absicherung terminologischer Klarheit abzugrenzen. Soweit etwa im gesellschaftlichen Diskurs von „anthropometrischen Daten“ gesprochen wird, wird darunter regelmäßig auf menschliche Körpermaße Bezug genommen. Anthropometrie (von griechisch anthropos [Mensch] und metron [Maß]) ist die Lehre der Ermittlung und Anwendung der Maße des menschlichen Körpers.[40] Anthropometriewird etwa in der Ergonomie zur Gestaltung von Arbeitsplätzen, Fahrzeugen, Werkzeugen und Möbeln genutzt sowie im Arbeitsschutz zur Festlegung von Sicherheitsmaßnahmen (z.B. Bemessungen von Schutzabdeckungen) oder Abständen zu gefahrenträchtigen Teilen.[41] Außerdem dient sie als Ausgangslage für die Erstellung von Standards zur Berechnung von Konfektionsgrößen in der Bekleidungsindustrie. Demgegenüber handelt es sich bei biometrischen Daten um einen technisch-juristischen Begriff, der bislang von ideologischen Fragestellungen freigehalten wurde und daher im vorliegenden Kontext vorzugswürdig erscheint.

I.5. Biometrische Daten von Kindern

Über eine eigenständige Definition biometrischer Daten von Kindern verfügen weder die DS-GVO noch die anderen einschlägigen europäischen Rechtsvorschriften. Während eine solche gesonderte Bestimmung und ggf. Regulierung biometrischer Kinderdaten auf den ersten Blick auch nicht erforderlich erscheint, erschließt sich bei näherem Hinsehen, warum eine solche eigenständige (gesetzgeberische) Befassung mit biometrischen Kinderdaten durchaus sinnvoll wäre: Zum einen besteht eine besondere Schutzbedürftigkeit von Kindern hinsichtlich der Verarbeitung (vgl. Art. 4 Nr. 2 DS-GVO) ihrer biometrischen Daten. Diese ergibt sich bereits aus der zeitlichen Dimension der Nutzung biometrischer Kinderdaten: Angesichts der höheren erwarteten Lebensdauer von Kindern ergibt sich eine besonders lange Betroffenheit junger Menschen von der Nutzung ihrer personenbezogenen Daten und besonderen Kategorien personenbezogener

39 So Simitis/Hornung/Spiecker gen. Döhmann/Petri, Datenschutzrecht, 1. Auflage 2019, Art. 9 Rn. 12.

40 https://de.wikipedia.org/wiki/Anthropometrie, abgerufen am 18.01.2025.

41 https://de.wikipedia.org/wiki/Anthropometrie, abgerufen am 18.01.2025.

Daten. Zudem sind wegen der langen „Laufzeit" ihrer Daten die möglichen Nutzungskontexte besonders offen und wenig überschaubar. Hier spielt neben dem zeitlichen Faktor selbst auch die sich beschleunigende Nutzungsperspektive durch Forschung/Entwicklung zu datenbasierten Vorhaben und Verwertungsmöglichkeiten eine Rolle. Zudem ist mit Blick auf die lange Laufzeit (gerade bei unveränderlichen identifizierenden biometrischen Daten) der wirtschaftliche Wert dieser Datenarten besonders groß – was wiederum den Aufwand für technologische Fortentwicklungen rentabler macht.

Andererseits sind nicht alle biometrischen Kinderdaten gleichermaßen von diesen Faktoren betroffen. Bestimmte biometrische Daten sind nämlich entwicklungs- und wachstumsbedingt bei Kindern noch in der Veränderung begriffen (wie etwa Gesichtszüge, die Stimme oder der individuelle Gang durch eine Fortentwicklung der menschlichen Proportionen), insbesondere bei dieser Zielgruppe ist eine eindeutige Identifikation auf Dauer nicht gewährleistet. Dies kann im Einzelfall positive wie negative Konsequenzen für die einzelne betroffene Person haben, insbesondere wenn veraltete Daten Teil der algorithmischen Entscheidungsgrundlage bleiben. So kann etwa eine Identifikation oder Verifikation wachstumsbedingt scheitern, auch Schutzmechanismen können alterungsbedingt versagen oder fälschlich ausgelöst werden. Die langfristigen Konsequenzen dieser Situationen sind heute kaum abschätzbar.

Umgekehrt sind andere biometrische Faktoren (wie der Fingerabdruck oder die Iris) solchen Entwicklungen nicht oder nur marginal unterworfen und können zeitlich nahezu unbegrenzt ihr Identifikationspotenzial bewahren. Damit ergibt sich hinsichtlich biometrischer Kinderdaten ein insgesamt uneinheitliches Bild, das allerdings wegen der aufgezeigten besonderen Gefährdungspotenziale eine gesetzgeberische Befassung verdient hätte.

Nachfolgend ist in einem ersten Schritt näher zu bestimmen, wie sich biometrische Daten von personenbezogenen Daten (vgl. Art. 4 Nr. 1 DS-GVO) unterscheiden und welche Folgen diese Unterscheidung im Regelungsbereich der DS-GVO zeitigt (vgl. unter II). Sodann ist der Blick auf weitere Rechtsquellen, insbesondere den DSA und die KI-VO auszuweiten (vgl. unter III).

II. Persönliche Daten: besondere Schutzbedürfnisse bei den Daten von Kindern (DS-GVO)

II.1. Personenbezogene Daten

Wie bereits erläutert (vgl. oben Kapitel I) versteht die DS-GVO unter „personenbezogenen Daten“ (vgl. Art. 4 Nr. 1) „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen“.[42]

aa) Aufmerksamkeit verdient dabei die Frage, welche Daten sich überhaupt auf eine identifizierte oder identifizierbare Person beziehen. Der **Bezug** von Daten auf Personen ist keineswegs immer schon in einer Weise gegeben, dass es nur um deren Identifizierbarkeit ginge.[43] Dieser Bezug wird vielmehr in bestimmten Kontexten als Ergebnis einer sinngehaltserzeugenden Leistung tatsächlich oder potenziell und gegebenenfalls erstmals hergestellt; auch gestaltet er sich vielfältig und von unterschiedlicher Dichte.[44] Antworten darauf, wann sich Daten in datenschutzrechtlich relevanter Weise auf identifizierte oder über bestimmte Identifikatoren identifizierbare Personen beziehen (können), sind daher nicht nur (akteurs-)relativ, sondern auch äußerst kontextabhängig. Sie können Wahrscheinlichkeitsannahmen, Prognosen und wertende Beurteilungenerfordern und benötigen in einigen Fällen schlicht eine (gesetzgeberische, aufsichtsbehördliche oder gerichtliche) Dezision.[45] Hier zeigen sich zentrale Abgrenzungs- und Anwendungsprobleme des Datenschutzrechts insgesamt.[46]

bb) Das gilt umso mehr vor dem Hintergrund von automatisierten Verarbeitungsformen im Big-Data-Kontext oder aufgrund von Re-Identifikationsmöglichkeiten durch Zugang zu und Verknüpfung von Daten. Man steht damit vor der Frage, ob dem Merkmal des Personenbezugs, das den Anwendungsbereich des Datenschutzrechts ein- und abgrenzt, im gesamten davon erfassten Spektrum wirklich ausreichende Leistungs- und **Differenzierungskraft** zukommt.[47] Für eine sinnvolle Gestaltung, Auslegung und Anwendung der einschlägigen datenschutzrechtlichen Regelungen ist es daher wichtig, die dahinterstehenden Schutzgüter und rechtlich schutzwürdigen Datenschutzinteressen zu verstehen und zu schärfen.[48]

II.2. Verhältnis personenbezogener zu biometrischen Daten

Biometrische Daten (vgl. dazu oben I b aa) sind in Art. 4 Nr. 14 DS-GVO) legal definiert als „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder

42 Dazu insgesamt instruktiv Wolff/Brink/v. Ungern-Sternberg, BeckOK DatenschutzR/Albers/Veit, 46. Ed. 01.08.2023, DS-GVO Art. 9 Rn. 16.

43 Ausführlich Wolff/Brink/v. Ungern-Sternberg, BeckOK DatenschutzR/Albers/Veit, 46. Ed. 01.08.2023, DS-GVO Art. 9 Rn. 16.

44 Näher bei Voßkuhle/Eifert/Möllers VerwR/Albers § 22 Rn. 15 ff., 41.

45 Vgl. auch Herbst NVwZ 2016, 902 ff.; aus der Rspr. etwa BVerwG NVwZ 2020, 1114 (1117).

46 So auch Wolff/Brink/v. Ungern-Sternberg, BeckOK DatenschutzR/Albers/Veit, 46. Ed. 01.08.2023, DS-GVO Art. 9 Rn. 16.

47 Kritisch dazu Wolff/Brink/v. Ungern-Sternberg, BeckOK DatenschutzR/Albers/Veit, 46. Ed. 01.08.2023, DS-GVO Art. 9 Rn. 16.

48 Wolff/Brink/v. Ungern-Sternberg, BeckOK DatenschutzR/Veit, 46. Ed. 01.08.2023, DS-GVO Art. 9 Rn. 16.

bestätigen, wie Gesichtsbilder oder daktyloskopische Daten" (vgl. dazu auch Erwägungsgrund 51 der DS-GVO). Diese eigene Schutzkategorie der eindeutig identifizierenden Biometriedaten[49] ist demnach eine Teilmenge aller personenbezogenen Daten des Art. 4 Nr. 1 DS-GVO und aufgrund der Anknüpfung an bestimmte Merkmale und ihr Identifizierungspotenzial erheblich konturschärfer als die Gesamtmenge personenbezogener Daten.

Soweit die zukunftsgerichtete Einordnung und Bewertung der Nützlichkeit und des Risikopotenzials personenbezogener Daten in Rede steht, empfiehlt es sich daher, an die Kategorie biometrischer Daten anzuknüpfen und die Unwägbarkeiten allgemeiner personenbezogener Daten zu vermeiden.

II.3. Schutz der Daten von Kindern durch die DS-GVO

Die Datenschutz-Grundverordnung schützt personenbezogene Daten, auch diejenigen von Kindern. Dass Kindern darüber hinaus einen besonderen Schutz verdienen, ergibt sich bereits aus der EU-Grundrechte-Charta.[50] Dort heißt es in Artikel 24: „Rechte des Kindes

> (1) Kinder haben Anspruch auf den Schutz und die Fürsorge, die für ihr Wohlergehen notwendig sind. Sie können ihre Meinung frei äußern. Ihre Meinung wird in den Angelegenheiten, die sie betreffen, in einer ihrem Alter und ihrem Reifegrad entsprechenden Weise berücksichtigt.
>
> (2) Bei allen Kinder betreffenden Maßnahmen öffentlicher oder privater Einrichtungen muss das Wohl des Kindes eine vorrangige Erwägung sein."

Dies legt einen spezifischen Schutz der Daten von Kindern in der DS-GVO nahe.

aa) DS-GVO zur Schutzbedürftigkeit von Kinderdaten: Eine Analyse der DS-GVO erhellt, dass diese die **besondere Schutzbedürftigkeit von Kindern** in einer Reihe von Vorschriften durchaus anerkennt.[51]

Nach Art. 6 Abs. 1 lit. f DS-GVO ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn „die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich [ist], sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, **insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt"**. Hier trägt die DS-GVO also dem Umstand Rechnung, dass legitime Verarbeitungsinteressen von Verantwortlichen stärker zurücktreten müssen, wenn diese Daten von Kindern verarbeiten.

Woraus sich das gesteigerte Schutzbedürfnis von Kindern bei der Verarbeitung ihrer personenbezogenen Daten ergibt, erschließt sich (zumindest ansatzweise) aus Erwägungsgründen. Erwägungsgründe europäischer Rechtsakte werden im Gesetzgebungsprozess mitberaten und dienen der Auslegung der Verordnungs-Artikel, können diese jedoch nicht verdrängen. In Erwägungsgrund 38 der DS-GVO heißt es:

> „Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind."

---

49 Kühling/Buchner/Weichert, 4. Aufl. 2024, DS-GVO Art. 9 Rn. 32.

50 Der besondere Schutzbedarf ist im Recht anerkannt, vgl. Roßnagel, Der Datenschutz von Kindern in der DS-GVO, ZD 2020, 88.

51 Dazu Roßnagel, Der Datenschutz von Kindern in der DS-GVO, ZD 2020, 88.

Diese Begründung ist zwar sicherlich nicht als abschließend zu betrachten; weitere Gründe für die Schutzbedürftigkeit lassen sich etwa auch aus der besonderen Dauer der Verarbeitungsmöglichkeiten personenbezogener Kinderdaten oder der – ebenfalls zeitlich gesteigerten – Unabsehbarkeit der Verwendungsszenarien dieser Daten ableiten. Aber mit den Aspekten des eingeschränkten Risikobewusstseins von Kindern und ihrer erst zu entwickelnden Fähigkeiten, eigene Rechte planvoll wahrzunehmen, hat die DS-GVO hier jedenfalls zwei valide Schutzgründe benannt.

Einer Reihe weiterer Vorschriften der DS-GVO lässt sich klar entnehmen, dass die DS-GVO die mit Art. 24 der EU-Grundrechte-Charta vorgegebene besondere Schutzbedürftigkeit von Kindern anerkennt und in den Regelungskanon aufnimmt:

So bestimmt Art. 12 Abs. 1 DS-GVO im KapitΩel III (Recht der betroffenen Person) in Abschnitt 1 (Transparenz und Modalitäten):

> „(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen […] in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten."

Gerade bei der Bereitstellung der für Betroffene essenziellen Informationen über die Verarbeitung ihrer personenbezogenen Daten „denkt" der europäische Gesetzgeber also besonders an Kinder und ihre entwicklungsbedingt eingeschränkten Möglichkeiten, derlei Informationen umfassend aufzunehmen und zu verstehen.

Erwägungsgrund 58 bestimmt hierzu:

> „Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden. […] Wenn sich die Verarbeitung an Kinder richtet, sollten aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann."

Ähnliche Berücksichtigungen der gesteigerten Schutzbedürftigkeit von Kindern bei der Verarbeitung ihrer personenbezogenen Daten finden sich auch zu Kapitel IV (Verantwortlicher und Auftragsverarbeiter), in welchem die Pflichten des Verantwortlichen zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen (sog. TOMs) statuiert werden. In Erwägungsgrund 75 heißt es zu Art. 24 DS-GVO daher weiter:

> „Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn […] personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden".

Damit erkennt die DS-GVO die Notwendigkeit einer kindgerechten Sprache bei der Erfüllung der datenschutzrechtlichen Informationspflichten an.[52]

52 Roßnagel, Der Datenschutz von Kindern in der DS-GVO, ZD 2020, 88 ff.

Auch das Betroffenenrecht auf Löschung personenbezogener Daten (Art. 17 DS-GVO, „Recht auf Vergessenwerden“) nimmt die Situation von Kindern in den Blick, wenn es in Erwägungsgrund 65 wie folgt ausgestaltet wird:

> „Dieses Recht ist insbesondere wichtig in Fällen, in denen die betroffene Person ihre Einwilligung noch im Kindesalter gegeben hat und insofern die mit der Verarbeitung verbundenen Gefahren nicht in vollem Umfang absehen konnte und die personenbezogenen Daten — insbesondere die im Internet gespeicherten — später löschen möchte. Die betroffene Person sollte dieses Recht auch dann ausüben können, wenn sie kein Kind mehr ist.“

Die DS-GVO erkennt also an, dass sich aus der Schutzbedürftigkeit von Kindern ein Recht auf Löschung von sog. „Jugendsünden“[53] ergeben kann.

Hieraus lässt sich ableiten, dass die DS-GVO in einer Reihe von Vorschriften (und den dazugehörigen Erwägungsgründen) die besondere Schutzbedürftigkeit von Kindern durchaus adressiert und erweiterte materiellrechtliche Anforderungen an die Rechtmäßigkeit der Verarbeitung personenbezogener Daten von Kindern stellt.

bb) Besonderer prozeduraler Schutz von Kindern: Auf die besondere Schutzbedürftigkeit von Kindern wird von der DS-GVO nicht nur durch erweiterte materiellrechtliche Anforderungen an die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten von Kindern reagiert, sie nutzt auch verfahrensmäßige Möglichkeiten des Kinderschutzes. Hier ist auf Art. 57 Abs. 1 lit. b DS-GVO hinzuweisen, der sich mit den gesetzlichen Aufgaben der Datenschutz-Aufsichtsbehörden befasst und es zu den Aufgaben der Datenschutz-Aufsichtsbehörden zählt, „die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung zu sensibilisieren und sie darüber aufzuklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder.[54] Durch diese Anordnung der „besonderen Beachtung“ spezifischer Maßnahmen der Aufsichtsbehörden für Kinder im Rahmen der öffentlichkeitsorientierten Sensibilisierung für Fragen des Datenschutzes wird den Behörden zur Pflicht gemacht, solche Maßnahmen zu entwickeln und umzusetzen und dies mit gesteigertem Nachdruck unter erhöhtem Einsatz ihrer sächlichen und personellen Mittel zu tun.

Tatsächlich lässt sich bei einigen Aufsichtsbehörden auch erkennen, dass dieser Gesetzesauftrag der DS-GVO zugunsten von Kindern wahrgenommen und umgesetzt wird.[55]

cc) Sondernorm zu KI Art. 22 DS-GVO: Von besonderer, hier gleich in zweifacher Hinsicht großer Bedeutung ist die Norm des Art. 22 DS-GVO (Automatisierte Entscheidungen im Einzelfall einschließlich Profiling). Ihr Absatz 1 lautet:

> „Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.“

Damit ist zum einen die im Kontext von Werbemaßnahmen relevante Frage der Profilbildung einzelner Betroffener angesprochen, welche in der Erhebung ihrer personenbezogenen Daten zum Zwecke der Zuordnung zu Kategorien von Interessen und Eigenschaften besteht, die eine zielgerichtete „personalisierte“ Werbung erleichtert.

---

53 Roßnagel, Der Datenschutz von Kindern in der DS-GVO, ZD 2020, 88 ff.
Zum durchaus problematischen Begriff sei auf Art. 17 e der UN-Kinderrechtskonvention verwiesen.

54 Ähnlich die Aufgabe des KI-Gremiums in Art. 66 lit. f KI-VO.

55 Vgl. etwa das länderübergreifende Portal Young Data unter https://youngdata.de oder die Aktivitäten des LfDI Baden-Württemberg unter https://www.baden-wuerttemberg.datenschutz.de/datenschutz-kinderleicht/, abgerufen am 18.01.2025.

Zum Verbot des sogenannten Profiling (gemäß Art. 22 DS-GVO) erläutert Erwägungsgrund 71:

> „Die betroffene Person sollte das Recht haben, keiner Entscheidung — was eine Maßnahme einschließen kann — zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wie die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen. Zu einer derartigen Verarbeitung zählt auch das ‚Profiling', das in jeglicher Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person besteht, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. […] Diese Maßnahme sollte kein Kind betreffen."

Mit diesem Verbot des Profilings von Kindern trifft die DS-GVO eine der wenigen klaren und eindeutigen Schutzmaßnahmen zugunsten von Minderjährigen. Die Durchsetzung dieses Verbots leidet allerdings darunter, dass die Minderjährigkeit der Betroffenen für Verarbeiter nicht offensichtlich sein muss und zum anderen den Aufsichtsbehörden die Mittel fehlen, die Profilierung von Kindern und den Handel mit solchen Profildaten aufzuklären und zu ahnden.

Zum anderen verdient Art. 22 DS-GVO besondere Beachtung, weil er mit dem Verbot automatisierter Entscheidungen eine erst mit dem Aufstieg der Anwendungen KünstlicherIntelligenz vollständig beachtete Norm darstellt, welche die Nutzung von KI-Anwendungen massiv einschränkt.

KI stellt eine ökonomisch hochrelevante Innovation dar, die gerade dort besonders wertschöpfend eingesetzt werden kann, wo eine Vielzahl zwar nicht komplexer, aber häufiger und vielschrittiger Entscheidungen zu treffen sind. Gute Beispiele dafür sind das Erkennen von Personen in großen Menschenmengen anhand zuvor erhobener Identifikatoren (z.B. Gesichtserkennung in der Öffentlichkeit), die Auswahl von passend qualifizierten Beschäftigten aus einer Vielzahl von Bewerber*innen oder die Ermittlung von Auffälligkeiten aus einem Strom von Finanzdaten (im Wege der Mustererkennung). Hier werden Entscheidungen in automatisierten Verfahren vorgelagert getroffen, bei richtigem Verständnis eröffnet sich damit ein Anwendungsfeld für das Verbot der Art. 22 DS-GVO. Dies ist in seinen Folgen deswegen so relevant, da Art. 22 DS-GVO mit dem Verbot, der KI Entscheidungen zu überlassen, und dem Einfordern einer (zumindest nachgelagerten) menschlichen Kontrolle die erwartbaren Effizienzgewinne aus dem Einsatz von KI massiv schmälert oder gar vernichtet – hier kollidieren ökonomische Interessen offensichtlich mit dem verbreiteten Human-in-the-Loop-Ansatz.

Dieser zweite, für die weitere wirtschaftliche Nutzung von Verfahren der KI zentrale Aspekt, weist allerdings keine Verbindung zum Thema Kinderschutz im Rahmen der DS-GVO auf.

dd) Nur eingeschränkt relativer Schutz durch DS-GVO: Die DS-GVO verfolgt also **keinen absoluten Schutz von Kindern**. Obwohl zumindest die wirtschaftliche Verwertung der personenbezogenen Daten von Kindern aus guten Gründen verboten werden könnte, hat sich der EU-Gesetzgeber gegen ein solches Schutzniveau entschieden. Er hat stattdessen einen **bloß relativen Schutz** personenbezogener Kinderdaten statuiert – und selbst diesen **differenziert er nach Lebensaltersstufen**: Unter 13 Jahren erfahren Minderjährige einen vollständigen Schutz, ab dem Alter von 16 Jahren wird dieser Schutz jedoch erheblich eingeschränkt.

So bestimmt etwa Art. 8 DS-GVO hinsichtlich der „Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft“ in Abs. 1: „Gilt Artikel 6 Absatz 1 Buchstabe a bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat. Hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird. Die Mitgliedstaaten können durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.“

Im Spannungsfeld zwischen Schutz- und Beteiligungsrechten ist der Schutz personenbezogener Kinderdaten ab dem 16. Lebensjahr von der eigenen Entscheidung des Minderjährigen abhängig und damit erheblich eingeschränkt; zwischen dem 13. und 16. Lebensjahr des Minderjährigen obliegt der Schutz der Kinderdaten dem Willen der Sorgeberechtigten, ist also ebenfalls eingeschränkt.

In Erwägungsgrund 38 heißt es dazu:

> „Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Ein solcher besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen. Die Einwilligung des Trägers der elterlichen Verantwortung sollte im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein.“

Auch hier wird erkennbar: Einen vollständigen Schutz von Kindern strebt die DS-GVO nicht an, dieser beschränkt sich auf bestimmte Altersgruppen und Verarbeitungszwecke (Werbezwecke, Erstellung von Persönlichkeits- oder Nutzerprofilen). Auch die gesetzlichen Modalitäten des Schutzes – etwa die Maßgaben für elterliche Information und Einwilligung – belegen, dass **keineswegs an einen umfassenden Kinderschutz** gedacht wird. So verpflichtet Art. 8 Abs. 2 DS-GVO den Verantwortlichen für die Verarbeitung von Kinderdaten lediglich dazu „unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen (zu unternehmen), um sich in solchen Fällen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde“. Auch hier wird also zugunsten der ungestörten Verarbeitung (und wirtschaftlichen Verwertung)[56] von Kinderdaten vom Gesetzgeber in Kauf genommen, dass elterliche Schutzbemühungen leerlaufen, weil nicht sie, sondern Dritte (ggf. auch das Kind selbst) ihre Einwilligung fingieren. Weitere Schutzmöglichkeiten zugunsten Minderjähriger lässt die DS-GVO bewusst aus und behandelt in weiten Bereichen Kinder wie Erwachsene[57]: Sei es bei internationalen Datentransfers nach Art. 44 ff. DS-GVO, bei Zweckänderungen gemäß Art. 6 Abs. 4 DS-GVO oder bei der Einwilligung in die Verarbeitung sensibler Daten nach Art. 9 Abs. 2 lit. a DS-GVO. Auch die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO wird nicht auf Fälle der Verarbeitung von Kinderdaten erweitert, technisch-organisatorische Pflichten werden durch die Wahrscheinlichkeit, auch Kinderdaten zu verarbeiten, nicht schärfer.[58] Der Schutz von Kindern ist in der DS-GVO also durchaus angelegt, allerdings ist er nicht prioritär und auch nicht konsequent durchgehalten.

56 Zum Schutz von Kindern vor wirtschaftlicher Ausbeutung vgl. Art. 32 UN-Kinderrechtskonvention.

57 Roßnagel, Der Datenschutz von Kindern in der DS-GVO, ZD 2020, 88 ff.

58 Kritisch auch Roßnagel, Der Datenschutz von Kindern in der DS-GVO, ZD 2020, 88 ff.

Um mit Roßnagel zu sprechen: „Die DS-GVO schützt Kinder nur punktuell, jedoch nicht in allen Situationen, in denen ein besonderer Schutz erforderlich ist. Hinter den wenigen Regelungen ist kein Gesamtkonzept erkennbar."[59]

Die DS-GVO hat die Aufgabe eines besonderen Datenschutzes für Kinder zwar erkannt, aber bisher nur punktuell und daher weder konzeptionell noch situativ ausreichend gelöst.[60] Im Vordergrund steht der allgemeine Schutz personenbezogener Daten, die vor wirtschaftlicher Ausbeutung, staatlichem Übergriff und technischer Gefährdung bewahrt werden sollen. Personenbezogene Daten von Kindern genießen dabei durchaus einen besonderen Schutz, der in mehreren Vorschriften der DS-GVO zum Ausdruck kommt – dem allerdings kein so hoher Stellenwert wie besonderen Kategorien personenbezogener Daten (Art. 9 DS-GVO – zu denen auch biometrische Daten zählen) zukommt und zu dessen Gunsten auch keine Sondernormen wie die Art. 85 ff. DS-GVO erlassen wurden (Schutz der Meinungs- und Pressefreiheit Art. 85 DS-GVO, der Informationsfreiheit Art. 85, 86 DS-GVO, von Beschäftigtendaten Art. 88 DS-GVO oder der Forschungsfreiheit Art. 89 DS-GVO). **Kinderschutz ist demnach ein durchaus relevantes, aber kein überragend wichtiges Gut der DS-GVO.**

Dies sollte bei der Bewertung der Frage berücksichtigt werden, ob die Rechte von Kindern und Jugendlichen vor den Gefahren des digitalen Zeitalters durch die DS-GVO hinreichend geschützt werden – die Antwort hierauf heißt eindeutig: Nein.

Die Schutzbedürftigkeit von Kindern und die besonderen Risiken der Verarbeitung von biometrischen Daten in Verfahren der KI sind vor diesem Hintergrund herauszuarbeiten.

59 Roßnagel, Der Datenschutz von Kindern in der DS-GVO, ZD 2020, 88 ff., 90.

60 Roßnagel, Der Datenschutz von Kindern in der DS-GVO, ZD 2020, 88 ff., 92.

III. Einordnung biometrischer Daten in den Kontext von DS-GVO, DSA, KI-Verordnung und weiteren relevanten Gesetzgebungen

Die DS-GVO ist nicht die alleinige relevante europäische Gesetzgebung, wenn es um die Nutzung biometrischer Kinderdaten geht.

III.1. Digital Services Act

Der Digital Services Act (DSA, Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG) ist eine Verordnung der Europäischen Union, um einheitliche[61] europäische Haftungs- und Sicherheitsvorschriften für digitale Plattformen, Dienste und Produkte zu schaffen. Durch die Pflicht der Online-Plattformen zur Moderation von Online-Inhalten soll er insbesondere die Verbreitung illegaler und „schädlicher" (harmful) Inhalte (Straftaten, „Hass und Hetze" sowie Desinformation) zurückdrängen und Internet-Nutzer*innen damit besser schützen. Im Zeitalter des sog „Plattformkapitalismus"[62] dient er damit der besseren Durchsetzung europäischer Rechtsmaßstäbe, die gesetzlichen Pflichten sind dabei nach Unternehmensgröße gestaffelt: Die „sehr großen" Online-Plattformen und Suchmaschinen wie Facebook, Wikipedia oder Google Search müssen einige Vorschriften bereits ab November 2022 befolgen. Dazu gehören die zentralen Risikobewertungen, welche den Grundstein für die Vorsorgemaßnahmen der Plattformen legen sollen. Seit dem 17. Februar 2024 gilt die Verordnung für alle digitalen Akteure.[63] Online-Plattformen und Suchmaschinen können mit Geldbußen von bis zu 6 Prozent ihres weltweiten Umsatzes belegt werden, für sehr große Online-Plattformen (mit mehr als durchschnittlich monatlich 45 Millionen aktiven Nutzer*innen des Dienstes[64]) ist die EU-Kommission Aufsichtsbehörde. Minderjährige genießen den besonderen Schutz des DSA: Plattformen, die von Miderjährigen genutzt werden, müssen besondere Maßnahmen zu deren Schutz ergreifen, u.a. gilt ein vollständiges Verbot zielgerichteter Werbung (targeted advertising).

aa) Personenbezogene Daten
Zwar knüpft der DSA an verschiedenen Stellen an das Tatbestandsmerkmal „personenbezogene Daten" an (vgl. Art. 26 Abs. 3 DSA bzw. Art. 39 Abs. 1 Satz 2 DSA), der Schutz von Einzelpersonen bei der Verarbeitung personenbezogener Daten wird jedoch einzig durch die einschlägigen Vorschriften des Unionsrechts in diesem Bereich geregelt, insbesondere durch die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG (vgl. Erwägungsgrund 10 Abs. 3 DSA). Demnach ist für die Definition und den Schutzumfang personenbezogener Daten allein auf die DS-GVO abzustellen.

bb) Biometrische Daten
Ähnlich stellt sich die Rechtslage in Bezug auf biometrische Daten dar: Zwar nimmt Art. 26 Abs. 3 DSA auf „sensible" Daten Bezug („Die Anbieter von Online-Plattformen dürfen Nutzern keine Werbung anzeigen, die auf Profiling gemäß Artikel 4 Nummer 4 der Verordnung (EU) 2016/679 unter Verwendung besonderer Kategorien personenbezogener

61 Zuvor galt das deutsche Netzwerkdurchsetzungsgesetz vom 1. September 2017, BGBl. I S. 3352.

62 Stefan Krempl, Digital Services Act: Rechtliches Betriebssystem gegen das wilde Netz. In: heise online vom 16. Dezember 2020.

63 Zusammenfassung der Gesetzgebung in EUR-Lex (Amt für Veröffentlichungen der Europäischen Union), https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM:4625430, abgerufen am 03.02.2025.

64 https://ec.europa.eu/commission/presscorner/detail/de/ip_23_2413, abgerufen am 18.01.2025.

Daten gemäß Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 beruht“) und reguliert damit auch die Verarbeitung biometrischer Daten – verweist dabei allerdings auf die DS-GVO, welche somit maßgeblich bleibt (vgl. Erwägungsgrund 94).

cc) Daten von Kindern/Minderjährigen

Umfangreicher sind die Bestimmungen des DSA zu Minderjährigen und ihrem Schutz im Kontext digitaler Plattformen, Dienste und Produkte. Eine Vielzahl allgemeiner Schutzmaßnahmen zugunsten von Minderjährigen enthält Artikel 28 zum Online-Schutz Minderjähriger. Dort ist bestimmt:

> „(1) Anbieter von Online-Plattformen, die für Minderjährige zugänglich sind, müssen geeignete und verhältnismäßige Maßnahmen ergreifen, um für ein hohes Maß an Privatsphäre, Sicherheit und Schutz von Minderjährigen innerhalb ihres Dienstes zu sorgen.(2) Anbieter von Online-Plattformen dürfen auf ihrer Schnittstelle keine Werbung auf der Grundlage von Profiling gemäß Artikel 4 Absatz 4 der Verordnung (EU) 2016/679 unter Verwendung personenbezogener Daten des Nutzers darstellen, wenn sie hinreichende Gewissheit haben, dass der betreffende Nutzer minderjährig ist.“

Neben der allgemein gehaltenen Vorgabe eines „hohen Maßes an Privatsphäre“ enthält Art. 28 DSA allerdings keine spezifischen Schutzvorgaben – insbesondere nicht zum hier interessierenden Schutz biometrischer Kinderdaten vor KI-Verarbeitungen. Das faktisch niedrige Schutzniveau wird auch dadurch bestimmt, dass die Anbieter der Online-Plattformen die Minderjährigkeit ihrer Nutzer*innen nicht eigens feststellen müssen (vgl. Art. 28 Abs. 3 DSA: „Zur Einhaltung der in diesem Artikel festgelegten Verpflichtungen sind die Anbieter von Online-Plattformen nicht verpflichtet, zusätzliche personenbezogene Daten zu verarbeiten, um festzustellen, ob der Nutzer minderjährig ist.“). Damit läuft der Schutzansatz praktisch ins Leere. Daran ändert auch die Bezugnahme auf das besondere Schutzbedürfnis von Kindern (etwa in Erwägungsgrund 12, welcher die „Weitergabe von Darstellungen sexuellen Missbrauchs von Kindern“ beispielhaft erwähnt) oder die Beteuerung in Erwägungsgrund 71 nichts: „Der Schutz von Minderjährigenist ein wichtiges politisches Ziel der Union.“ Ein tatsächlicher Schutz setzt erst dann ein, wenn sich der Dienst „an Minderjährige richtet“ oder „überwiegend von Minderjährigen genutzt wird“ oder wenn „dem Anbieter in anderer Weise bekannt ist, dass einige seiner Nutzer minderjährig sind“. Dies ist allerdings nicht durchgehend der Fall, ein konsequenter Schutz Minderjähriger wird vom DSA also keineswegs umfassend sichergestellt. Teilweise sind die Schutzvorgaben auch auf Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen beschränkt (Erwägungsgrund 89). Andere Vorgaben an die Anbieter bleiben vage und unverbindlich (Erwägungsgrund 71: „Sie sollten bewährte Verfahren und die verfügbare Anleitung – etwa jene in der Mitteilung der Kommission mit dem Titel „Eine digitale Dekade für Kinder und Jugendliche: die neue europäische Strategie für ein besseres Internet für Kinder (BIK+)“ – berücksichtigen.“) Konsequenter sind die Schutzvorschriften des DSA lediglich in Bezug auf Werbung/Profiling bei Minderjährigen (vgl. Erwägungsgrund 95) Auch bei der Ermittlung und Bewertung systemischer Risiken von Online-Angeboten wird regelmäßig auf das Schutzbedürfnis von Kindern eingegangen, etwa in Artikel 34 DSA (Risikobewertung), der die in Artikel 24 der EU-Grundrechte-Charta verankerten Rechte des Kindes (lit. b) und Minderjährige als Schutzgruppe (lit. d) erwähnt.[65]

Auch hier sind allerdings nur die Anbieter sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen adressiert. Gleiches gilt für die Pflichten zur Risikominimierung in Artikel 35 DSA. Dort werden unter den Risikominderungsmaßnahmen u.a. aufgeführt (lit. j): „gezielte Maßnahmen zum Schutz der Rechte des Kindes, darunter auch Werkzeuge zur Altersüberprüfung und zur elterlichen Kontrolle sowie Werkzeuge, die es Minderjährigen ermöglichen sollen, Missbrauch zu melden bzw. Unterstützung zu erhalten“

65 Vgl. dazu insbesondere Erwägungsgrund 83 DSA.

(vgl. dazu auch Erwägungsgrund 81, der es zu den Risiken im Zusammenhang mit der Gestaltung von Online-Schnittstellen zählt, absichtlich oder unabsichtlich die Schwächen und Unerfahrenheit von Minderjährigen aus(zu)nutzen oder Suchtverhalten zu fördern; dazu auch Erwägungsgrund 104 mit dem Verweis auf negative Auswirkungen auf Minderjährige, etwa die Ausnutzung einer Gewinnerzielungsabsicht, die für schutzbedürftige Nutzer wie z. B. Minderjährige besonders schädlich seien).

Schließlich betont auch der DSA die Notwendigkeit, Informationspflichten so nachzukommen, dass auch Minderjährige davon profitieren können (zur kindgerechten Gestaltung von Informationspflichten vgl. Art. 14 Abs. 3 DSA, Allgemeine Geschäftsbedingungen): „Richtet sich ein Vermittlungsdienst in erster Linie an Minderjährige oder wird er überwiegend von Minderjährigen genutzt, so erläutert der Anbieter von Vermittlungsdiensten die Bedingungen und jegliche Einschränkungen für die Nutzung des Dienstes so, dass Minderjährige sie verstehen können.“[66] Demnach weist der **DSA** durchaus Bestimmungen zu Minderjährigen und ihrem Schutz im Kontext digitaler Plattformen, Dienste und Produkte auf – der Schutz ist aber nur sporadisch, bleibt zum Teil auf besonders große Anbieter beschränkt und wird lediglich bei der auf Kinder zugeschnittenen Online-Werbung konkreter.

III.2. KI-Verordnung

Die Verordnung über künstliche Intelligenz (KI-Verordnung, KI-VO; englisch AI Act) ist ein Rechtsakt der Europäischen Union zur Regulierung von künstlicher Intelligenz (Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz). Seit 2019 verhandelt, wurde sie am 12. Juli 2024 verkündet; ihre Regelungen treten mit einigen Ausnahmen am 2. August 2026 in Kraft.[67]

Die KI-VO teilt KI-Technologien, darunter auch generative KI, in vier verschiedene Risikokategorien auf, von „KI-Systemen mit inakzeptablem Risiko“ über „KI-Systeme mit hohem Risiko“ und „KI-Systeme mit Transparenzanforderungen“ bis hin zu „KI-Systemen mit keinem/niedrigem Risiko“. An diese Risikostufen werden unterschiedliche Verbote bzw. Compliance-, Berichts-, Dokumentations-, Sorgfalts- und Informationspflichten gekoppelt, die KI-VO setzt damit (ebenfalls) einen risikobasierten Ansatz um. So werden Technologien mit inakzeptablem Risiko wie Social Scoring oder biometrsche Videoüberwachung bzw. Gsichtserkennung oder automatisierte Emotionserkennung und Verhaltensbeeinflussung für private Anbieter vollständig verboten. Allerdings wurde ein Verbot von Predictive Policing (statistische Auswertung auf Wahrscheinlichkeit von Verbrechen) oder der biometrischen Überwachung (Auswertung biometrischer Daten in einer Echtzeit-Analyse) nicht in die KI-VO aufgenommen.[68]

66 Dazu auch Erwägungsgrund 46.

67 Vgl. https://www.wbs.legal/it-und-internet-recht/datenschutzrecht/fahrplan-nach-in-kraft-treten-ai-act-wird-schrittweise-anwendbar-81008/, abgerufen am 18.01.2025.

68 Zur Kritik vgl. Markus Reuter: Ampel verpasst Grundrechteschutz bei der Regulierung künstlicher Intelligenz, Netzpolitik.org. vom 7. Dezember 2022, https://netzpolitik.org/2022/ai-act-der-europaeischen-union-ampel-verpasst-grundrechteschutz-bei-der-regulierung-kuenstlicher-intelligenz/, abgerufen am 04.02.2025.

Zu den Hochrisiko-KI-Systemen zählen insbesondere auch Systeme, die biometrische Daten verarbeiten (Art. 6 Abs. 2 KI-VO, Anhang III Ziff. 1 a und b). Anbieter von Hochrisiko-KI-Systemen müssen u. a. ein Risikomanagementsystem einrichten, Anforderungen an die Datenqualität erfüllen und menschliche Aufsicht über die KI sicherstellen.[69]

Verstoßen Unternehmen gegen die KI-VO, drohen Strafen bis zu 7 Prozent des weltweiten Vorjahresumsatzes. Eine individuelle Rechtsdurchsetzung (wie sie etwa die DS-GVO mit Schadenersatzansprüchen in Art. 82 DS-GVO vorsieht) ermöglicht die KI-VO nicht.

aa) Personenbezogene Daten

Die KI-VO knüpft als Rechtsakt an KI-Technologien an, gilt also unabhängig davon, ob KI-Modelle oder -Systeme personenbezogene Daten verwenden oder beinhalten. Allerdings finden sich auch Regelungen in der KI-VO, die tatbestandlich an personenbezogene Daten anknüpfen. Dabei stellt Art. 2 Abs. 7 KI-VO zunächst klar, dass das Schutzregime der DS-GVO Vorrang genießt:

> „Die Rechtsvorschriften der Union zum Schutz personenbezogener Daten, der Privatsphäre und der Vertraulichkeit der Kommunikation gelten für die Verarbeitung personenbezogener Daten im Zusammenhang mit den in dieser Verordnung festgelegten Rechten und Pflichten. Diese Verordnung berührt nicht die Verordnung (EU) 2016/679 bzw. (EU) 2018/1725 oder die Richtlinie 2002/58/EG bzw. (EU) 2016/680, unbeschadet des Artikels 10 Absatz 5 und des Artikels 59 der vorliegenden Verordnung."

Dies bestätigt auch Erwägungsgrund 10:

> „Diese Verordnung soll die Anwendung des bestehenden Unionsrechts zur Verarbeitung personenbezogener Daten, einschließlich der Aufgaben und Befugnisse der unabhängigen Aufsichtsbehörden, die für die Überwachung der Einhaltung dieser Instrumente zuständig sind, nicht berühren. Sie lässt ferner die Pflichten der Anbieter und Betreiber von KI-Systemen in ihrer Rolle als Verantwortliche oder Auftragsverarbeiter, die sich aus dem Unionsrecht oder dem nationalen Recht über den Schutz personenbezogener Daten ergeben, unberührt, soweit die Konzeption, die Entwicklung oder die Verwendung von KI-Systemen die Verarbeitung personenbezogener Daten umfasst. Ferner sollte klargestellt werden, dass betroffene Personen weiterhin über alle Rechte und Garantien verfügen, die ihnen durch dieses Unionsrecht gewährt werden, einschließlich der Rechte im Zusammenhang mit der ausschließlich automatisierten Entscheidungsfindung im Einzelfall und dem Profiling."

Auch bei den einschlägigen Definitionen bedient sich die KI-VO bei der DS-GVO, etwa in Art. 3 Nr. 37 („besondere Kategorien personenbezogener Daten" nach Artikel 9 Absatz 1 DS-GVO) oder Art. 3 Nr. 50 („personenbezogene Daten" im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) 2016/679) bzw. Nr. 51 („nicht personenbezogene Daten"). Auch werden Transparenzpflichten der DS-GVO in Bezug genommen (Artikel 50 KI-VO, Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme).[70]

69 Vgl. Art. 8 ff. KI-VO.

70 Allerdings mit relevanten Ausnahmen in Art. 50 Abs. 3 Satz 2 KI-VO: „Diese Pflicht gilt nicht für gesetzlich zur Aufdeckung, Verhütung oder Ermittlung von Straftaten zugelassene KI-Systeme, die zur biometrischen Kategorisierung und Emotionserkennung im Einklang mit dem Unionsrecht verwendet werden, sofern geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen."

Ausnahmsweise[71] abweichende Regulierungen wie Artikel 10 (Daten und Daten-Governance; hier: Abs. 5 „Soweit dies für die Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen im Einklang mit Absatz 2 Buchstaben f und g dieses Artikels unbedingt erforderlich ist, dürfen die Anbieter solcher Systeme ausnahmsweise besondere Kategorien personenbezogener Daten verarbeiten, wobei sie angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen müssen.“) oder Art. 59 KI-VO (Weiterverarbeitung personenbezogener Daten zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse im KI-Reallabor; Abs. 1: „Rechtmäßig für andere Zwecke erhobene personenbezogene Daten dürfen im KI-Reallabor ausschließlich für die Zwecke der Entwicklung, des Trainings und des Testens bestimmter KI-Systeme im Reallabor verarbeitet werden, wenn alle der folgenden Bedingungen erfüllt sind: […]“) bestätigen eher diese grundsätzliche Zuordnung. [72]

bb) Biometrische Daten

Auch zu biometrischen Daten verhält sich die KI-VO. Sie knüpft in Art. 3 Nr. 34 KI-VO an die vorrangige Definition in Art. 4 Nr. 14 DS-GVO an[73], differenziert dann jedoch weiter zwischen „biometrischer Identifizierung“ (Art. 3 Nr. 35) und „biometrischer Verifizierung“ (Art. 3 Nr. 36). Im differenzierten Risikosystem finden sich KI-Systeme im Bereich der Biometrie in ANHANG III der KI-VO als Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2 KI-VO „Nr. 1 Biometrie, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

a) biometrische Fernidentifizierungssysteme. Dazu gehören nicht KI-Systeme, die bestimmungsgemäß für die biometrische Verifizierung, deren einziger Zweck darin besteht, zu bestätigen, dass eine bestimmte natürliche Person die Person ist, für die sie sich ausgibt, verwendet werden sollen;

b) KI-Systeme, die bestimmungsgemäß für die biometrische Kategorisierung nach sensiblen oder geschützten Attributen oder Merkmalen auf der Grundlage von Rückschlüssen auf diese Attribute oder Merkmale verwendet werden sollen“.

Zur Erläuterung dieser Einstufung führt Erwägungsgrund 54 KI-VO aus: „Da biometrische Daten eine besondere Kategorie personenbezogener Daten darstellen, sollten einige kritische Anwendungsfälle biometrischer Systeme als hochriskant eingestuft werden, sofern ihre Verwendung nach den einschlägigen Rechtsvorschriften der Union und den nationalen Rechtsvorschriften zulässig ist.“

Insgesamt arbeitet die KI-VO also durchaus mit den Tatbestandsmerkmalen „personenbezogene Daten“ und „biometrische Daten“, knüpft dabei allerdings in untergeordneter Weise an die Vorgaben der DS-GVO an.

---

71 Vgl. zum Grundsatz Erwägungsgrund 63: „Diese Verordnung sollte nicht so verstanden werden, dass sie eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten, gegebenenfalls einschließlich besonderer Kategorien personenbezogener Daten, bildet, es sei denn, in dieser Verordnung ist ausdrücklich etwas anderes vorgesehen.“

72 Dazu Erwägungsgrund 69: „Das Recht auf Privatsphäre und den Schutz personenbezogener Daten muss während des gesamten Lebenszyklus des KI-Systems sichergestellt sein.“

73 Vgl. Erwägungsgrund 14: „Der in dieser Verordnung verwendete Begriff „biometrische Daten“ sollte im Sinne des Begriffs „biometrische Daten“ nach Artikel 4 Nummer 14 der Verordnung (EU) 2016/679, Artikel 3 Nummer 18 der Verordnung (EU) 2018/1725 und Artikel 3 Nummer 13 der Richtlinie (EU) 2016/680 ausgelegt werden.“

cc) Daten von Kindern
Im Normtext der KI-VO ist nicht ausdrücklich von Kindern oder Minderjährigen die Rede, allerdings nimmt Art. 5 KI-VO, der „Verbotene Praktiken im KI-Bereich" auflistet, deutlich auf diese Gruppe Bezug, wenn er in Absatz 1 bestimmt: „Folgende Praktiken im KI-Bereich sind verboten:

[...]

b) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das eine **Vulnerabilität oder Schutzbedürftigkeit** einer natürlichen Person oder einer bestimmten Gruppe von Personen **aufgrund ihres Alters**, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation mit dem Ziel oder der Wirkung **ausnutzt**, das Verhalten dieser Person oder einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu verändern, die dieser Person oder einer anderen Person **erheblichen Schaden zufügt** oder mit hinreichender Wahrscheinlichkeit zufügen wird;"

Lediglich mittelbar ist der Bezug zu Kindern in Anhang III Nr. 3 KI-VO, wenn KI-Systeme im Bereich der „Allgemeinen und beruflichen Bildung" als Hochrisiko-KI-Systeme eingestuft werden.

Erst in Erwägungsgrund 9 ist von Minderjährigen die Rede, wenn auch ohne eigene Regelungsintention der KI-VO:

> „So sollten etwa die nationalen arbeitsrechtlichen Vorschriften und die Rechtsvorschriften zum Schutz **Minderjähriger**, nämlich Personen unter 18 Jahren, unter Berücksichtigung der Allgemeinen Bemerkung Nr. 25 (2021) des UNCRC über die Rechte der Kinder im digitalen Umfeld von dieser Verordnung unberührt bleiben, sofern sie nicht spezifisch KI-Systeme betreffen und mit ihnen andere legitime Ziele des öffentlichen Interesses verfolgt werden."

Einzig in Erwägungsgrund 48 KI-VO bekennt sich die KI-VO zur Schutzbedürftigkeit von Kindern, verweist aber auch hier auf andere Vorschriften als führend:

> „Es muss betont werden, dass **Kinder** — zusätzlich zu diesen Rechten — über spezifische Rechte verfügen, wie sie in Artikel 24 der Charta und im Übereinkommen der Vereinten Nationen über die Rechte des Kindes (UNCRC) — im Hinblick auf das digitale Umfeld weiter ausgeführt in der Allgemeinen Bemerkung Nr. 25 des UNCRC — verankert sind; in beiden wird die Berücksichtigung der Schutzbedürftigkeit der Kinder gefordert und ihr Anspruch auf den Schutz und die Fürsorge festgelegt, die für ihr Wohlergehen notwendig sind."

Laut **KI-Verordnung** liegt demnach durchaus ein erhöhtes Schutzbedürfnis für Kinder vor, dieses wird von der Verordnung allerdings nicht eigenständig ausgearbeitet. Vielmehr belässt es die KI-VO bei Verweisen auf andere einschlägige Schutzvorschriften. Zudem werden die in der KI-VO angelegten Ausnahmevorschriften – etwa beim KI-Einsatz zur Sicherung der nationalen Sicherheit oder bei Grenzkontrollen – unterschiedslos auch auf Kinder erstreckt. Minderjährige genießen hier demnach keinen besonderen Schutzstatus.

So könnten nach den Bestimmungen der KI-VO auch unter Terrorverdacht geratene Jugendliche KI-Anwendungen unterworfen werden, ohne dass ihre altersbedingte Schutzbedürftigkeit berücksichtigt würde. Auch der Einsatz KI-basierter Altersschätzung – etwa an der Staatsgrenze bei der Ein- oder Ausreise – ist von der KI-VO nicht weiter beschränkt.

Zwischenfazit

Ein angemessener Schutz der Rechte von Kindern und Jugendlichen vor den Gefahren des digitalen Zeitalters (hier: KI-Entwicklung und -Anwendungen) kann daher allenfalls aus der Zusammenschau der Schutzwirkungen mehrerer Gesetze (vgl. DS-GVO, KI-VO bzw. DSA) erzielt werden – bedürfte aber noch **zusätzlicher gesetzgeberischer Anstrengungen**, ggf. auch in einem eigens auf die Rechte und Interessen von Kindern und Jugendlichen zugeschnittenen Rechtsakt.

Ein solcher Rechtsakt kann wegen der Vorrangwirkung europäischen Rechts nur auf europäischer Rechtssetzungsebene verortet werden und sollte, da EU-Richtlinien sich in den vergangenen Jahrzehnten als nur bedingt steuerungsfähig erwiesen haben, in Gestalt einer Verordnung erlassen werden. Damit wäre seine unmittelbare, nationales Recht in der Anwendung verdrängende Regulierung möglich, die fundamentale Rechte von Kindern in der digitalen Lebenswelt wirksam absichert.

Ausgehend von einer Schutzbedarfsanalyse müsste die **„Verordnung zum Schutz und zur Befähigung von Kindern in der digitalen Welt“** einerseits die Vulnerabilität von Minderjährigen erfassen und überwinden helfen, andererseits aber auch durchgehend berücksichtigen, dass Kindern eigene Rechte und je nach Entwicklungsstand selbst ausgeübte Freiheiten auch im Digitalen zustehen. Daher sollte der Rechtsakt insbesondere die folgenden Themen aufgreifen und regulieren:

- Zugang von Kindern zum Möglichkeitsraum Internet
- Schutzkonzepte zu altersbedingt besonders schädlichen Inhalten des Internets
- Schaffen eines Rechts auf Teilhabe und Befähigung zur Teilhabe im Digitalen
- Entwicklung des Schutzverhältnisses von Kindern und Sorgeberechtigten
- Entscheidungsmöglichkeiten bei Erreichen der Volljährigkeit
- Garantie eines Rechts auf unbelasteten Eintritt in die Volljährigkeit

Diesem Rechtsakt müsste zudem, um ein stimmiges Schutzkonzept darzustellen, Vorrangwirkung gegenüber den übrigen genannten Rechtsakten der Europäischen Union zukommen, um seine Schutzwirkung vollständig entfalten zu können.

IV. Entwicklung zulässiger Einsatzfelder für biometrische Kinderdaten in KI-Anwendungen

Mit Blick auf mögliche Einsatzfelder für biometrische Daten von Minderjährigen in KI-Anwendungen ergibt sich damit die folgende Ausgangslage: Die DS-GVO schränkt zwar den Einsatz biometrischer Daten erheblich ein, sieht aber keine prinzipiellen Erweiterungen dieses Schutzes personenbezogener Daten mit Blick auf Kinder vor. Das macht auch weder der DSA noch die KI-VO. Letztere verbietet zwar bestimmten Einsatzszenarien von KI, diese Verbote zielen aber nicht auf den erweiterten Schutz von Kindern, sondern sind auf bestimmte Einsatzzwecke der KI fokussiert.

Damit lassen sich – exemplarisch – Einsatzfelder herausarbeiten und eingrenzen, bei denen nach aktueller europäischer Rechtslage die Verwendung biometrischer Kinderdaten in KI-Anwendungen als rechtmäßig einzustufen ist.

Bevor diese Beispielsfälle eingehender erörtert werden, sollten mit Blick auf die Eigenarten der Entwicklung und des Einsatzes von KI-Modellen zwei Szenarien unterschieden und gleichsam „vor die Klammer gezogen" werden:

IV.1. Datenverarbeitung zum Training von Basismodellen

Künstliche Intelligenz begegnet uns heute in Form von Anwendungen, etwa als App für Chats (z.B. ChatGPT) oder als Unterstützungs-Tool bei alltäglichen Datenverarbeitungen (etwa Copilot im Microsoft Office). Diese Anwendungen basieren auf sog. **KI-Modellen**, also auf Programmen, die anhand einer Reihe von Daten trainiert wurden, um bestimmte Muster zu erkennen oder bestimmte Entscheidungen ohne weiteres menschliches Eingreifen zu treffen. Als Basismodelle wurden sie noch nicht auf einen konkreten Einsatzzweck hin trainiert,[74] bilden jedoch die Grundlage für LLMs oder Bilderkennung, die zu ihrem spezifischen Einsatzzweck ein weiteres spezialisiertes Training erfahren. Gleichzeitig sind diese vortrainierten Datensätze Grundlage fast aller im Einsatz befindlichen KI-Systeme. Modelle der künstlichen Intelligenz wenden unterschiedliche Algorithmen auf relevante Dateneingaben an, um die Aufgaben oder den Output zu erreichen, für die sie programmiert wurden.[75]

Sowohl das Programmieren von KI-Modellen als auch die Nutzung von KI-basierten Anwendungen kann Berührungspunkte zu personenbezogenen Daten haben: Das Training von KI-Modellen erfolgt unter Einsatz sehr großer Datenmengen, in denen auch personenbezogene Daten enthalten sein können. Zwar werden die Algorithmen der KI-Modelle selbst in der Regel keine personenbezogenen Daten umfassen, aber sie bilden jene personenbezogenen Daten in ihrer Struktur ab, mit denen sie trainiert wurden. Ob KI-Modelle daher selbst als personenbezogen anzusehen sind (und daher an der DS-GVO zu messen sind), bleibt umstritten – auch die Opinion des Europäischen Datenschutz-Ausschusses (EDSA) vom Dezember 2024[76] lässt diese Frage unbeantwortet[77] und weist die Entscheidung darüber den jeweils zuständigen Datenschutz-Aufsichtsbehörden zu. Hier stehen sich zwei Argumentationslinien

74 Eine datenschutzrechtliche Rechtfertigung (vgl. Art. 5 Abs. 1 lit. b DS-GVO) des Einsatzes personenbezogener Trainingsdaten kann also nicht über den Einsatzzweck erfolgen.

75 Vgl. etwa https://www.ibm.com/de-de/topics/ai-model „Was ist ein KI-Modell", abgerufen am 06.02.2025.

76 EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (Adopted on 17 December 2024).

77 „EDPB considers that AI models trained with personal data cannot, in all cases, be considered anonymous (a case-by-case basis)".

(„Die Digitalisierung hat nahezu alle Daten personenbeziehbar gemacht“ versus „In großen Datenmengen wie bei Trainingsdaten geht jeder Personenbezug notwendig verloren“) unversöhnlich gegenüber. Sicher ist hingegen, dass der Einsatz personenbezogener Daten zu Zwecken des Trainings eines KI-Modells der DS-GVO, insbesondere den Prinzipien des Art. 5 DS-GVO unterfällt.

Gewendet auf unsere Fragestellung lässt sich daher grundsätzlich sagen, dass die Nutzung biometrischer Kinderdaten zu **Zwecken des Trainings** einer KI einer gesetzlichen Basis aus Art. 6 Abs. 1 DS-GVO bedarf. Dabei kommt die naheliegendste Rechtsgrundlage, nämlich der praktisch bedeutsamste Art. 6 Abs. 1 lit. f DS-GVO (berechtigtes Interesse), vorliegend nicht zum Zuge, da diese auf einer Abwägung der berechtigten Verarbeitungsinteressen des Verantwortlichen mit den schutzwürdigen Interessen von Betroffenen beruhende Grundlage im Kontext besonders sensibler (besonderer Kategorien) personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO so gut wie niemals einschlägig sein wird: Die gebotene Abwägung schlägt wegen der Sensibilität biometrischer Daten zugunsten der Betroffenen aus; soweit es um den Einsatz von Kinderdaten geht, also um gesteigert schutzwürdige Daten, wird dieses Ergebnis praktisch unausweichlich.

Zwar kennt das Verarbeitungsverbot des Art. 9 DS-GVO Ausnahmen, in Abs. 2 finden sich aber nur wenige, die für den Einsatz von Kinderdaten zum Training einer KI nutzbar gemacht werden können: Eine Einwilligung (Art. 9 Abs. 2 lit. a DS-GVO) ist zumindest äußerst unpraktikabel, da das Modelltraining regelmäßig sehr große Datenmengen erfordert und diese Vielzahl von Einwilligungen (der Sorgeberechtigten) wohl nicht eingeholt werden könnten. Eher denkbar wäre eine Ausnahme im Kontext von Art. 9 Abs. 2 lit. c DS-GVO. Danach ist die Verarbeitung besonderer Kategorien personenbezogener Daten dann ausnahmsweise zulässig, wenn sie „zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich [ist] und die betroffene Person […] aus körperlichen oder rechtlichen Gründen außerstande [ist], ihre Einwilligung zu geben“. Hierauf wird in Beispiel 1 (Grenzkontrollen unter Einsatz KI-basierter Altersverifikation) näher eingegangen.

Denkbar wäre schließlich ein Einsatz biometrischer Kinderdaten zum Training eines KI-Modells für Zwecke der öffentlichen Gesundheit (Art. 9 Abs. 2 lit. i DS-GVO) bzw. Gesundheitsvorsorge (Art. 9 Abs. 2 lit. h DS-GVO), auf diese Konstellation geht Beispiel 2 näher ein. Das KI-Training auf das sog. Forschungsprivileg der DS-GVO zu stützen (vgl. Art. 9 Abs. 2 lit. j DS-GVO), liegt zwar nicht fern, zumal Art. 89 DS-GVO die Schutzstandards der DS-GVO im Forschungskontext massiv absenkt. Allerdings fordert Art. 9 Abs. 2 lit. j DS-GVO hierfür eine ausdrückliche gesetzliche Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats der EU, die bislang zugunsten des KI-Trainings nicht geschaffen wurde. Denkbar sind in diesem Kontext immer auch ein auf spezialgesetzlicher Grundlage erfolgendes KI-Training (Art. 9 Abs. 2 lit. g DS-GVO, Verarbeitung aufgrund erheblichen öffentlichen Interesses; dazu sogleich Beispiel 1), bislang wurden die Gesetzgeber hierfür jedoch nicht tätig; Art. 9 Abs. 4 eröffnet den Mitgliedstaaten vielmehr umgekehrt auch die Möglichkeit, solche Verarbeitungen biometrischer Daten weiter einzuschränken. Damit bleibt – jedenfalls für nicht-staatliche Akteure – letztlich nur die Einwilligung der Betroffenen (nach Art. 9 Abs. 2 lit. a i.V.m. Art. 6 Abs. 1 lit. a DS-GVO) als Basis für die Verarbeitung biometrischer Kinderdaten zu Zwecken des Trainings von KI-Modellen – und diese Einwilligungen sind im erforderlichen (riesigen) Umfang weder zu erlangen noch zu managen.

Daher lässt sich prognostizieren, dass wegen der strikten Vorgaben der DS-GVO ein Training von KI-Modellen mit biometrischen Kinderdaten wohl weit überwiegend **außerhalb der EU stattfinden wird** – und damit für europäische Wertvorstellungen unerreichbar bleibt. Dass dies sowohl unter wirtschaftlichen Gesichtspunkten als auch mit Blick auf die Gewährleistung des Kinderschutzes eine durchaus problematische Prognose ist, liegt auf der Hand.

IV.2. Datenverarbeitung im Rahmen der Nutzung von KI-Systemen

Auch bei der **Anwendung** von KI-Systemen kann es zur Nutzung biometrischer Kinderdaten kommen. Denkbar ist dies etwa dann, wenn der KI-Nutzer im Rahmen seiner Eingaben (prompts) solche personenbezogenen Daten dem KI-System zuführt, aber auch im Rahmen des Anwendungsprozesses, wenn das KI-System weitere Daten zur optimalen Erfüllung der Anwendungsaufgabe recherchiert (etwa im Internet erhebt).

Die Rechtslage stellt sich ähnlich dar wie zum Einsatz von Trainingsdaten für KI-Modelle dargelegt: Ohne ausdrückliche gesetzliche Grundlage hierfür kommt letztlich wieder nur Art. 6 Abs. 1 lit. a i.V.m. Art. 9 Abs. 2 lit. a DS-GVO in Betracht. Allerdings sind hier abweichend zwei wesentliche Aspekte zu beachten: Zum einen ist bei Anwendungsvorgängen eine einwilligungsbasierte Datenverarbeitung wesentlich plausibler darzustellen, jedenfalls soweit der Nutzer selbst seine biometrischen Daten in der Anwendung freigibt. Bei Minderjährigen wäre hier „nur" zu berücksichtigen, dass in der Regel die Sorgeberechtigten die Einwilligung abgeben bzw. genehmigen müssen. Zum anderen stellt sich, jedenfalls nach Auffassung des EDSA,[78] die Zusatzproblematik, dass nach der sog. **Infektionsthese** ein rechtswidriges Training von KI-Modellen auf die Rechtmäßigkeit der Nutzung der KI-Anwendung „durchschlagen" kann, also an sich rechtmäßige Verarbeitungen rechtswidrig macht. Diese Position des EDSA ist allerdings umstritten, sie findet in der DS-GVO, welche ansonsten die Rechtmäßigkeit von Verarbeitungsschritten jeweils separat beurteilt, auch wenig Stützung. Die Nutzung biometrischer Kinderdaten im Rahmen von KI-Anwendungen lässt sich demnach grundsätzlich einwilligungsbasiert rechtfertigen, bei Einholung der Einwilligung im Anwendungsprozess kann dies auch durchaus praktikabel sein.

IV.3. Art. 22 DS-GVO als Unikat

Nach Maßgabe der DS-GVO ist ein zweiter Aspekt beim Einsatz von KI zu beachten, der die Nutzbarkeit von KI-Anwendungen in der EU wesentlich beeinträchtigt: Als Unikat reguliert Art. 22 DS-GVO nicht die Verwendung personenbezogener Daten, sondern diskriminiert die Automatisierung von Entscheidungsprozessen. Danach hat jede Person „das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung […] beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt". Besondere Bedeutung hat Art. 22 DS-GVO, der bislang allenfalls im Bereich personalisierter Werbung (Profiling) eine gewisse Rolle spielte, durch eine Entscheidung des EuGH (sog. Schufa-Urteil)[79] erhalten, welche den Anwendungsbereich der Vorschrift erheblich ausweitete. Demnach soll unter „Entscheidung" i. S. v. Art. 22 Abs. 1 DS-GVO nicht nur das abschließende Votum in einer Entscheidungssituation zu verstehen sein, sondern auch bereits jede vorbereitende Handlung, auf welche sich der Verantwortliche „maßgeblich" stützt.[80]

78 EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (Adopted on 17 December 2024).

79 URTEIL DES GERICHTSHOFS (Erste Kammer) vom 7. Dezember 2023, C-634/21 https://curia.europa.eu/juris/document/document.jsf;jsessionid=689CCB95A2A8725D7D9595DF4CAEC509?text=&docid=280426&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=28920507.

80 „sofern von diesem Wahrscheinlichkeitswert maßgeblich abhängt, ob ein Dritter, dem dieser Wahrscheinlichkeitswert übermittelt wird, ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet", EuGH-Urteil vom 7. Dezember 2023, C-634/21, Entscheidungssatz.

Ob vom EuGH intendiert oder nicht, hat er damit die Einsatzmöglichkeiten von KI wesentlich beschränkt: Die angestrebten Effizienzgewinne kann der Einsatz von KI nur erzielen, wenn die „automatisierte Verarbeitung“ (der Einsatz KI-generierter und generierender Algorithmen) mit ihren Vorschlägen auch unmittelbar durchdringt und an die Stelle menschlicher Entscheidungen tritt. Jedes mehr als nur stichprobenartige menschliche „Nachprüfen“ der KI-Entscheidung mindert deren Effizienz in zeitlicher Hinsicht und schwächt die angestrebte Einheitlichkeit der Entscheidungsprozesse und -ergebnisse. Dies wird gegen Kinderrechte und Kindeswohl in Stellung gebracht werden, indem sinkende Effizienz als Wirtschaftsfaktor verstanden wird, der alle anderen Werte und Interessen verdrängt. Zwar kennt auch Art. 22 DS-GVO Ausnahmen von diesem Verbot, Abs. 2 lit. c lässt eine ausdrückliche Einwilligung der betroffenen Person zu (unter den Maßgaben des Abs. 3). Allerdings sieht Abs. 4 eine Gegenausnahme vor, soweit Entscheidungen nach Abs. 2 auf Art.-9-Daten beruhen. Die in Abs. 4 aufgeführten Rückausnahmen (Art. 9 Abs. 2 lit. a und g DS-GVO) sind für den hier untersuchten Einsatz biometrischer Daten von Kindern auf Einwilligungs- bzw. gesetzlicher Basis zwar einschlägig, bei KI-Anwendungen stellt sich wegen der massenhaften Datenverarbeitung jedoch sofort wieder die Frage nach der Praktikabilität, sämtliche Verarbeitungen auf Einwilligungsbasis abzuwickeln.

Gesetzliche Erlaubnisse des Einsatzes von KI in diesen Szenarien existieren bislang nicht.

IV.4. Drei Beispiele aus der Praxis

aa) Beispiel 1: Grenzkontrollen mit KI-gestützter Altersverifikation
Bei der Einreise von Migrant*innen ins Bundesgebiet können diesen unter Umständen keine in Deutschland anerkannten Identitätspapiere vorliegen, auch die Bundespolizei verfügt nur in Ausnahmefällen über Möglichkeiten der sicheren Identifikation. Dies hat zur Folge, dass allein- oder mitreisende Minderjährige ihr Alter (und damit ihre besondere Schutzbedürftigkeit) nicht nachweisen können und ihnen Schutzbestimmungen des Asyl- und Ausländerrechts nicht zugutekommen. Dies führt dazu, dass im Asylverfahren Alterseinschätzungen vorgenommen werden müssen, um die Minderjährigkeit zu überprüfen.

Hier liegt ein Einsatzfeld von KI-gestützter Altersverifikation. Auf Grundlage von Datensätzen Dritter (in der Regel kommen Gesichtsbilder zum Einsatz), die als Trainingsdaten Verwendung finden, werden KI-Modelle darauf trainiert, Muster in den Datensätzen zu erkennen (in der Regel werden Verhältnisse der Gesichtspartien zueinander als Muster entwickelt), welche eine belastbare Einschätzung des Alters bzw. der Altersgruppe (sicher unter 18 Jahren/wahrscheinlich unter 18 Jahren/wahrscheinlich über 18 Jahren/sicher über 18 Jahren) abgeben können.[81] Bei der Einreise werden die biometrischen Daten[82] der einreisenden Person der entsprechenden KI-Anwendung zugeführt,[83] welche das Ergebnis der Bundespolizei zuleitet.

81 Marktanbieter geben an, ihre KI könne das Alter bis auf etwa 2 Jahre genau einschätzen, vgl. Automatisierte Altersverifikation: KI checkt das Alter im Edeka-Markt | Computerwoche, abgerufen am 6.2.2025. Vgl. auch https://www.mind-verse.de/news/zukunft-des-einkaufens-durch-ki-gestuetzte-altersverifikation-in-supermaerkten, abgerufen am 6.2.2025. Andere Anbieter geben die Ungenauigkeit mit „weniger als 1 Jahr“ an, vgl. https://www.innovative-technology.com/age_identity_verification/. Im Gegensatz zu den Herstellerangaben urteilen Hruschka/Nestler, dass „alle bekannten Verfahren zur Alterseinschätzung keine verlässlichen Ergebnisse liefern können“ Vgl. https://www.kindernothilfe.de/-/media/knh/infothek-neu/fachpublikationen/gutachten-geas.pdf, S. 35-40.

82 Dies ist ein Unterschied zu sogenannten Age Categorizern, die ebenfalls auf eine proprietäre, KI-gestützte Software aufbauen, sich allerdings an Social-Media-Profilangaben und Nutzungsverhalten orientieren, also keine Art.-9-Daten nutzen, vgl. https://www.heise.de/news/Altersverifikation-So-will-Meta-luegende-Teenies-erkennen-10004849.html, abgerufen am 6.2.2025.

83 Frühere Altersverifikationssysteme waren nur bei Vorliegen gültiger Ausweise nutzbar, vgl. etwa https://www.pxl-vision.com/de/produkt/pxl-age?kw=altersverifikation, abgerufen am 6.2.2025.

KI-gestützte Altersverifikation bei der Einreise zielt nicht auf die Identifikation oder Verifikation der Identität der einreisewilligen Person, da entsprechende Identitätsdaten zuvor weder erhoben noch gespeichert wurden und in der Regel auch ansonsten nicht (beim Herkunfts- oder einem Durchreiseland der einreisewilligen Person) abrufbar sind.

aaa) Beispiel 1: Zulässig nach DS-GVO?
KI-gestützte Altersverifikation bei der Einreise erfolgt unter Verwendung biometrischer Daten. Allgemein ist die Altersverifikation mit biometrischen Daten etwa zum Ausschluss von Kindern von gefährdenden Anwendungen (Gewaltdarstellungen im Internet / Pornographie / politisch-extremistische Darstellungen) gemäß Art. 9 Abs. 2 lit. c i. V. m. Art. 6 I lit. d DS-GVO (die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben) grundsätzlich möglich. Wegen des Einsatzes biometrischer Daten scheitert die Rechtsgrundlage Art. 6 Abs. 1 lit. f DS-GVO allerdings regelmäßig an den überwiegenden Interessen der (minderjährigen) betroffenen Person.

Soweit es sich um eine für den Verantwortlichen verpflichtende Altersverifikation für alle Nutzer handelt, ist auch eine Verarbeitung nach Art. 9 Abs. 2 lit. g i. V. m. Art. 6 Abs. 1 lit. c bzw. e DS-GVO denkbar. Einschlägig ist bei diesen Fällen stets auch Art. 11 DS-GVO, der die Pflichten des Verantwortlichen beschränkt, soweit (wie hier) eine Identifikation der betroffenen Person nicht angestrebt ist. Zu berücksichtigen ist hier ferner, dass fehlerhafte KI-gestützte Altersverifikationen die Zugangsrechte der betroffenen Personen unberechtigt einschränken können.[84]

Im vorliegenden Fall (Grenzkontrollen mit KI-gestützter Altersverifikation) kommt als datenschutzrechtliche Rechtsgrundlage Art. 9 Abs. 2 lit. g i. V. m. Art. 6 Abs. 1 lit. c bzw. e DS-GVO in Betracht, dazu wäre jeweils eine gesetzliche Grundlage zu schaffen, welche „in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht“ (vgl. Art. 9 Abs. 2 lit. g DS-GVO). Dies bedeutet, dass die gesetzliche Grundlage etwa in Anwendung des Verhältnismäßigkeitsgrundsatzes die Identifikation der betroffenen Einreisenden zverbieten müsste und dass eine Prüfpflicht bzgl. der Fehlerquote der KI-Anwendung anzuordnen wäre, da bei Minderjährigen bzw. ethnischen Minderheiten eine erhöhte Fehleranfälligkeit der KI-Anwendung zu vermuten wäre.[85] Zudem steht es den Mitgliedstaaten gemäß Art. 9 Abs. 4 DS-GVO offen, zusätzliche Bedingungen, einschließlich Beschränkungen, einzuführen oder aufrechtzuerhalten, da vorliegend die Verarbeitung von biometrischen Daten betroffen ist.

bbb) Zulässig nach KI-VO?
Auch die KI-VO spricht kein grundsätzliches Verbot KI-gestützter Altersverifikation bei der staatlichen Einreisekontrolle aus.

Insoweit ergeben sich bereits Zweifel an der Anwendbarkeit der KI-VO, die gemäß Art. 2 Abs. 3 UA 1 KI-VO nur in den unter das Unionsrecht fallenden Bereichen gilt und keinesfalls die Zuständigkeiten der Mitgliedstaaten in Bezug auf die nationale Sicherheit berührt. Nach Art. 2 Abs. 3 UA 2 und 3 KI-VO gilt diese Verordnung auch „nicht für KI-Systeme, wenn und soweit sie ausschließlich für […] Zwecke der nationalen Sicherheit

84 Zum Recht auf Teilhabe und Zugang zu Informationen im Internet – auch durch Jugendliche – mahnt der DKSB: „Kinder und Jugendliche haben neben dem Recht auf Schutz auch ein Recht auf Teilhabe und Befähigung.“ Es gehe darum, dass sie „selbstbestimmt und selbstsicher im Umgang mit diesen Geräten und Medien werden“ (https://netzpolitik.org/2024/ausweispflicht-wie-alterskontrollen-das-internet-umkrempeln-sollen/), abgerufen am 6.2.2025.

85 Die KI müsste insbesondere auf verschiedene Ethnien, Hautfarben, Geschlechter und Altersgruppen trainiert werden, vgl. https://www.computerwoche.de/article/2833949/ki-checkt-das-alter-im-edeka-markt.html.

in Verkehr gebracht, in Betrieb genommen oder, mit oder ohne Änderungen, verwendet werden, unabhängig von der Art der Einrichtung, die diese Tätigkeiten ausübt. Diese Verordnung gilt nicht für KI-Systeme, die nicht in der Union in Verkehr gebracht oder in Betrieb genommen werden, wenn die Ausgaben in der Union ausschließlich für […] Zwecke der nationalen Sicherheit verwendet werden, unabhängig von der Art der Einrichtung, die diese Tätigkeiten ausübt."

Hält man die KI-VO demgegenüber für anwendbar – etwa weil geordnete Migration keine Gefahr für die nationale Sicherheit bedeutet – so fällt die KI-gestützte Altersverifikation bei der staatlichen Einreisekontrolle nicht unter die KI-Verbote des Art. 5 KI-VO. Dies ergibt sich für Art. 5 Abs. 1 lit. b und c KI-VO bereits daraus, dass eine bessere Schutzgewährung angestrebt wird und keinesfalls eine Ausnutzung oder Schädigung der Minderjährigen. Auch ist eine Gesichtserkennung nach Art. 5 Abs. 1 lit. e KI-VO nicht bezweckt. Ob damit eine biometrische Kategorisierung i. S. v. Art. 5 Abs. 1 lit g KI-VO betrieben wird, ist zwar offen, jedenfalls erfolgt diese nicht zu diskriminatorischen Zwecken. Eine biometrische Echtzeit-Fernidentifizierung gemäß Art. 5 Abs. 1 lit h KI-VO erfolgt jedenfalls nicht.

Allerdings handelt es sich bei einer KI-gestützten Altersverifikation anlässlich der staatlichen Einreisekontrolle wohl um ein sog. Hochrisiko-KI-System nach Art. 6 Abs. 2 KI-VO i. V. m. Anhang III Nr. 1 b (Biometrie: KI-Systeme, die bestimmungsgemäß für die biometrische Kategorisierung nach sensiblen oder geschützten Attributen oder Merkmalen auf der Grundlage von Rückschlüssen auf diese Attribute oder Merkmale verwendet werden sollen – als sensibles Merkmal kommt hier sowohl die bestehende als auch die nicht bestehende Minderjährigkeit in Betracht) bzw. i. V. m. Anhang III Nr. 7 c und d (Migration, Asyl und Grenzkontrolle: Unterstützung der Prüfung von Asyl- und Visumanträgen sowie Aufenthaltstiteln bzw. Verwendung zur Anerkennung natürlicher Personen).

Eine Unterausnahme gemäß Abs. 3 des Art. 6 KI-VO ist bei richtigem Verständnis nicht gegeben. Danach gilt „abweichend von Absatz 2 […] ein in Anhang III genanntes KI-System nicht als hochriskant, wenn es kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst". Davon wird bei einer KI-gestützten Altersverifikation anlässlich der staatlichen Einreisekontrolle nicht auszugehen sein: Zum einen birgt der KI-Einsatz das Risiko, den Minderjährigenschutz zu verlieren, zum anderen wird in der Praxis das Ergebnis der KI-Anwendung die Entscheidung über die Kategorisierung einreisewilliger Personen maßgeblich beeinflussen.

Dass es sich bei der Altersverifikation um eine „eng gefasste Verfahrensaufgabe" i. S. v. Art. 6 Abs. 3 UA 2 a KI-VO handeln könnte, schließt UA 3 i. V. m. Art. 4 Nr. 4 DS-GVO (vgl. Art. 3 Nr. 52 KI-VO) aus, da die KI-gestützte Altersverifikation eine „automatisierte Verarbeitung personenbezogener Daten [darstellt], die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen [hier: das Alter einer Person], zu bewerten".

Damit treffen den Betreiber des KI-Systems die Pflichten aus Abschnitt 2 der KI-VO (Anforderungen an Hochrisiko-KI-Systeme), verboten wird eine KI-gestützten Altersverifikation anlässlich der staatlichen Einreisekontrolle aber gerade nicht. Daher stellt die Rechtsordnung an den Betrieb einer KI-gestützten Altersverifikation anlässlich der staatlichen Einreisekontrolle also erhebliche Anforderungen – verhindert deren Einsatz auf gesetzlicher Grundlage aber nicht.

bb) Beispiel 2: Biometrische Gesundheitsdaten von Kindern in KI-Anwendung

Die Nutzung biometrischer Daten von Minderjährigen als KI-Trainingsdaten und in KI-gesteuerten Entscheidungsprozessen ist im Gesundheitssektor besonders naheliegend. Hier kann KI ihre Stärken bei der Mustererkennung, aber auch bei der Analyse sehr

großer Datenmengen und bei der visuellen Darstellung komplexer Strukturen ausspielen. Gerade bei der Erkennung und Behandlung von Erkrankungen Minderjähriger besteht ein erhebliches Forschungs- und Therapiedefizit, weil die westliche Medizin traditionell auf die Behandlung erwachsener Männer ausgerichtet ist.

Die Einsatzgebiete sind dabei vielfältig, etwa das Erkennen von individuellen Krankheitsgefährdungen oder Anlagen zu physischen und psychischen Erkrankungen oder die KI-basierte Therapie von Kindern mit seltenen Erkrankungen unter Einsatz biometrischer Parameter zur Krankheitserkennung und -bestimmung.

aaa) Zulässig nach DS-GVO?
Soweit es um die Nutzung biometrischer Daten von Minderjährigen als KI-Trainingsdaten geht, kann nach oben (4 a) verwiesen werden. Datenschutzrechtlich ist die Forschung nach Art. 89 DS-GVO (auch bei Art.-9-Daten, vgl. Art. 9 Abs. 2 j DS-GVO) massiv privilegiert, hier genügen regelmäßig schon einfache „geeignete Garantien" wie die Pseudonymisierung (vgl. Art. 89 Abs. 1 S. 2 DS-GVO), um das Training zu rechtfertigen. Bereits die Beachtung einfacher bzw. niedriger Datenschutz-Standards (Verschlüsselung, differenziertes Zugriffs- und Berechtigungssystem) erfüllen hier die gesetzlichen Vorgaben. Dieses Ergebnis ist auch stimmig, soweit bei KI-basierter Forschung zur Kindergesundheit die Schaden-Nutzen-Abwägung positiv ausfällt.
Auch die individuelle Behandlung inkl. Diagnostik und Therapie, welche die Erhebung und Nutzung biometrischer Daten minderjähriger Patient*innen in KI-Anwendungen umfasst, ist datenschutzrechtlich zu rechtfertigen. Denkbar ist dies über Art. 9 Abs. 2 lit. c, g, h und i, jeweils i. V. m. Art. 6 Abs. 1 lit. d (und ausnahmsweise auch f) DS-GVO; hier kommt bei der medizinischen Behandlung auch eine Einwilligung nach Art. 9 Abs. 2 lit. a i. V. m. Art. 6 Abs. 1 lit. a DS-GVO in Betracht.

bbb) Zulässig nach KI-VO?
Der KI-VO ist kein grundsätzliches Verbot der Nutzung biometrischer Daten von Minderjährigen als KI-Trainingsdaten und in KI-gesteuerten Entscheidungsprozessen im Gesundheitssektor zu entnehmen, die KI-Verbote des Art. 5 KI-VO sind nicht einschlägig.

Ggf. sind eingesetzte KI-Systeme als Hochrisiko-KI-Systeme nach Art. 6 Abs. 2 KI-VO einzustufen. Anzuwenden ist hier Anhang III Nr. 1 b (Biometrie: KI-Systeme, die bestimmungsgemäß für die biometrische Kategorisierung nach sensiblen oder geschützten Attributen oder Merkmalen auf der Grundlage von Rückschlüssen auf diese Attribute oder Merkmale verwendet werden sollen – als sensibles Merkmal kommt hier das Vorliegen oder Nicht-Vorliegen von Krankheitsmerkmalen in Betracht; zu deren Sensibilität vgl. Art. 9 Abs. 1 DS-GVO).

Eine Unterausnahme gemäß Abs. 3 des Art. 6 KI-VO kann allerdings je nach Einsatzart der KI-Anwendung vorliegen: Entweder die KI-Anwendung ist nicht als hochriskant zu bewerten, weil es in Bezug auf die Gesundheit nicht Risiken, sondern (zusätzliche) Chancen bietet, oder es kann nach UA 2 b, c und d auch eine lediglich hinzutretende KI-Ausgabe vorliegen, welche die zuvor abgeschlossene medizinische Bewertung weder ersetzt noch dominiert.

Wie aufgeschlossen gerade das europäische und nationale Recht im Bereich der (KI-basierten) Gesundheitsdatenforschung sind, zeigen Gesetzgebungsinitiativen wie der„Europäische Raum für Gesundheitsdaten (EHDS)[86] oder das deutsche „Gesetz zur verbesserten Nutzung von Gesundheitsdaten" vom 25.03.2024.[87]

86 https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_de, abgerufen am 6.2.2025.

87 https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/detail/gesundheitsdatennutzungsgesetz.html, abgerufen am 6.2.2025.

Daher stellt die Rechtsordnung an die Nutzung biometrischer Daten von Minderjährigen als KI-Trainingsdaten und in KI-gesteuerten Entscheidungsprozessen im Gesundheitssektor erhebliche Anforderungen – verhindert deren Einsatz aber nicht, sondern fördert ihn sogar.

bb) Beispiel 3: Biometrische Kinderdaten beim Einsatz von KI im Bildungssektor
Der Nutzung biometrischer Daten von Minderjährigen als KI-Trainingsdaten und in KI-gesteuerten Entscheidungsprozessen wird auch im Bildungssektor erhebliches Gewicht zukommen: Zum einen bei der Entwicklung individualisierbarer, KI-basierter Lernmethoden, welche individuell angepasste Lernverfahren ermöglichen. Dafür sind biometrische Daten von Kindern (als wichtigste Gruppe der Bildungssuchenden) für Trainingszwecke von Nutzen, die

a) Lernverhalten individuell festhalten, also eine persönliche Zurechnung von Trainingsdaten zu Testpersonen erlauben (etwa durch Einsatz von Gesichtserkennung), und

b) eine Verhaltensanalyse der lernenden Testpersonen (z. B. Aufmerksamkeitsspanne, Kommunikationsbereitschaft und -fähigkeit) und ihrer Emotionen (Emotionserkennung) auf Basis biometrischer Daten erlauben.

Zum anderen sind biometrische Daten von Minderjährigen in KI-gesteuerten Anwendungen nutzbar, welche individuelles Lernverhalten von Minderjährigen in der Schule sowie bestehende Leistungsschwächen erkennen und dies zur nachfolgenden gezielten Unterstützung heranziehen. Auch hierzu wird während des Unterrichts

a) Lernverhalten individuell festgehalten, also eine persönliche Zurechnung von Leistungsdaten zu bestimmten Bildungssuchenden erlaubt (etwa durch Einsatz von Gesichtserkennung), und

b) eine Verhaltensanalyse der lernenden Personen (z. B. Aufmerksamkeitsspanne, Kommunikationsbereitschaft und -fähigkeit) und ihrer Emotionen (Emotionserkennung) auf Basis biometrischer Daten vorgenommen und mit dem individuellen Lernerfolg abgeglichen.

Auf dieser Basis können individuell Lernmethoden angepasst und für die Lernenden optimiert werden.

aaa) Zulässig nach DS-GVO?
Hinsichtlich der Nutzung biometrischer Daten von Minderjährigen als **KI-Trainingsdaten im Bildungssektor** kann nach oben (4 a) verwiesen werden. Datenschutzrechtlich ist die Forschung nach Art. 89 DS-GVO (auch bei Art.-9-Daten, vgl. Art. 9 Abs. 2 j DS-GVO) massiv privilegiert, „geeignete Garantien" wie die Pseudonymisierung (vgl. Art. 89 Abs. 1 S. 2 DS-GVO) und die Beachtung einfacher Datenschutz-Standards (Verschlüsselung, differenziertes Zugriffs- und Berechtigungssystem) erfüllen bereits die gesetzlichen Vorgaben. Die Verarbeitung biometrischer Kinderdaten zum Zwecke der Gesichtserkennung ist damit ebenso zu rechtfertigen wie für Zwecke der Verhaltensanalyse und Emotionserkennung.

Wesentlich schwieriger ist die Nutzung biometrischer Daten von Minderjährigen **in KI-gesteuerten Anwendungen** im Bildungssektor zu rechtfertigen. Möglich erscheint zwar eine Einwilligung nach Art. 9 Abs. 2 lit. a i. V. m. Art. 6 Abs. 1 lit. a DS-GVO, sie erscheint jedoch als allgemeine und dauerhafte Basis von langfristigen Bildungsmaßnahmen schon wegen ihrer jederzeitigen Widerruflichkeit (Art. 7 Abs. 3 DS-GVO) wenig geeignet; zudem begegnet die Einwilligung auch deswegen erheblichen Vorbehalten, weil Bildung häufig durch staatliche oder kommunale Stellen angeboten wird und damit an der Freiwilligkeit der Einwilligung – auch wegen des individuellen Angewiesenseins auf Bildungserfolge – erhebliche Zweifel bestehen (vgl. Art. 4 Nr. 11 i. V. m. ErwGr. 43 DS-GVO).

Andere Rechtsgrundlagen für die Verarbeitung biometrischer Kinderdaten sind nicht ersichtlich, bleibt also wiederum nur die Schaffung einer entsprechenden gesetzlichen Grundlage und die Verarbeitung nach Art. 9 Abs. 2 lit. g DS-GVO. Am erheblichen öffentlichen Interesse einer breiten und fundierten Bildung aller Bürger*innen besteht kein Zweifel. Zu den „angemessenen und spezifischen Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" dürften insbesondere zählen:

- eine umfassende Zweckbindung der erhobenen Daten unter Ausschluss jeder Zweckänderung gemäß Art. 6 Abs. 4 DS-GVO;
- eine zeitliche Beschränkung der Erfassungsmaßnahmen bis zur Klärung der individuell angemessenen Lernmethode; spätere Überprüfungen dürften allenfalls stichprobenartig zulässig sein;
- ein umfassendes Konzept zur Datensicherheit (Zugriffsbeschränkungen, Verschlüsselung etc.);
- kurze Löschfristen für ausgewertete Daten und eine frühestmögliche Ersetzung der Rohdaten durch aggregierte Daten

Da es sich bei der Entscheidung über passende Lernmethoden und erzielbare Lernerfolge um solche erheblicher persönlicher Relevanz handelt, ist das Verbot automatisierter Entscheidungen nach Art. 22 DS-GVO (dazu ausführlich oben 4 b) einschlägig. Danach dürfen Ausgaben der KI nicht ohne menschliche Überprüfung (Human-in-the-Loop-Ansatz) umgesetzt werden. Zwar sind hier gesetzliche Ausnahmevorschriften denkbar (vgl. Art. 22 Abs. 2 lit. b DS-GVO), allerdings müssten hierbei „angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person" ins Gesetz aufgenommen werden. Ob sich die Schutzwirkung des Art. 22 DS-GVO durch eine ausdrückliche Einwilligung der Sorgeberechtigten (vgl. Art. 22 Abs. 2 lit. c DS-GVO) beseitigen lässt, dürfte angesichts staatlicher Schutzpflichten im Bildungssektor zumindest fraglich sein.

bbb) Zulässig nach KI-VO?

Die KI-gestützte Gesichtserkennung, eine Verhaltensanalyse der lernenden Personen (z. B. Aufmerksamkeitsspanne, Kommunikationsbereitschaft und -fähigkeit) und ihrer Emotionen (Emotionserkennung) auf Basis biometrischer Daten begegnet aus Sicht der KI-VO erheblichen Einwänden. Die KI-Verbote des Art. 5 KI-VO bedürfen hier der näheren Betrachtung:

Lit. a (Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person) kann je nach Lernmethode einschlägig sein, allerdings fehlt es an der vorausgesetzten Schädigungsintention.

Für lit. b und c (Ausnutzung der Vulnerabilität oder Schutzbedürftigkeit einer natürlichen Person / Bewertung oder Einstufung von natürlichen Personen oder Gruppen von Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale) fehlt es ebenfalls an einer möglichen Schädigung bzw. Schlechterstellung oder Benachteiligung.

Lit. e (Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen) fehlt es daran, dass „Überwachungsaufnahmen" eingesetzt werden. In der Bildungseinrichtung erfolgt die Individualisierung der Lernenden nicht durch unspezifische Überwachungserfassung, sondern im Rahmen der Zuordnung des Verhaltens vorab bekannter Personen.

Einschlägig erscheint jedoch das Verbot des Art. 5 Abs. 1 lit. f KI-VO, das die Verwendung von KI-Systemen „zur Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz und in Bildungseinrichtungen, es sei denn, die Verwendung des KI-Systems soll aus medizinischen Gründen oder Sicherheitsgründen eingeführt oder auf den Markt gebracht

werden“ untersagt. Das betrifft die o. g. Maßnahmen zur Emotionserkennung. Diese dürften damit unzulässig sein; eine ausnahmsweise Zulassung solcher Anwendungen durch (mitgliedstaatliches) Gesetz ist nicht vorgesehen.

Die weiteren KI-gestützten Nutzungen biometrischer Daten von Minderjährigen im Bildungssektor sind demgegenüber zulässig, allerdings handelt es sich bei ihnen um sog. Hochrisiko-KI-Systeme nach Art. 6 Abs. 2 KI-VO i. V. m. Anhang III Nr. 1 b (Biometrie: KI-Systeme, die bestimmungsgemäß für die biometrische Kategorisierung nach sensiblen oder geschützten Attributen oder Merkmalen auf der Grundlage von Rückschlüssen auf diese Attribute oder Merkmale verwendet werden sollen – als sensibles Merkmal kommt hier insbesondere die Lernfähigkeit und Begabung Minderjähriger in Betracht) bzw. i. V. m. Anhang III Nr. 3 (Allgemeine und berufliche Bildung: insbesondere b) KI-Systeme, die bestimmungsgemäß für die Bewertung von Lernergebnissen verwendet werden sollen, einschließlich des Falles, dass diese Ergebnisse dazu dienen, den Lernprozess Personen in Einrichtungen oder Programmen aller Ebenen der allgemeinen und beruflichen Bildung zu steuern; c) KI-Systeme, die bestimmungsgemäß zum Zweck der Bewertung des angemessenen Bildungsniveaus, das eine Person im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung erhalten wird oder zu denen sie Zugang erhalten wird, verwendet werden sollen).

Eine Unterausnahme gemäß Abs. 3 des Art. 6 KI-VO ist bei richtigem Verständnis nicht gegeben. Danach gilt „abweichend von Absatz 2 […] ein in Anhang III genanntes KI-System nicht als hochriskant, wenn es kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst“. Davon wird bei einer KI-gestützten Lernüberwachung nicht auszugehen sein: Zum einen birgt der KI-Einsatz das Risiko, den Anspruch auf Bildung zu verlieren, zum anderen wird in der Praxis das Ergebnis der KI-Anwendung die Entscheidung über die Kategorisierung bildungssuchender Personen, etwa hinsichtlich ihres Lernerfolgs, maßgeblich beeinflussen. Damit treffen den Betreiber des KI-Systems die Pflichten aus Abschnitt 2 der KI-VO (Anforderungen an Hochrisiko-KI-Systeme). Daher stellt die Rechtsordnung an die Nutzungbiometrischer Daten von Minderjährigen als KI-Trainingsdaten und in KI-gesteuerten Entscheidungsprozessen im Bildungssektor erhebliche Anforderungen – verhindert deren Einsatz auf gesetzlicher Grundlage aber lediglich, soweit eine KI-gestützte Emotionserkennung stattfindet.

Fazit

Daten von Kindern sind, obwohl ihr Schutzbedürfnis allgemein betont wird, weder nach der DS-GVO noch nach dem DSA oder der KI-VO systematisch und ausreichend geschützt. Das gilt auch für biometrische Daten von Kindern, deren gesetzliches Schutzniveau trotz der Besonderheiten gerade biometrischer Kinderdaten nicht weiter angepasst wurde.

Aktuell setzen zwar viele KI-Anwendungen zu ihrer praktischen Nutzbarkeit ein Tätigwerden des europäischen bzw. nationalen Gesetzgebers voraus – ob dabei allerdings Kinderdaten mit Blick auf ihre besondere Schutzbedürftigkeit angemessen geschützt werden, bleibt offen.

Ohne weiteres Eingreifen der Gesetzgebung, etwa durch eine „EU-Verordnung zum Schutz und zur Befähigung von Kindern in der digitalen Welt“ oder durch nationale Gesetze als Verarbeitungsgrundlage für Kinderdaten für KI-Modelle und -Anwendungen wird sich ein hinreichendes Schutzniveau nicht erreichen lassen.

Zusammenfassung der wesentlichen Ergebnisse

1. Biometrische Daten sind in Anlehnung an die DS-GVO zu verstehen als „mit technischen Verfahren gewonnene personenbezogene Daten zu den Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen (Verifikation)".

2. Weder die KI-VO noch der DSA weisen eigenständige Definitionen biometrischer Daten auf. Andere begriffliche oder definitorische Ansätze (etwa „anthropometrische Daten") bleiben möglich, sind aber zur Absicherung terminologischer Klarheit abzugrenzen

3. Über eine eigenständige Definition biometrischer Daten von Kindern verfügen weder die DS-GVO noch die anderen einschlägigen europäischen Rechtsvorschriften.

4. Wegen der besonderen Schutzbedürftigkeit von Kindern hinsichtlich der Verarbeitung ihrer biometrischen Daten, aber auch wegen der teilweisen Wandelbarkeit biometrischer Daten von Kindern ergibt sich ein insgesamt uneinheitliches Bild, das allerdings wegen der aufgezeigten besonderen Gefährdungspotenziale eine gesetzgeberische Befassung verdient hätte.

5. Die Datenschutz-Grundverordnung schützt personenbezogene Daten, auch diejenigen von Kindern. Dass Kindern darüber hinaus einen besonderen Schutz verdienen, ergibt sich bereits aus der EU-Grundrechte-Charta.

6. Eine Analyse der DS-GVO erhellt, dass diese die besondere Schutzbedürftigkeit von Kindern in einer Reihe von Vorschriften durchaus anerkennt und erweiterte matriell rechtliche Anforderungen an die Rechtmäßigkeit der Verarbeitung personenbezogener Daten von Kindern stellt.

7. Mit diesem Verbot des Profilings von Kindern trifft die DS-GVO eine der wenigen klaren und eindeutigen Schutzmaßnahmen zugunsten von Minderjährigen.

8. Die DS-GVO verfolgt keinen absoluten Schutz von Kindern. Obwohl zumindest die wirtschaftliche Verwertung der personenenbezogenen Daten von Kindern mit guten Gründen verboten werden könnte, hat sich der EU-Gesetzgeber gegen ein solches Schutzniveau entschieden. Er hat stattdessen einen bloß relativen Schutz personenbezogener Kinderdaten statuiert – und selbst diesen differenziert er nach Lebensaltersstufen. Der Schutz von Kindern ist in der DS-GVO also weder prioritär noch konsequent durchgehalten.

9. Kinderschutz ist demnach ein durchaus relevantes, aber kein überragend wichtiges Gut der DS-GVO.

10. Der Digital Services Act (DSA) weist durchaus Bestimmungen zu Minderjährigen und ihrem Schutz im Kotext digitaler Plattformen, Dienste und Produkte auf – der Schutz ist aber nur sporadisch, bleibt zum Teil auf besonders große Anbieter beschränkt und wird lediglich bei der auf Kinder zugeschnittenen Online-Werbung konkreter.

11. Insgesamt arbeitet die KI-VO durchaus mit den Tatbestandsmerkmalen „personenbezogene Daten" und „biometrische Daten", knüpft dabei allerdings in untergeordneter Weise an die Vorgaben der DS-GVO an.

12. Laut KI-VO liegt durchaus ein erhöhtes Schutzbedürfnis für Kinder vor, dieses wird von der Verordnung allerdings nicht eigenständig ausgearbeitet. Vielmehr belässt es die KI-VO bei Verweisen auf andere einschlägige Schutzvorschriften. Zudem werden die in der KI-VO angelegten Ausnahmevorschriften etwa beim KI-Einsatz zur Sicherung der nationalen Sicherheit oder bei Grenzkontrollen unterschiedslos auch auf Kinder estreckt – Minderjährige genießen hier demnach keinen besonderen Schutzstatus.

13. Ein angemessener Schutz der Rechte von Kindern und Jugendlichen vor den Gefahren des digitalen Zeitalters kann allenfalls aus der Zusammenschau der Schutzwirkungen mehrerer Gesetze (vgl. DS-GVO, KI-VO bzw. DSA) erzielt werden – bedürfte aber noch zusätzlicher gesetzgeberischer Anstrengungen, ggf. auch in einem eigens auf die Rechte und Interessen von Kindern und Jugendlichen zugeschnittenen Rechtsakt.

14. Diese „Verordnung zum Schutz und zur Befähigung von Kindern in der digitalen Welt" soll einerseits die Vulnerabilität von Minderjährigen erfassen und überwinden, andererseits aber auch durchgehend berücksichtigen, dass Kindern eigene Rechte und je nach Entwicklungsstand selbst ausgeübte Freiheiten auch im Digitalen zustehen.

15. Daher sollte der Rechtsakt insbesondere den Zugang von Kindern zum Möglichkeitsraum Internet, Schutzkonzepte zu altersbedingt besonders schädlichen Inhalten des Internets, das Schaffen eines Rechts auf Teilhabe und Befähigung zur Teilhabe im Digitalen, die Entwicklung des Schutzverhältnisses von Kindern und Sorgeberechtigten sowie eine Garantie eines Rechts auf unbelasteten Eintritt in die Volljährigkeit umfassen. Ihm müsste zudem Vorrangwirkung gegenüber den übrigen EU-Rechtsakten zukommen.

16. Künstliche Intelligenz begegnet uns heute in Form von Anwendungen, die auf sog. KI-Modellen basieren. Die Nutzung biometrischer Kinderdaten zu Zwecken des Trainings eines KI-Modells bedarf einer gesetzlichen Basis aus Art. 6 Abs. 1 DS-GVO, unterliegt jedoch einem grundsätzlichen Verarbeitungsverbot aus Art. 9 Abs. 1 DS-GVO.

17. Unter den Ausnahmen vom Verarbeitungsverbot in Art. 9 Abs. 2 DS-GVO finden sich nur wenige, die für den Einsatz von Kinderdaten zum Training von KI-Modellen nutzbar gemacht werden können: Eine Einwilligung (Art. 9 Abs. 2 lit. a DS-GVO) ist zumindest äußerst unpraktikabel, denkbar wäre eine Ausnahme „zum Schutz lebenswichtiger Interessen der betroffenen Person" (Art. 9 Abs. 2 lit. c DS-GVO). Möglich wäre auch ein Einsatz biometrischer Kinderdaten zum Training eines KI-Modells für Zwecke der öffentlichen Gesundheit (Art. 9 Abs. 2 lit. i DS-GVO) bzw. Gesundheitsvorsorge (Art. 9 Abs. 2 lit. h DS-GVO). Um KI-Training auf das sog. Forschungsprivileg der DS-GVO zu stützen (vgl. Art. 9 Abs. 2 lit. j DS-GVO), bedürfte es einer ausdrücklichen gesetzliche Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats der EU, die bislang zugunsten des KI-Trainings mit Kinderdatennicht geschaffen wurde.

18. Solche spezialgesetzlichen Grundlagen für KI-Trainings werden von der DS-GVO akzeptiert (vgl. Art. 9 Abs. 2 lit. g DS-GVO, Verarbeitung aufgrund erheblichen öffentlichen Interesses), Art. 9 Abs. 4 DS-GVO eröffnet den Mitgliedstaaten umgekehrt auch die Möglichkeit, solche Verarbeitungen biometrischer Daten weiter einzuschränken.

19. Wegen der strikten Vorgaben der DS-GVO zum Training von KI-Modellen mit biometrischen Kinderdaten lässt sich prognostizieren, dass dieses – was sowohl wirtschaftlich als auch mit Blick auf die Gewährleistung des Kinderschutzes problematisch ist - wohl weit überwiegend außerhalb der EU stattfinden wird.

20. Auch bei der Anwendung von KI-Systemen kann es zur Nutzung biometrischer Kinderdaten kommen. Ohne ausdrückliche gesetzliche Grundlage kommen letztlich wieder nur Einwilligungen nach Art. 6 Abs. 1 lit. a i. V. m. Art. 9 Abs. 2 lit. a DS-GVO in Betracht. Allerdings sind bei Anwendungsvorgängen einwilligungsbasierte Datenverarbeitun wesentlich plausibler darzustellen. Nach Auffassung des EDSA kann allerdings ein rechtswidriges Training von KI-Modellen auf die Rechtmäßigkeit der Nutzung der KI-Anwendung „durchschlagen“ (sog. Infektionsthese).

21. Beim Einsatz von KI ist zusätzlich Art. 22 DS-GVO zu beachten, der die Nutzbarkeit von KI-Anwendungen in der EU wesentlich beeinträchtigt: Er diskriminiert die Automatisierung von Entscheidungsprozessen. Danach hat jeder „das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung […] beruhenden Entscheidung unterworfen zu werden“.

22. Die Rechtsprechung des EuGH zu Art. 22 DS-GVO beschränkt die Einsatzmöglichkeiten von KI wesentlich, da angestrebte Effizienzgewinne erheblich reduziert werden

23. Drei Beispiele erläutern die Einsatzfelder biometrischer Kinderdaten für KI-Modelle und -Anwendungen: Grenzkontrollen mit KI-gestützter Altersverifikation (Beispiel 1), biometrische Gesundheitsdaten von Kindern in KI-Anwendungen (Beispiel 2) und biometrische Kinderdaten beim Einsatz von KI im Bildungssektor (Beispiel 3)

24. Die DS-GVO schließt den Einsatz biometrischer Kinderdaten für KI-Modelle und -Anwendungen nicht grundsätzlich aus, die KI-VO tut dies nur in wenigen Einsatzszenarien – etwa bei der automatisierten Emotionserkennung und Verhaltensbeeinflussung mittels KI. Der DSA schließlich reguliert den Einsatz von biometrischen Kinderdaten in KI nur sporadisch.

25. Ohne weiteres Eingreifen der Gesetzgebung, etwa durch eine „EU-Verordnung zum Schutz und zur Befähigung von Kindern in der digitalen Welt“ oder durch nationale Gesetze als Verarbeitungsgrundlage für Kinderdaten für KI-Modelle und -Anwendungen wird ein angemessenes Schutzniveau nicht erreichen lassen.

Literaturverzeichnis

Kommentare

Gola, Peter / Heckmann, Dirk (Hrsg.): Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. 3. Auflage München 2022. zit. als: Gola/Heckmann/Bearbeiter, DS-GVO.

Kühling, Jürgen / Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. 4. Auflage München 2024. zit. als: Kühling/Buchner/Weichert, 4. Aufl. 2024, DS-GVO.

Paal, Boris P. / Pauly, Daniel A. (Hrsg.): Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG. 3. Auflage München 2021. zit. als: Paal/Pauly/Bearbeiter, DS-GVO.

Simitis, Spirios / Hornung, Gerrit / Spiecker gen. Döhmann, Indra (Hrsg.): Datenschutzrecht. 1. Auflage Baden-Baden 2019. zit. als: Simitis/Hornung/Spiecker gen. Döhmann/Bearbeiter, Datenschutzrecht.

Taeger, Jürgen / Gabel, Detlev (Hrsg.): DSGVO – BDSG – TDDDG. 5. Auflage Frankfurt 2025. zit. als: Taeger/Gabel/Mester, DS-GVO.

Voßkuhle, Andreas / Eifert, Martin / Möllers, Christoph (Hrsg.): Grundlagen des Verwaltungsrechts. 3. Auflage München 2022. zit. als: Voßkuhle/Eifert/Möllers VerwR/Bearbeiter.

Wolff, Heinrich Amadeus / Brink, Stefan (Hrsg.): BeckOK DatenschutzR. 46. Ed. 1.8.2023. zit. als: Wolff/Brink BeckOK DatenschutzR/Bearbeiter.

Monographien und Aufsätze

Seite „Biometrie“. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 18. Dezember 2024, 14:41 UTC. URL: https://de.wikipedia.org/wiki/Biometrie. zuletzt abgerufen am 13.02.2025.

Seite „Anthropometrie“. In: Wikipedia – Die freie Enzyklopädie. Bearbeitungsstand: 9. Februar 2025, 11:49 UTC. URL: https://de.wikipedia.org/wiki/Anthropometrie. zuletzt abgerufen am 13.02.2025.

Die Landesbeauftragte für den Datenschutz Niedersachsen: Biometrie und Datenschutz (online). URL: https://www.lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/biometrie/biometrie-und-datenschutz-55984.html. zuletzt abgerufen am 13.02.2025.

Hill, Jürgen: Automatisierte Altersverifikation: KI checkt das Alter im Edeka-Markt. computerwoche.de, 30.04.2024 (online). URL: https://www.computerwoche.de/article/2833949/ki-checkt-das-alter-im-edeka-markt.html. zuletzt abgerufen am 06.02.2025.

IBM: Was ist ein KI-Modell. ibm (online). URL: https://www.ibm.com/de-de/topics/ai-model „Was ist ein KI-Modell“. zuletzt abgerufen am 06.02.2025.

Krempl, Stefan: Digital Services Act: Rechtliches Betriebssystem gegen das wilde Netz. 16.12.2020, heise online (online). URL: https://www.heise.de/news/Digital-Services-Act-Rechtliches-Betriebssystem-gegen-das-wilde-Netz-4991003.html. zuletzt abgerufen am 13.02.2025.

Meineck, Sebastian: Wie Alterskontrollen das Internet umkrempeln sollen. Netzpolitik.org, 29.02.2024 (online). URL: https://netzpolitik.org/2024/ausweispflicht-wie-alterskontrollen-das-internet-umkrempeln-sollen/. zuletzt abgerufen am 13.02.2025.

Reuter, Markus: Ampel verpasst Grundrechteschutz bei der Regulierung künstlicher Intelligenz. Netzpolitik.org., 07.12.2022 (online). URL: https://netzpolitik.org/2022/ai-act-der-europaeischen-union-ampel-verpasst-grundrechteschutz-bei-der-regulierung-kuenstlicher-intelligenz/. zuletzt abgerufen am 04.02.2025.

Reuter, Wiebke: Umgang mit sensiblen Daten bei allgemeiner Videoüberwachung. In: Zeitschrift für Datenschutz 2018, 564–569. zit. als: Reuter, ZD 2018, 564.

Roßnagel, Alexander: Der Datenschutz von Kindern in der DS-GVO. In: Zeitschrift für Datenschutz 2020, 88–92. zit. als: Roßnagel, ZD 2020, 88.

Solmecke, Christian: AI-Act wird schrittweise anwendbar. wbs legal, 18.12.2024 (online). URL: https://www.wbs.legal/it-und-internet-recht/datenschutzrecht/fahrplan-nach-in-kraft-treten-ai-act-wird-schrittweise-anwendbar-81008/. zuletzt abgerufen am 13.02.2025.

Stoll, Kathrin: Altersverifikation: So will Meta lügende Teenies erkennen. heise online, 05.11.2024 (online). URL: https://www.heise.de/news/Altersverifikation-So-will-Meta-luegende-Teenies-erkennen-10004849.html. zuletzt abgerufen am 06.02.2025.

Leitlinien und Guidelines

EDSA, Guidelines 2/2021 v. 07.07.2021

EuGH, Gutachten v. 26.07.2017, 1/15, Rn. 121 f.

EDSA, Leitlinien 03/2019, Version 2.0 v. 29.01.2020 Rn. 63 f.

EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (Adopted on 17 December 2024).

https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_de

https://ec.europa.eu/commission/presscorner/detail/de/ip_23_2413

Deutsches Kinderhilfswerk e. V.

Leipziger Straße 116-118
10117 Berlin
Fon: +49 30 308693-0
Fax: +49 30 308693-93
E-Mail: dkhw@dkhw.de
www.dkhw.de

Deutsches Zentralinstitut für soziale Fragen (DZI)

Geprüft + Empfohlen

ISBN: 978-3-922427-81-0