Stellungnahme 28/2024 zu bestimmten Datenschutzaspekten im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen von KI-Modellen

Angenommen am 17. Dezember 2024

Kurzfassung

KI-Technologien bieten zahlreiche Möglichkeiten und Vorteile für eine Vielzahl von Sektoren und gesellschaftlichen Aktivitäten.

Durch den Schutz des Grundrechts auf Datenschutz unterstützt die DSGVO diese Möglichkeiten und fördert andere EU-Grundrechte, darunter das Recht auf Gedanken-, Meinungs- und Informationsfreiheit, das Recht auf Bildung oder die unternehmerische Freiheit. Auf diese Weise ist die Datenschutz-Grundverordnung ein rechtlicher Rahmen, der verantwortungsvolle Innovation fördert.

In diesem Zusammenhang und unter Berücksichtigung der durch diese Technologien aufgeworfenen Datenschutzfragen ersuchte die irische Aufsichtsbehörde den EDSB um eine Stellungnahme zu Fragen von allgemeiner Geltung gemäß Artikel 64 Absatz 2 der Datenschutzgrundverordnung. Das Ersuchen bezieht sich auf die Verarbeitung personenbezogener Daten im Zusammenhang mit der Entwicklungs- und Einführungsphase von Modellen der Künstlichen Intelligenz ("**KI**"). Im Einzelnen geht es in dem Ersuchen um folgende Fragen: (1) wann und wie ein KI-Modell als "anonym" angesehen werden kann; (2) wie die für die Verarbeitung Verantwortlichen die Angemessenheit des berechtigten Interesses als Rechtsgrundlage in der Entwicklungs- und (3) der Einführungsphase nachweisen können; und (4) welche Folgen die unrechtmäßige Verarbeitung personenbezogener Daten in der Entwicklungsphase eines KI-Modells für die anschließende Verarbeitung oder den Betrieb des KI-Modells hat.

In Bezug auf die erste Frage wird in der Stellungnahme erwähnt, dass die Behauptung der Anonymität eines KI-Modells von den zuständigen ORKB von Fall zu bewertet werden sollte, da der EDSB der Ansicht ist, dass KI-Modelle, die mit personenbezogenen Daten trainiert wurden, nicht in allen Fällen als anonym angesehen werden können. Damit ein KI-Modell als anonym angesehen werden kann, sollte sowohl (1) die Wahrscheinlichkeit einer direkten (einschließlich probabilistischen) Extraktion personenbezogener Daten über Personen, deren personenbezogene Daten zur Entwicklung des Modells verwendet wurden, als auch (2) die Wahrscheinlichkeit, solche personenbezogenen Daten absichtlich oder unabsichtlich aus Abfragen zu erhalten, unter Berücksichtigung "*aller Mittel, die nach vernünftigem Ermessen* vom für die Verarbeitung Verantwortlichen oder einer anderen Person *verwendet werden können*", unbedeutend sein.

Für ihre Bewertung sollten die ORKBn die von der für die Verarbeitung Verantwortlichen zur Verfügung gestellten Unterlagen zum Nachweis der Anonymität des Modells prüfen. Diesbezüglich enthält die Stellungnahme eine nicht präskriptive und nicht erschöpfende Liste von Methoden, die von den für die Verarbeitung Verantwortlichen zum Nachweis der Anonymität verwendet werden können und somit von den ORKBn bei der Bewertung der Anonymitätsbehauptung eines für die Verarbeitung Verantwortlichen zu berücksichtigen sind. Dies betrifft beispielsweise die Ansätze, die von den für die Verarbeitung Verantwortlichen während der Entwicklungsphase verfolgt werden, um die Erhebung personenbezogener Daten, die für die Ausbildung verwendet werden, zu verhindern oder einzuschränken, ihre Identifizierbarkeit zu verringern, ihre Extraktion zu verhindern oder eine Zusicherung hinsichtlich der Widerstandsfähigkeit gegen Angriffe nach dem Stand der Technik zu geben.

In Bezug auf die zweite und dritte Frage enthält die Stellungnahme allgemeine Erwägungen, die die für die Verarbeitung Verantwortlichen bei der Beurteilung der Frage berücksichtigen sollten, ob sie sich auf ein berechtigtes Interesse als angemessene Rechtsgrundlage für die Verarbeitung im Zusammenhang mit der Entwicklung und dem Einsatz von KI-Modellen berufen können.

In der Stellungnahme wird daran erinnert, dass es keine Hierarchie zwischen den in der Datenschutz-Grundverordnung vorgesehenen Rechtsgrundlagen gibt und dass es Sache der für die Verarbeitung Verantwortlichen ist, die geeignete Rechtsgrundlage für ihre Verarbeitungstätigkeiten zu ermitteln. In der Stellungnahme wird dann an den Dreistufentest erinnert, der bei der Bewertung der Verwendung des berechtigten Interesses als Rechtsgrundlage durchgeführt werden sollte, . h. (1) Ermittlung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder einem verfolgt wird; (2) Analyse der Notwendigkeit der Verarbeitung für die Zwecke des/der verfolgten berechtigten Interesses/Interessen (auch als "Erforderlichkeitsprüfung" bezeichnet); und (3) Bewertung, dass das/die berechtigte(n) Interesse(e) nicht durch die Interessen oder Grundrechte und -freiheiten der betroffenen Personen überlagert wird/werden (auch als "Abwägungsprüfung" bezeichnet).

In Bezug auf den ersten Schritt wird in der Stellungnahme daran erinnert, dass ein Interesse als legitim angesehen werden kann, wenn die folgenden drei kumulativen Kriterien erfüllt sind: das Interesse (1) ist rechtmäßig, (2) ist klar und präzise formuliert und (3) ist real und gegenwärtig (d. h. nicht spekulativ). Ein solches Interesse kann sich beispielsweise auf die Entwicklung eines KI-Modells beziehen, d. h. auf die Entwicklung des Dienstes eines Gesprächsagenten zur Unterstützung der Nutzer, oder auf seinen Einsatz, d. h. auf die Verbesserung der Erkennung von Bedrohungen in einem Informationssystem.

In Bezug auf den zweiten Schritt wird in der Stellungnahme daran erinnert, dass bei der Beurteilung der Erforderlichkeit Folgendes zu berücksichtigen ist: (1) ob die Verarbeitung die Verfolgung des berechtigten Interesses ermöglicht; und
(2) ob es keine weniger einschneidende Möglichkeit zur Verfolgung dieses Interesses gibt. Bei der Beurteilung, ob die Bedingung der Erforderlichkeit erfüllt ist, sollten die ORKB besonders darauf achten, wie viele personenbezogene Daten verarbeitet werden und ob dies zur Verfolgung des berechtigten Interesses verhältnismäßig ist, auch im Hinblick auf den Grundsatz der Datenminimierung.

In Bezug auf den dritten Schritt wird in der Stellungnahme daran erinnert, dass die Abwägungsprüfung unter Berücksichtigung der besonderen Umstände des jeweiligen Falles durchgeführt werden sollte. Anschließend wird ein Überblick über die Elemente gegeben, die die ORKB bei der Beurteilung der Frage berücksichtigen können, ob das Interesse eines für die Verarbeitung Verantwortlichen oder eines Dritten gegenüber den Interessen, Grundrechten und Freiheiten der betroffenen Personen überwiegt.

Im Rahmen des dritten Schritts werden in der Stellungnahme spezifische Risiken für die Grundrechte hervorgehoben, die entweder in der Entwicklungs- oder in der Einsatzphase von KI-Modellen auftreten können. Außerdem wird klargestellt, dass sich die Verarbeitung personenbezogener Daten während der Entwicklungs- und der Einsatzphase von KI-Modellen auf unterschiedliche Weise auf die betroffenen Personen auswirken kann, was positiv oder negativ sein kann. Um solche Auswirkungen zu bewerten, können die ORKB die Art der von den Modellen verarbeiteten Daten, den Kontext der Verarbeitung und die möglichen weiteren Folgen der Verarbeitung berücksichtigen.

In der Stellungnahme wird außerdem die Rolle der berechtigten Erwartungen der betroffenen Personen bei der Abwägungsprüfung hervorgehoben. Dies kann aufgrund der Komplexität der in KI-Modellen verwendeten Technologien und der Tatsache, dass es für betroffene Personen schwierig sein kann, die Vielfalt ihrer potenziellen Verwendungen sowie die verschiedenen damit verbundenen Verarbeitungstätigkeiten zu verstehen, wichtig sein. In diesem Zusammenhang können sowohl die Informationen, die den betroffenen Personen zur Verfügung gestellt werden, als auch der Kontext der Verarbeitung zu den Elementen gehören, die zu berücksichtigen sind, um zu beurteilen, ob die betroffenen Personen vernünftigerweise erwarten können, dass ihre personenbezogenen Daten verarbeitet werden. In Bezug auf den Kontext kann dies Folgendes umfassen: ob die personenbezogenen Daten öffentlich zugänglich waren oder nicht, die Art der Beziehung zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen (und ob eine Verbindung zwischen den beiden besteht), die Art des Dienstes, der Kontext, in dem die personenbezogenen Daten erhoben wurden, die Quelle von der die Daten erhoben wurden (d. h. die Website oder der Dienst, auf der bzw. dem die personenbezogenen Daten erhoben wurden, und die Datenschutzeinstellungen, die sie bieten), die potenzielle Weiterverwendung des Modells und die Frage, ob den betroffenen Personen tatsächlich bewusst ist, dass ihre personenbezogenen Daten überhaupt online sind.

In der Stellungnahme wird auch daran erinnert, dass der für die Verarbeitung Verantwortliche in Fällen, in denen die Interessen, Rechte und Freiheiten der betroffenen Personen das/die von dem für die Verarbeitung Verantwortlichen oder einem verfolgte(n) berechtigte(n) Interesse(n) zu überwiegen scheinen, die Einführung mildernder Maßnahmen in Betracht ziehen kann, um die Auswirkungen der Verarbeitung auf die betroffenen Personen zu begrenzen. Abschwächende Maßnahmen sind nicht mit den Maßnahmen zu verwechseln, die der für die Verarbeitung Verantwortliche ohnehin gesetzlich ergreifen muss, um die Einhaltung der DSGVO zu gewährleisten. Darüber hinaus sollten die Maßnahmen auf die Umstände des Einzelfalls und die Merkmale des KI-Modells, einschließlich seines Verwendungszwecks, zugeschnitten sein. In diesem Zusammenhang enthält die Stellungnahme eine nicht erschöpfende Liste von Beispielen für Abhilfemaßnahmen in Bezug auf die Entwicklungsphase (auch in Bezug auf Web Scraping) und die Einführungsphase. Abschwächende Maßnahmen können einer raschen Entwicklung unterworfen sein und sollten auf die Umstände des Einzelfalls zugeschnitten werden. Daher obliegt es den Nachhaltigkeitsprüfungen, die Angemessenheit der getroffenen Abhilfemaßnahmen von Fall zu Fall zu beurteilen.

In Bezug auf die vierte Frage wird in den Schlussanträgen allgemein daran erinnert, dass ORKB über einen Ermessensspielraum verfügen, um die mögliche(n) Zuwiderhandlung(en) zu bewerten und unter der Umstände des geeignete, notwendige und verhältnismäßige Maßnahmen auszuwählen. In den werden dann drei Szenarien betrachtet.

In Szenario 1 werden personenbezogene Daten in dem KI-Modell gespeichert (was bedeutet, dass das Modell nicht als anonym betrachtet werden kann, wie in der ersten Frage beschrieben) und anschließend von demselben für die Verarbeitung Verantwortlichen verarbeitet (beispielsweise im Zusammenhang mit der Einführung des Modells). In der Stellungnahme heißt es, dass die Frage, ob die Entwicklungs- und die Einführungsphase getrennte Zwecke verfolgen (und somit getrennte Verarbeitungstätigkeiten darstellen) und inwieweit sich das Fehlen einer Rechtsgrundlage für ursprüngliche Verarbeitungstätigkeit auf die Rechtmäßigkeit der nachfolgenden Verarbeitung auswirkt, von Fall zu Fall und je nach dem Kontext des Falles beurteilt werden sollte.

Bei Szenario 2 werden personenbezogene Daten in dem Modell gespeichert und von einem anderen für die Verarbeitung Verantwortlichen Zusammenhang mit dem Einsatz des Modells verarbeitet. Diesbezüglich heißt es in der Stellungnahme, dass die ORKB berücksichtigen sollten, ob der für die Verarbeitung Verantwortliche, der das Modell einsetzt, im Rahmen seiner Rechenschaftspflicht zum Nachweis der Einhaltung von Artikel 5 Absatz 1 Buchstabe a und Artikel 6 DSGVO eine angemessene Bewertung durchgeführt hat, um sich zu vergewissern, dass das KI-Modell nicht durch unrechtmäßige Verarbeitung personenbezogener Daten entwickelt wurde. Diese Bewertung sollte beispielsweise Quelle personenbezogenen Daten und die Frage berücksichtigen, ob die Verarbeitung in der Entwicklungsphase Gegenstand eines Verstoßes war, insbesondere wenn dieser von einer ORKB oder einem Gericht festgestellt wurde, und sollte je nach den Risiken, die die Verarbeitung in der Errichtungsphase mit sich bringt, weniger oder detaillierter sein.

In Szenario 3 verarbeitet ein für die Verarbeitung Verantwortlicher unrechtmäßig personenbezogene Daten, um das KI-Modell zu entwickeln, und stellt dann sicher, dass diese anonymisiert werden, bevor derselbe oder ein anderer für die Verarbeitung Verantwortlicher eine weitere Verarbeitung personenbezogener Daten im Zusammenhang mit dem Einsatz einleitet. Diesbezüglich heißt es in der Stellungnahme, dass die Datenschutz-Grundverordnung nach Ansicht des EDSB keine Anwendung findet, wenn nachgewiesen werden kann, dass der anschließende Betrieb des KI-Modells keine Verarbeitung personenbezogener Daten nach sich zieht. Daher sollte die Rechtswidrigkeit der ursprünglichen Verarbeitung keine Auswirkungen auf den späteren Betrieb des Modells haben. Wenn die für die Verarbeitung Verantwortlichen in der Folge personenbezogene Daten verarbeiten, die während der Errichtungsphase erhoben wurden, nachdem das Modell anonymisiert wurde, gilt nach Ansicht des EDSB die Datenschutz-Grundverordnung für diese Verarbeitungen. In diesen Fällen vertritt der EDSB in seiner Stellungnahme die Auffassung, dass die Rechtmäßigkeit der in der Errichtungsphase durchgeführten Verarbeitung nicht durch die Rechtswidrigkeit der ursprünglichen Verarbeitung beeinträchtigt werden sollte.

Inhaltsübersicht

Der Europäische Datenschutzausschuss

gestützt auf Artikel 63 und Artikel 64 Absatz 2 der 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 (im Folgenden "DSGVO"),

gestützt auf das EWR-Abkommen, insbesondere auf Anhang XI und Protokoll 37, geändert durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018[1],

gestützt auf Artikel 10 und Artikel 22 seiner Geschäftsordnung, in Erwägung

nachstehender Gründe

(1) Die Hauptaufgabe des Europäischen Datenschutzausschusses (nachstehend **"Ausschuss"** oder **"EDSB"**) besteht darin, die einheitliche Anwendung der DSGVO im gesamten Europäischen Wirtschaftsraum (**"EWR"**) sicherzustellen. Artikel 64 Absatz 2 DSGVO sieht vor, dass jede Aufsichtsbehörde (**"SA"**), der Vorsitzende des Ausschusses oder die Kommission beantragen kann, dass jede Angelegenheit, die von allgemeiner Bedeutung ist oder Auswirkungen in mehr als einem EWR-Mitgliedstaat hat, vom Ausschuss geprüft wird, um eine Stellungnahme zu erhalten. Ziel dieser Stellungnahme ist es, eine Angelegenheit zu prüfen, die von allgemeiner Bedeutung ist oder Auswirkungen in mehr als einem EWR-Mitgliedstaat hat.

(2) Die Stellungnahme des Ausschusses wird gemäß Artikel 64 Absatz 3 DSGVO in Verbindung mit Artikel 10 Absatz 2 der Geschäftsordnung des EDSB innerhalb von acht Wochen nach der Entscheidung des Vorsitzenden und der zuständigen Aufsichtsbehörde, dass die Akte vollständig ist, angenommen. Auf Beschluss des Vorsitzenden kann diese Frist unter Berücksichtigung der Komplexität der Angelegenheit um weitere sechs Wochen verlängert werden.

HAT FOLGENDE STELLUNGNAHME ABGEGEBEN

1 Einführung

1.1 Zusammenfassung der Fakten

1. Am 4. September 2024 ersuchte die irische Aufsichtsbehörde (die "**IE SA**" oder "**ersuchende SA**") den EDSB um eine Stellungnahme gemäß Artikel 64 Absatz 2 DSGVO in Bezug auf KI-Modelle und die personenbezogener Daten ("**das Ersuchen**").

2. Am 13. September 2024 betrachteten der Vorsitzende des Ausschusses und der IE SA das Dossier als vollständig. Am folgenden Arbeitstag, dem 16. September 2024, wurde die Akte vom EDPB-Sekretariat übermittelt. In Anbetracht der Komplexität der Angelegenheit beschloss der Vorsitzende des Ausschusses, die gesetzliche Frist im Einklang mit Artikel 64 Absatz 3 der Datenschutz-Grundverordnung und Artikel 10 Absatz 4 der Geschäftsordnung des EDSB zu verlängern.

3. Der Antrag bezieht sich auf bestimmte Elemente des Trainings, der Aktualisierung, der Entwicklung und des Betriebs von KI-Modellen, bei denen personenbezogene Daten Teil des relevanten Datensatzes sind. Die IE SA betont, dass der Antrag

[1] Die in dieser Stellungnahme enthaltenen Verweise auf "Mitgliedstaaten" sind als Verweise auf "EWR-Mitgliedstaaten" zu verstehen. Bezugnahmen auf die "Union" in dieser Stellungnahme sind als Bezugnahmen auf den "EWR" zu verstehen.

betrifft Schlüsselfragen, die große Auswirkungen auf die betroffenen Personen und die für die Verarbeitung Verantwortlichen im EWR haben, und dass es zum gegenwärtigen Zeitpunkt keine harmonisierte Position der nationalen Kontrollstellen gibt[2]. Die für die Zwecke dieser Stellungnahme verwendete Terminologie wird in den Abschnitten 2.2 und 2.3 näher erläutert.

4. Die folgenden Fragen wurden von der IE SA gestellt:

Frage 1: Wird davon ausgegangen, dass das endgültige KI-Modell, das unter Verwendung personenbezogener Daten trainiert wurde, in allen Fällen nicht der Definition personenbezogener Daten entspricht (wie in Artikel 4 Absatz 1 der Datenschutzgrundverordnung festgelegt)?

Wenn die Antwort auf Frage 1 "ja" lautet:

i. In welchem Stadium der Verarbeitungsvorgänge, die zu einem KI-Modell führen, werden personenbezogene Daten nicht mehr verarbeitet?

   a) Wie kann nachgewiesen werden, dass das KI-Modell keine personenbezogenen Daten verarbeitet?

ii. Gibt es Faktoren, die dazu führen würden, dass die Funktionsweise des endgültigen KI-Modells nicht mehr als anonym angesehen werden kann?

   a) Wenn ja, wie können die Maßnahmen zur Abschwächung, Verhinderung oder zum Schutz vor diesen Faktoren (um sicherzustellen, dass das KI-Modell keine personenbezogenen Daten verarbeitet) nachgewiesen werden?

Wenn die Antwort auf Frage 1 "nein" lautet:

i. Unter welchen Umständen könnte dies der Fall sein?

   a) Wenn ja, wie können die Schritte nachgewiesen werden, die unternommen wurden, um sicherzustellen, dass das KI-Modell keine personenbezogenen Daten verarbeitet?

Frage 2: Wenn sich ein für die Verarbeitung Verantwortlicher auf berechtigte Interessen als Rechtsgrundlage für die Verarbeitung personenbezogener Daten beruft, um ein KI-Modell zu erstellen, zu aktualisieren und/oder weiterzuentwickeln, wie sollte dieser für die Verarbeitung Verantwortliche die Angemessenheit der berechtigten Interessen als Rechtsgrundlage nachweisen, und zwar sowohl in Bezug auf die Verarbeitung von Daten Dritter als auch von Daten erster Wahl?

i. Welche Erwägungen sollte der für die Verarbeitung Verantwortliche berücksichtigen, um sicherzustellen, dass die Interessen der betroffenen Personen, deren personenbezogene Daten verarbeitet werden, in angemessener Weise gegen die Interessen des für die Verarbeitung Verantwortlichen abgewogen werden, wenn es um Folgendes geht

   a) Daten von Dritten

   b) Erstanbieter-Daten

Frage 3: Wenn sich ein für die Verarbeitung Verantwortlicher nach der Schulung auf berechtigte Interessen als Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen eines KI-Modells oder eines KI-Systems, zu dem ein KI-Modell gehört, beruft, wie sollte ein für die Verarbeitung Verantwortlicher die Angemessenheit der berechtigten Interessen als Rechtsgrundlage nachweisen?

Frage 4: Wenn festgestellt wird, dass ein KI-Modell unter Verwendung unrechtmäßig verarbeiteter personenbezogener Daten erstellt, aktualisiert oder entwickelt wurde, welche Auswirkungen hat dies gegebenenfalls auf die Rechtmäßigkeit der weiteren oder späteren Verarbeitung oder des Betriebs des KI-Modells, entweder allein oder als Teil eines KI-Systems, wenn:

[2] Antrag, S.1.

i. Verarbeitet das KI-Modell, entweder allein oder als Teil eines KI-Systems, personenbezogene Daten?

ii. Weder das KI-Modell noch das KI-Modell als Teil eines KI-Systems verarbeitet personenbezogene Daten?

1.2 Zulässigkeit des Ersuchens um eine Stellungnahme nach Artikel 64 Absatz 2 der DSGVO

5. Artikel 64 Absatz 2 DSGVO sieht vor, dass jede Aufsichtsbehörde insbesondere beantragen kann, dass der Ausschuss jede Angelegenheit, die von allgemeiner Bedeutung ist oder Auswirkungen in mehr als einem Mitgliedstaat hat, im Hinblick auf die Einholung einer Stellungnahme prüft.

6. Die antragstellende ORKB richtete Fragen an den EDSB zu Datenschutzaspekten im Zusammenhang mit KI-Modellen. In ihrem Ersuchen führte sie aus, dass viele Organisationen inzwischen KI-Modelle, einschließlich großer Sprachmodelle ("**LLM**"), einsetzen, deren Betrieb, Schulung und Verwendung jedoch "*eine Reihe weitreichender Datenschutzbedenken*"[3] aufwirft, die "*Auswirkungen auf betroffene Personen in der gesamten EU/im EWR*"[4] haben.

7. Der Antrag wirft im Wesentlichen Fragen auf zu (i) der Anwendung des Begriffs der personenbezogenen Daten, (ii) Grundsatz der Rechtmäßigkeit unter besonderer Berücksichtigung der Rechtsgrundlage des berechtigten Interesses im Zusammenhang mit KI-Modellen sowie zu (iii) den Folgen einer unrechtmäßigen Verarbeitung personenbezogener Daten in der Entwicklungsphase von KI-Modellen auf die spätere Verarbeitung oder den Betrieb des Modells.

8. Der Ausschuss ist der Ansicht, dass der Antrag eine "*Angelegenheit von allgemeiner Bedeutung*" im Sinne von Artikel 64 Absatz 2 DSGVO betrifft. Insbesondere geht es um die Auslegung und Anwendung von Artikel 4 Absatz 1, Artikel 5 Absatz 1 Buchstabe a und Artikel 6 DSGVO in Bezug auf die Verarbeitung personenbezogener Daten bei der Entwicklung und dem Einsatz von KI-Modellen. Wie die antragstellende ORKB hervorhebt, wirft die Anwendung dieser Bestimmungen auf KI-Modelle systemische, abstrakte und neuartige Fragen auf[5]. Die rasche Entwicklung und der Einsatz von KI-Modellen durch immer mehr Organisationen wirft spezifische Fragen auf, und wie in dem Antrag hervorgehoben wird, *"wird der EDSB in hohem Maße davon profitieren, einen gemeinsamen Standpunkt zu in diesem Antrag aufgeworfenen Fragen zu erreichen, da diese Fragen für die kurz- und mittelfristig geplante Arbeit des EDSB von zentraler Bedeutung sind*"[6]. Darüber hinaus schaffen KI-Technologien viele Möglichkeiten und Vorteile für eine Vielzahl von Sektoren und gesellschaftlichen Aktivitäten. Außerdem ist die Datenschutz-Grundverordnung ein rechtlicher Rahmen, der verantwortungsvolle Innovation fördert. Daraus folgt, dass ein allgemeines Interesse daran besteht, diese Bewertung in Form einer Stellungnahme des EDSB vorzunehmen, um die kohärente Anwendung bestimmter Bestimmungen der Datenschutz-Grundverordnung im Zusammenhang mit KI-Modellen sicherzustellen.

9. Die alternative Bedingung von Artikel 64 Absatz 2 DSGVO bezieht sich auf Sachverhalte, die "*Wirkungen in mehr als einem Mitgliedstaat entfalten*". Der EDSB erinnert daran, dass der Begriff "Auswirkungen" *lato sensu* auszulegen ist und daher nicht nur auf rechtliche Auswirkungen beschränkt ist[7]. Da immer mehr KI-Modelle trainiert und von einer wachsenden Zahl von Organisationen im EWR verwendet werden, haben sie Auswirkungen auf eine große Zahl von betroffenen Personen

[3] Antrag, S.1.

[4] Ebd.

[5] Antrag, S. 2.

[6] Antrag, S.1. Wie im EDPB-Arbeitsprogramm für 2024-2025 erwähnt, das am 8. Oktober 2024 angenommen wurde und unter https://www.edpb.europa.eu/system/files/2024-10/edpb_work_programme_2024-2025_en.pdf ist, abrufbar plant der EDPB *unter anderem* die Herausgabe von Leitlinien zu Anonymisierung, Pseudonymisierung und Data Scraping im Zusammenhang mit generativer KI.

[7] EDPB, Internes Dokument 3/2019 zu internen Leitlinien zu Artikel 64 (2) DSGVO, angenommen am 8. Oktober 2019, Absatz 15, verfügbar unter . unter . www.edpb.europa.eu/system/files/2022-https://07/internaledpb_document_201903_art64.2_en.pdf.

im gesamten EWR, von denen einige bereits Bedenken bei ihrer zuständigen ORKB geäußert haben[8]. Daher ist der EDSB der Ansicht, dass die von der antragstellenden ORKB angesprochene Angelegenheit auch diese Bedingung erfüllt.

10. Der Antrag enthält eine schriftliche Begründung über den Hintergrund und die Beweggründe für die Vorlage der Fragen beim Ausschuss, einschließlich des einschlägigen Rechtsrahmens. Daher ist der Ausschuss der Ansicht, dass der Antrag im Einklang mit Artikel 10 Absatz 3 der EDPB-Geschäftsordnung begründet ist.

11. Gemäß Artikel 64 Absatz 3 der Datenschutz-Grundverordnung[9] gibt der EDSB keine Stellungnahme ab, wenn er bereits eine Stellungnahme zu der Angelegenheit abgegeben hat. Der EDSB hat noch keine Stellungnahme zu dieser Angelegenheit abgegeben und die Fragen, die sich aus dem Ersuchen ergeben, noch nicht beantwortet.

12. Aus diesen Gründen ist der Ausschuss der Ansicht, dass der Antrag zulässig ist und die sich daraus ergebenden Fragen in dieser Stellungnahme (die "**Stellungnahme**") gemäß Artikel 64 Absatz 2 der Datenschutz-Grundverordnung analysiert werden sollten.

2 Anwendungsbereich und Schlüsselbegriffe

2.1 Umfang der Stellungnahme

13. Der Ausschuss stimmt mit der antragstellenden ORKB darin überein, dass die Entwicklung und der Einsatz von KI-Modellen aus Sicht des Datenschutzes grundlegende Fragen des Datenschutzes aufwerfen. Die Fragen beziehen sich insbesondere auf: (i) wann und wie ein KI-Modell als "anonym" angesehen werden kann (Frage 1 des Antrags); (ii) wie die für die Verarbeitung Verantwortlichen die Angemessenheit des berechtigten Interesses als Rechtsgrundlage in der Entwicklungs- (Frage 2 des Antrags) und der Einführungsphase (Frage 3 des Antrags) nachweisen können; und (iii) ob die unrechtmäßige Verarbeitung personenbezogener Daten in der Entwicklungsphase Auswirkungen auf die Rechtmäßigkeit der nachfolgenden Verarbeitung oder des Betriebs des KI-Modells hat (Frage 4 des Antrags).

14. Der EDSB erinnert daran, dass die ORKB für die Überwachung der Anwendung der Datenschutz-Grundverordnung zuständig sind und zu ihrer einheitlichen Anwendung in der gesamten Union beitragen sollten[10]. Es daher in der Zuständigkeit der ORKB, spezifische KI-Modelle zu untersuchen und dabei Einzelfallprüfungen vorzunehmen.

15. Diese Stellungnahme bietet den zuständigen ORKB einen Rahmen für die Beurteilung konkreter Fälle, in denen sich (einige) der in dem Ersuchen aufgeworfenen Fragen stellen würden. Diese Stellungnahme erhebt keinen Anspruch auf Vollständigkeit, sondern enthält vielmehr allgemeine Überlegungen zur Auslegung der einschlägigen Bestimmungen, die die zuständigen ORKBn bei der Ausübung ihrer Ermittlungsbefugnisse weitestgehend berücksichtigen sollten. Diese Stellungnahme richtet sich zwar an die zuständigen ORKB und bezieht sich auf deren Tätigkeiten und Befugnisse, lässt jedoch die Verpflichtungen der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter nach der Datenschutz-Grundverordnung unberührt. Gemäß dem in Artikel 5 Absatz 2 DSGVO verankerten Grundsatz der Rechenschaftspflicht müssen die für die Verarbeitung Verantwortlichen für die Einhaltung aller Grundsätze im Zusammenhang mit der Verarbeitung personenbezogener Daten verantwortlich sein und dies auch nachweisen können.

16. In einigen Fällen können in der Stellungnahme einige Beispiele angeführt werden, aber in Anbetracht des breiten Spektrums im Ersuchen enthaltenen Fragen sowie der verschiedenen Arten von KI-Modellen, die darin behandelt werden, werden in dieser Stellungnahme nicht alle möglichen Szenarien berücksichtigt. Die mit KI-Modellen verbundenen Technologien sind einer raschen Entwicklung unterworfen; dementsprechend sollten die Überlegungen des EDPB in dieser Stellungnahme vor diesem Hintergrund interpretiert werden.

[8] Antrag, S. 1-2.

[9] Artikel 64 Absatz 3 der Datenschutz-Grundverordnung und Artikel 10 Absatz 4 der .

[10] Artikel 51 Absatz 1 DS-GVO und Artikel 51 Absatz 2 DS-GVO.

17. **In dieser Stellungnahme werden die nachstehenden Bestimmungen nicht analysiert, die bei der Bewertung der für KI-Modelle geltenden Datenschutzanforderungen dennoch eine wichtige Rolle spielen können:**

- **Verarbeitung besonderer Datenkategorien:** Der EDSB verweist auf das Verbot der Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 DSGVO und die begrenzten Ausnahmen gemäß Artikel 9 Absatz 2 DSGVO[11]. In diesem Zusammenhang hat der Gerichtshof der Europäischen Union (**"EuGH"**) weiter klargestellt, dass "*wenn ein Datensatz, der sowohl sensible als auch nicht-sensible Daten enthält, [...] en bloc erhoben wird, ohne dass es möglich ist, die Daten zum Zeitpunkt der Erhebung voneinander zu trennen, die Verarbeitung dieses Datensatzes als verboten im Sinne von Artikel 9 Absatz 1 der DSGVO anzusehen ist, wenn er mindestens ein sensibles Datenelement enthält und keine der Ausnahmen in Artikel 9 Absatz 2 dieser Verordnung gilt*"[12] . Darüber hinaus betonte der EuGH, dass *"für die Anwendung der Ausnahmeregelung des Artikels 9 Absatz 2 Buchstabe e der Datenschutz-Grundverordnung zu prüfen ist, ob die betroffene Person ausdrücklich und durch eine eindeutige bestätigende Handlung beabsichtigt hat, die betreffenden personenbezogenen Daten der Öffentlichkeit zugänglich zu machen"*[13]. Diese Überlegungen sollten berücksichtigt werden, wenn die Verarbeitung personenbezogener Daten im Rahmen von KI-Modellen besondere Datenkategorien umfasst.

- **Automatisierte Entscheidungsfindung, einschließlich Profiling**: Die im Rahmen von KI-Modellen durchgeführten Verarbeitungen können in den Anwendungsbereich von Artikel 22 DSGVO fallen, der den für die Verarbeitung Verantwortlichen zusätzliche Pflichten auferlegt und zusätzliche Garantien für die betroffenen Personen vorsieht. Der EDSB verweist in diesem Zusammenhang auf seine Leitlinien zur automatisierten Einzelentscheidung und zum Profiling für die Zwecke der Verordnung 2016/679[14].

- **Vereinbarkeit der Zwecke**: Artikel 6 Absatz 4 DSGVO enthält für bestimmte Rechtsgrundlagen Kriterien, die ein für die Verarbeitung Verantwortlicher zu berücksichtigen hat, um festzustellen, ob die Verarbeitung für einen anderen Zweck mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. Diese Bestimmung kann im Zusammenhang mit der Entwicklung und dem Einsatz von KI-Modellen relevant sein, und ihre Anwendbarkeit sollte von den ORKB bewertet werden.

- **Datenschutz-Folgenabschätzungen** ("**DPIAs**") (Artikel 35 GDPR): Datenschutz-Folgenabschätzungen sind ein wichtiges Element der Rechenschaftspflicht, wenn die Verarbeitung im Rahmen von KI-Modellen wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen wird[15].

- **Grundsatz des Datenschutzes durch Technik** (Artikel 25 Absatz 1 DSGVO): Der Datenschutz durch Technik ist eine wesentliche Schutzmaßnahme, die von den Aufsichtsbehörden im Zusammenhang mit der Entwicklung und dem Einsatz eines KI-Modells zu bewerten ist.

---

[11] Siehe auch den EDPB-Bericht über die Arbeit der ChatGPT-Taskforce, der am 23. Mai 2024 angenommen wurde, Absatz 18: "Bei der Verarbeitung besonderer Kategorien personenbezogener Daten muss zusätzlich eine der Ausnahmen von Artikel 9 Absatz 2 gelten, damit die Verarbeitung rechtmäßig ist. *Im Prinzip kann eine dieser Ausnahmen Artikel 9 Absatz 2 Buchstabe e der DSGVO sein. Die bloße Tatsache, dass personenbezogene Daten öffentlich zugänglich sind, bedeutet jedoch nicht, dass "die betroffene Person diese Daten offenkundig öffentlich gemacht hat" [...]*".

[12] Urteil des EuGH vom 4. Juli 2023, Rechtssache C-252/21, *Meta gegen Bundeskartellamt* (ECLI:EU:C:2023:537), Randnr. 89.

[13] Urteil des EuGH vom 4. Juli 2023, Rechtssache C-252/21, *Meta gegen Bundeskartellamt* (ECLI:EU:C:2023:537), Randnr. 77.

[14] Leitlinien der Artikel-29-Datenschutzgruppe (**"WP29"**) zur automatisierten Einzelentscheidung und zum Profiling für die Zwecke der Verordnung (EU) 2016/679 in der zuletzt überarbeiteten und am 6. Februar 2018 angenommenen Fassung, vom EDSB am 25. Mai 2018 gebilligt. Siehe auch Urteil des EuGH vom 7. Dezember 2023, Rechtssache C-634/21, *SCHUFA Holding u. a.* (ECLI:EU:C:2023:957).

[15] WP29-Leitlinien zur Datenschutz-Folgenabschätzung (DPIA) und zur Feststellung, ob die Verarbeitung im Sinne der Verordnung (EU) 2016/679 "wahrscheinlich zu einem hohen Risiko führt", überarbeitet und angenommen am 4. Oktober 2017, vom EDPB am 25. Mai 2018 gebilligt.

2.2 Schlüsselbegriffe

18. Einleitend möchte der EDSB die in dieser Stellungnahme verwendeten Begriffe und Konzepte erläutern, und zwar ausschließlich für die Zwecke dieser Stellungnahme:

- "**Erstdaten**" beziehen sich auf personenbezogene Daten, die der für die Verarbeitung Verantwortliche bei den betroffenen Personen erhoben hat.
- "**Daten von Dritten**" bezieht sich auf personenbezogene Daten, die die für die Verarbeitung Verantwortlichen nicht von den betroffenen Personen erhalten haben, sondern von einem gesammelt oder erhalten haben, beispielsweise von einem Datenmakler oder durch Web Scraping.
- "**Web Scraping**" ist eine gängige Technik zum Sammeln von Informationen aus öffentlich zugänglichen Online-Quellen. Informationen, die beispielsweise von Diensten wie Nachrichtenagenturen, sozialen Medien, Forendiskussionen und persönlichen Websites gesammelt werden, können personenbezogene Daten enthalten.
- Der Antrag bezieht sich auf den **"Lebenszyklus" von KI-Modellen** sowie auf verschiedene Phasen, die unter anderem die "Erstellung", die "Entwicklung", das "Training", die "Aktualisierung", die "Feinabstimmung", den "Betrieb" oder die "Nachschulung" von KI-Modellen betreffen. Der EDSB räumt ein, dass solche Phasen je nach den Umständen bei der Entwicklung und dem Einsatz von KI-Modellen stattfinden und die Verarbeitung personenbezogener Daten für verschiedene Verarbeitungszwecke umfassen können. Dennoch hält es der EDSB für die Zwecke dieser Stellungnahme für wichtig, die Kategorisierung der wahrscheinlich vorkommenden Phasen zu straffen. Daher spricht der EDSB für die Zwecke dieser Stellungnahme von der "**Entwicklungsphase**" und der "**Einführungsphase**". Die Entwicklung eines KI-Modells umfasst alle Phasen vor dem Einsatz des KI-Modells und beinhaltet unter anderem die Entwicklung des Codes, die Sammlung personenbezogener Trainingsdaten, die Vorverarbeitung der personenbezogenen Trainingsdaten und das Training. Der Einsatz eines KI-Modells umfasst alle Phasen, die mit der Nutzung eines KI-Modells zusammenhängen, und kann alle nach der Entwicklungsphase durchgeführten Maßnahmen umfassen. Der EDSB ist sich der Vielfalt der Anwendungsfälle und ihrer potenziellen Folgen für die Verarbeitung personenbezogener Daten bewusst; die ORKB sollten daher prüfen, ob die in dieser Stellungnahme enthaltenen Bemerkungen für die von ihnen zu bewertende Verarbeitung relevant sind.
- Der EDSB weist auch darauf hin, dass sich der Begriff "**Training**" erforderlichenfalls auf den Teil der Entwicklungsphase bezieht, in dem KI-Modelle aus Daten lernen, die ihnen zugedachte Aufgabe zu erfüllen (wie im nächsten Abschnitt dieser Stellungnahme erläutert).
- Der Begriff und der Anwendungsbereich von **KI-Modellen**, wie er vom EDPB für die Zwecke dieser Stellungnahme verstanden wird, wird im folgenden Abschnitt näher erläutert.

2.3 KI-Modelle im Zusammenhang mit der Stellungnahme

19. Im EU-Gesetz über künstliche Intelligenz ("**KI-Gesetz**")[16] wird ein "KI-System" wie folgt definiert: "*ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie arbeitet, und das nach seiner Einführung Anpassungsfähigkeit zeigen kann, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen können*"[17]. In Erwägungsgrund (12) des KI-Gesetzes wird der Begriff "KI-System" weiter erläutert. Ein wesentliches Merkmal von KI-Systemen ist demnach ihre Fähigkeit, Schlussfolgerungen zu ziehen. Die Techniken, die es ermöglichen

[16] 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 (Gesetz über künstliche Intelligenz).

[17] Artikel 3 Absatz 1 des AI-Gesetzes.

Inferenzen beim Aufbau eines KI-Systems umfassen maschinelles Lernen, logik- und wissensbasierte Ansätze.

20. KI-Modelle" hingegen werden im KI-Gesetz nur indirekt definiert: *Obwohl KI-Modelle wesentliche Bestandteile von KI-Systemen sind, stellen sie für sich genommen keine KI-Systeme dar. KI-Modelle bedürfen der Hinzufügung weiterer Komponenten, wie z.B. einer Benutzerschnittstelle, um zu KI-Systemen zu werden. KI-Modelle sind typischerweise in KI-Systeme integriert und bilden einen Teil von ihnen*"[18].

21. Der EDSB geht davon aus, dass die im Antrag vorgeschlagene Definition eines KI-Modells enger gefasst ist als die des KI-Gesetzes, da *der* Begriff "KI-Modell" "*das Produkt umfasst, das sich aus den Trainingsmechanismen ergibt, die im Zusammenhang mit künstlicher Intelligenz, maschinellem Lernen, Deep Learning oder anderen verwandten Verarbeitungskontexten auf einen Satz von Trainingsdaten angewandt werden",* und weiter ausgeführt wird: "*Der Begriff gilt für KI-Modelle, die für weiteres Training, Feinabstimmung und/oder Entwicklung vorgesehen sind, sowie für KI-Modelle, die dies nicht sind*[19].

22. Auf dieser Grundlage nahm der EDSB diese Stellungnahme an, wobei er davon ausging, dass sich ein KI-System auf ein KI-Modell stützt, um seinen beabsichtigten Zweck zu erfüllen, indem es das Modell in einen größeren Rahmen einbindet (z. B. könnte ein KI-System für den Kundendienst ein KI-Modell verwenden, das auf der Grundlage historischer Gesprächsdaten trainiert wurde, um Antworten auf Benutzeranfragen zu geben).

23. Darüber hinaus sind die für diese Stellungnahme relevanten KI-Modelle (oder "**Modelle**") solche, die durch einen Trainingsprozess entwickelt werden. Ein solcher Trainingsprozess ist ein Teil der Entwicklungsphase, in der die Modelle aus Daten lernen, um ihre beabsichtigte Aufgabe zu erfüllen. Der Trainingsprozess erfordert daher einen Datensatz, aus dem das Modell Muster erkennt und "lernt". In diesen Fällen verwendet das Modell verschiedene Techniken, um eine Darstellung des aus dem Trainingsdatensatz extrahierten Wissens zu erstellen. Dies ist vor allem beim maschinellen Lernen der Fall.

24. In der Praxis ist jedes KI-Modell ein Algorithmus, dessen Funktionsweise durch eine Reihe von Elementen bestimmt wird. Deep-Learning-Modelle haben beispielsweise häufig die Form eines neuronalen Netzes mit mehreren Schichten, die aus Knoten bestehen, die durch Kanten verbunden sind, die Gewichte haben, die während des Trainings angepasst werden, um die Beziehungen zwischen Eingaben und Ausgaben zu lernen. Die Merkmale eines einfachen Deep-Learning-Modells : (i) die Art und Größe jeder Schicht, (ii) das jeder Kante zugewiesene Gewicht (manchmal als "Parameter" bezeichnet), (iii) die Aktivierungsfunktionen[20] zwischen den Schichten und möglicherweise (iv) andere Operationen, die zwischen den Schichten stattfinden können. Beim Training eines einfachen Deep-Learning-Modells für die Bildklassifizierung werden beispielsweise Eingaben (die "**Bildpixel**") mit Ausgaben verknüpft, und die Gewichte können so angepasst werden, dass in den meisten Fällen die richtige Ausgabe erzeugt wird.

25. Weitere Beispiele für Deep-Learning-Modelle sind LLMs und generative KI, die z. B. für die Generierung menschenähnlicher Inhalte und die Erstellung neuer Daten verwendet werden.

26. **Auf der Grundlage der vorstehenden Erwägungen und im Einklang mit dem Ersuchen erstreckt sich der Anwendungsbereich dieser Stellungnahme nur auf die Untergruppe der KI-Modelle, die das Ergebnis eines Trainings solcher Modelle mit personenbezogenen Daten sind.**

3 Zur Begründetheit des Antrags

3.1 Über die Art von KI-Modellen in Bezug auf die Definition von personenbezogenen Daten

[18] Erwägungsgrund 97 AI-Gesetz.
[19] Antrag, S. 3.
[20] D. h. Funktionen, die auf der Grundlage von Eingaben und Gewichten die Ausgabe eines neuronalen Knotens berechnen, die dann an die nächste Schicht des neuronalen Netzes weitergeleitet wird.

27. Artikel 4 Absatz 1 DSGVO definiert personenbezogene Daten als "*alle Informationen über eine bestimmte oder bestimmbare natürliche Person*" (d. h. die betroffene Person). Darüber hinaus sieht Erwägungsgrund 26 DSGVO vor, dass die Datenschutzgrundsätze nicht für anonyme Informationen gelten sollten, d. h. Informationen, die sich nicht auf eine bestimmte oder bestimmbare natürliche Person beziehen, wobei "*alle Mittel, die nach vernünftigem Ermessen eingesetzt werden können*", von dem für die Verarbeitung Verantwortlichen oder einer anderen Person berücksichtigt werden. Dazu gehören: (i) Daten, die sich nie auf eine bestimmte oder bestimmbare Person bezogen haben, und (ii) personenbezogene Daten, die in einer anonymisiert wurden, dass die betroffene Person nicht oder nicht mehr identifizierbar ist.

28. Dementsprechend kann Frage 1[21] des Antrags dadurch beantwortet werden, dass analysiert wird, ob ein KI-Modell, das aus einem Training resultiert, das die Verarbeitung personenbezogener Daten beinhaltet, in allen Fällen als anonym betrachtet werden sollte. Aufgrund der Formulierung der Frage wird sich der EDSB in diesem Abschnitt auf den Prozess des "Trainings" eines KI-Modells beziehen.

29. Zuallererst möchte der EDPB die folgenden allgemeinen Überlegungen anstellen. KI-Modelle, unabhängig davon, ob sie mit personenbezogenen Daten trainiert wurden oder nicht, sind in der Regel darauf ausgelegt, Vorhersagen zu treffen oder Schlussfolgerungen zu ziehen, d. h. sie sind darauf ausgelegt, Schlussfolgerungen zu ziehen. Darüber hinaus sind KI-Modelle, die mit personenbezogenen Daten trainiert wurden, häufig so konzipiert, dass sie Rückschlüsse auf andere Personen ziehen als diejenigen, deren personenbezogene Daten zum Trainieren des KI-Modells verwendet wurden. Einige KI-Modelle sind jedoch speziell dafür ausgelegt, personenbezogene Daten über Personen bereitzustellen, deren personenbezogene Daten zum Trainieren des Modells verwendet wurden, oder solche Daten auf irgendeine Weise verfügbar zu machen. In diesen Fällen enthalten solche KI-Modelle von Natur aus (und in der Regel zwangsläufig) Informationen über eine bestimmte oder bestimmbare natürliche Person, so dass sie die Verarbeitung personenbezogener Daten beinhalten. Daher können diese Arten von KI-Modellen nicht als anonym angesehen werden. Dies wäre beispielsweise der Fall bei (i) einem generativen Modell, das anhand von Stimmaufnahmen einer Person feinabgestimmt wird, um deren zu imitieren, oder (ii) jedem Modell, das so konzipiert ist, dass es mit personenbezogenen Daten aus dem Training antwortet, wenn es nach Informationen über eine bestimmte Person gefragt wird.

30. Ausgehend von den obigen Erwägungen konzentriert sich der EDSB bei der Beantwortung von Frage 1 des Antrags auf die Situation von KI-Modellen, die nicht dazu bestimmt sind, personenbezogene Daten im Zusammenhang mit den Trainingsdaten zu liefern.

31. Der EDSB ist der Ansicht, dass selbst dann, wenn ein KI-Modell nicht absichtlich so konzipiert wurde, dass es aus den Trainingsdaten Informationen über eine identifizierte oder identifizierbare natürliche Person erzeugt, Informationen aus dem Trainingsdatensatz, einschließlich personenbezogener Daten, in den Parametern des Modells "absorbiert" bleiben können, d. h. durch mathematische Objekte dargestellt werden. Sie können sich von den ursprünglichen Trainingsdatenpunkten unterscheiden, aber immer noch die ursprünglichen Informationen dieser Daten enthalten, die letztendlich aus dem Modell extrahiert oder auf andere Weise direkt oder indirekt gewonnen werden können. Wann immer Informationen über bestimmte oder bestimmbare Personen, deren personenbezogene Daten zum Trainieren des Modells verwendet wurden, aus einem KI-Modell mit Mitteln gewonnen werden können, die nach vernünftigem Ermessen verwendet werden können, kann der Schluss gezogen werden, dass ein solches Modell nicht anonym ist.

32. In diesem Zusammenhang heißt es in dem Antrag: "*Bestehende Forschungsveröffentlichungen weisen auf einige potenzielle Schwachstellen hin, die in KI-Modellen vorhanden sein können und die zur Verarbeitung personenbezogener Daten führen könnten[(22),] sowie auf die Verarbeitung personenbezogener Daten, die stattfinden kann, wenn Modelle zur Verwendung mit anderen Daten eingesetzt werden, entweder über Anwendungsprogrammierschnittstellen (**"APIs"**) oder "prompte" Schnittstellen*[23].

[21] "*Wird davon ausgegangen, dass das endgültige KI-Modell, das unter Verwendung personenbezogener Daten trainiert wurde, in allen Fällen nicht der Definition von personenbezogenen Daten (gemäß Artikel 4 Absatz 1 DSGVO) entspricht*?

[22] Zum Beispiel Membership Inference Attacks (OWASP) und Model Inversion Attacks (OWASP & Veale et al, 2018).

[23] Antrag, S.1-2.

33. In diesem Sinne ist die Forschung zur Extraktion von Trainingsdaten besonders dynamisch[24]. Sie zeigt, dass es in einigen Fällen möglich ist, Mittel zu verwenden, die vernünftigerweise geeignet sind, personenbezogene Daten aus einigen KI-Modellen zu extrahieren, oder einfach durch Interaktionen mit einem KI-Modell (z. B. als Teil eines KI-Systems) versehentlich personenbezogene Daten zu erhalten. Kontinuierliche Forschungsanstrengungen in diesem Bereich werden dazu beitragen, die Restrisiken der Wiederverwendung[25] und der Extraktion personenbezogener Daten in jedem einzelnen Fall weiter zu bewerten.

34. **Auf der Grundlage der obigen Überlegungen ist der EDSB der Ansicht, dass KI-Modelle, die mit personenbezogenen Daten trainiert wurden, nicht in allen Fällen als anonym angesehen werden können. Stattdessen sollte die Feststellung, ob ein KI-Modell anonym ist, auf der Grundlage spezifischer Kriterien von Fall zu Fall beurteilt werden.**

3.2 Zu den Umständen, unter denen KI-Modelle als anonym angesehen werden können, und der damit verbundenen Demonstration

35. In Bezug auf Frage 1 Ersuchens[26] wird der EDSB ersucht, die Umstände zu klären, unter denen ein KI-Modell, das mit personenbezogenen Daten trainiert wurde, als anonym angesehen werden kann. In Bezug auf Frage 1(i)(a) des Antrags[27] wird der EDSB gebeten zu klären, welche Nachweise und/oder Unterlagen die ORKB bei der Beurteilung der Anonymität eines KI-Modells berücksichtigen sollten.

3.2.1 Allgemeine Überlegungen zur Anonymisierung im Zusammenhang mit der Seite

36. Die Verwendung des Ausdrucks "*alle Informationen*" in der Definition des Begriffs "*personenbezogene Daten*" in Artikel 4 Absatz 1 der Datenschutz-Grundverordnung spiegelt das Ziel wider, diesem Begriff einen weiten Geltungsbereich zuzuweisen, der alle Arten von Informationen umfasst, sofern sie *sich auf* die betroffene Person "*beziehen*", die identifiziert ist oder direkt oder indirekt identifiziert werden kann.

37. Informationen können sich auch dann auf eine natürliche Person beziehen, wenn sie technisch so organisiert oder kodiert sind (z. B. in einem ausschließlich maschinenlesbaren Format, unabhängig davon, ob es sich um ein geschütztes oder offenes Format handelt), dass der Bezug zu dieser natürlichen Person nicht unmittelbar erkennbar ist. In solchen Fällen können Softwareanwendungen verwendet werden, um bestimmte Daten leicht zu identifizieren, zu erkennen und zu extrahieren. Dies gilt insbesondere für KI-Modelle, bei denen die Parameter statistische Beziehungen zwischen den Trainingsdaten darstellen, und bei denen es möglich ist

---

[24] Siehe in diesem Zusammenhang zum Beispiel: (i) Veale M., Binns R., Edwards L., 2018, *Algorithms that remember: model inversion attacks and data protection law*. Phil. Trans. R. Soc. A 376: 20180083, verfügbar unter http://dx.doi.org/10.1098/rsta.2018.0083; (ii) Brown H., Lee K., Mireshghallah F., Shokri R., and Tramèr F., *What Does it Mean for a Language Model to Preserve Privacy?*, 2022, ACM Digital Library, FAccT '22, June 20, 2022, Seoul, Republic of Korea, verfügbar unter https://dl.acm.org/doi/abs/10.1145/3531146.3534642; (iii) Vassilev A., Oprea A., Fordyce A., Anderson H., *Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations*, Januar 2024, National Institute of Standards and Technology, verfügbar unter https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf; (iv) Carlini N., Tramèr F., Wallace E., Jagielski M., Herbert-Voss A., Lee K., Roberts A., Brown T., Song D., Erlingsson U., Oprea A., Raffel C., *Extracting Training Data from Large Language Models*, arXiv:2012.07805v2 [cs.CR] 15 Jun 2021, verfügbar unter https://arxiv.org/pdf/2012.07805; (v) Fredrikson M., Jha S., Ristenpart T., *Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures*, ACM Digital Library, 12 October 2015, verfügbar unter https://dl.acm.org/doi/abs/10.1145/2810103.2813677; (vi) Zhang Y., Jia R., Pei H., Wang W., Li B., Song D., *The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks*, arXiv:1911.07135v2 [cs.LG] 18 Apr 2020, verfügbar unter https://arxiv.org/pdf/1911.07135.

[25] Bei einem KI-System, das auf generativer KI basiert, entspricht die Regurgitation der Situation, in der sich die Ausgaben direkt auf die Trainingsdaten beziehen würden.

[26] "*Unter welchen Umständen könnte dies der Fall sein*?

[27] "*Wenn ja, wie können die Schritte nachgewiesen werden, die unternommen wurden, um sicherzustellen, dass das KI-Modell keine personenbezogenen Daten verarbeitet*?

Es ist möglich, genaue oder ungenaue (weil statistisch abgeleitete) personenbezogene Daten zu extrahieren, entweder direkt aus den Beziehungen zwischen den im Modell enthaltenen Daten oder durch Abfrage dieses Modells.

38. Da KI-Modelle in der Regel keine Datensätze enthalten, die direkt isoliert oder verknüpft werden können, sondern vielmehr Parameter, die probabilistische Beziehungen zwischen den im Modell enthaltenen Daten darstellen, kann es in realistischen Szenarien möglich sein, aus dem Modell Informationen abzuleiten[28], wie z. B. die Ableitung von Zugehörigkeiten. Damit eine ORKB mit dem für die Verarbeitung Verantwortlichen vereinbaren kann, dass ein bestimmtes KI-Modell als anonym angesehen werden kann, sollte sie daher zumindest prüfen, ob sie ausreichende Beweise dafür erhalten hat, dass i) personenbezogene Daten, die mit den Trainingsdaten in Zusammenhang stehen, nicht aus dem Modell extrahiert werden können[29] und ii) alle bei der Abfrage des Modells erzeugten Ausgaben sich nicht auf die betroffenen Personen beziehen, deren personenbezogene Daten zum Trainieren des Modells verwendet wurden.

39. Bei der Beurteilung, ob diese Bedingungen erfüllt sind, sollten drei Elemente von der NHB berücksichtigt werden.

40. Erstens sollten die ORKB die in den jüngsten WP29-Stellungnahmen und/oder EDPB-Leitlinien zu diesem Thema genannten Elemente berücksichtigen. In Bezug auf die Anonymisierung zum Zeitpunkt dieser Stellungnahme sollten die ORKB die Elemente in der Stellungnahme 05/2014 der WP29 zu Anonymisierungstechniken (die **"WP29-Stellungnahme 05/2014"**) berücksichtigen, in der es heißt, dass die Daten als anonym betrachtet werden können, wenn es nicht möglich ist, Informationen aus dem vermeintlich anonymen Datensatz , zu verknüpfen und abzuleiten[30]. Ferner heißt es dort, dass "*immer dann, wenn ein Vorschlag eines der Kriterien nicht erfüllt, eine gründliche Bewertung der Identifizierungsrisiken vorgenommen werden sollte*"[31]. **In Anbetracht der oben erwähnten Wahrscheinlichkeit einer Extraktion und eines Rückschlusses ist die EDPB**

[28] (i) Carlini N., Chien S., Nasr M., Song S., Terzis A., Tramer F., *Membership Inference Attacks From First Principles,* arXiv:2112.03570, verfügbar unter https://arxiv.org/abs/2112.03570;
(ii) Creţu A.M, Guépin F., and De Montjoye Y.A, *Correlation inference attacks against machine learning models*. Sci. Adv.10, eadj9260(2024). DOI:10.1126/sciadv.adj9260 verfügbar unter https://www.science.org/doi/10.1126/sciadv.adj9260;
(iii) Dana L., Pydi M. S., Chevaleyre Y., *Memorization in Attention-only Transformers* arXiv:2411.10115v1 [cs.AI] 15 November 2024, verfügbar unter: https://arxiv.org/abs/2411.10115;
(iv) Gehrke M., Liebenow J., Mohammadi E. & Braun T. et al. *Lifting in Support of Privacy-Preserving Probabilistic Inference*. Künstl Intell, 13. Juni 2024, verfügbar unter: https://doi.org/10.1007/s13218-024-00851-y;
(v) Hu H., *Membership Inference Attacks and Defenses on Machine Learning Models Literature*, verfügbar unter: https://github.com/HongshengHu/membership-inference-machine-learning-literature;
(vi) Nasr M., Carlini N., Hayase J., Jagielski M., Cooper A. F., Ippolito D., Choquette-Choo C. A., Wallace E., Tramèr F., and Lee K., *Scalable Extraction of Training Data from (Production) Language Models*, arXiv:2311.17035 28 November 2023, verfügbar unter: https://arxiv.org/abs/2311.17035;
(vii) Shokri R., Stronati M., Song C., Shmatikov V., *Membership Inference Attacks against Machine Learning Models* arXiv:1610.05820v2 [cs.CR], 31 March 2017, verfügbar unter https://arxiv.org/abs/1610.05820;
(viii) Staab R., Vero M., Mislav Balunović, Martin Vechev, 2024, *Beyond Memorization: Violating Privacy Via Inference with Large Language Models*, arXiv:2310.07298v2, 6. Mai 2024, verfügbar unter https://arxiv.org/abs/2310.07298;
(ix) Wu F., Cui L., Yao S., Yu S., *Inference Attacks in Machine Learning as a Service: A Taxonomy, Review, and Promising Directions* arXiv:2406.02027v1 [cs.LG], 27. Juni 2024, verfügbar unter https://arxiv.org/abs/2406.02027v1;
(x) Zhang J., Das D., Kamath G., Tramèr F., *Membership Inference Attacks Cannot Prove that a Model Was Trained On Your Data* arXiv:2409.19798v1, [cs.LG], 29 September 2024, verfügbar unter https://arxiv.org/abs/2409.19798;
(xi) Zhou Z., Xiang J., Chen C., and Su S., *Quantifying and Analyzing Entity-Level Memorization in Large Language Models*, arXiv:2308.15727v2 [cs.CL] 5 Nov 2023, verfügbar unter: https://arxiv.org/abs/2308.15727 .

[29] Die Extraktion umfasst insbesondere den Fall, dass personenbezogene Daten aus dem KI-Modell selbst abgeleitet werden, wobei die Abfrageschnittstellen kaum oder gar nicht verwendet werden.

[30] Stellungnahme der WP29 05/2014, S.24.

[31] Stellungnahme der WP29 05/2014, S.24.

ist der Ansicht, dass KI-Modelle sehr wahrscheinlich eine solch gründliche Bewertung der Risiken der Identifizierung erfordern.

41. Zweitens sollte diese Bewertung unter Berücksichtigung "*aller Mittel, die nach vernünftigem Ermessen* von dem für die Verarbeitung Verantwortlichen oder einer anderen Person zur Identifizierung von Personen *eingesetzt werden können*"[32], erfolgen, und die Bestimmung dieser Mittel sollte sich, wie in Erwägungsgrund 26 der Datenschutz-Grundverordnung erläutert, auf objektive Faktoren stützen, zu denen auch die folgenden gehören können:
    a. die Merkmale der Trainingsdaten selbst, das KI-Modell und das Trainingsverfahren[33];
    b. der Kontext, in dem das KI-Modell freigegeben und/oder verarbeitet wird[34];
    c. die zusätzlichen Informationen, die eine Identifizierung ermöglichen würden und der betreffenden Person zur Verfügung stehen könnten;
    d. die Kosten und den Zeitaufwand, die die Person benötigen würde, um diese zusätzlichen Informationen zu erhalten (falls sie ihr nicht bereits vorliegen)[35]; und
    e. die zum Zeitpunkt der Verarbeitung verfügbare Technologie sowie die technologischen Entwicklungen[36].

42. Drittens sollten die Kontrollstellen prüfen, ob die für die Verarbeitung Verantwortlichen das Risiko der Identifizierung durch den für die Verarbeitung Verantwortlichen und durch verschiedene Arten von "*anderen Personen*", einschließlich unbeabsichtigter Dritter, die auf das KI-Modell zugreifen, bewertet haben, wobei auch zu berücksichtigen ist, ob vernünftigerweise davon ausgegangen werden kann, dass sie in der Lage sind, Zugang zu den fraglichen Daten zu erhalten oder diese zu verarbeiten.

43. **Zusammenfassend vertritt der EDSB die Auffassung, dass für ein KI-Modell, das mit angemessenen Mitteln als anonym angesehen werden kann, sowohl (i) die Wahrscheinlichkeit einer direkten (einschließlich probabilistischen) Extraktion personenbezogener Daten von Personen, deren personenbezogene Daten zum Trainieren des Modells verwendet wurden, als auch (ii) die Wahrscheinlichkeit, solche personenbezogenen Daten absichtlich oder unabsichtlich aus Abfragen zu erhalten, für jede betroffene Person unbedeutend sein sollte[37]. Standardmäßig sollten die ORKB berücksichtigen, dass KI-Modelle wahrscheinlich eine gründliche Bewertung der Wahrscheinlichkeit einer Identifizierung erfordern, um zu einer Schlussfolgerung über ihren möglichen anonymen Charakter zu gelangen. Diese Wahrscheinlichkeit sollte unter Berücksichtigung "*aller Mittel, die nach vernünftigem Ermessen von* dem für die Verarbeitung Verantwortlichen oder einer anderen Person *eingesetzt werden* können", bewertet werden und auch eine unbeabsichtigte (Wieder-)Verwendung oder Offenlegung des Modells berücksichtigen.**

3.2.2 Elemente zur Bewertung der Restwahrscheinlichkeit der Identifizierung

44. Zwar können sowohl in der Entwicklungs- als auch in der Einführungsphase Maßnahmen ergriffen werden, um die Wahrscheinlichkeit zu verringern, dass personenbezogene Daten aus einem KI-Modell gewonnen werden, doch sollte bei der Bewertung der Anonymität eines KI-Modells auch der direkte Zugang zu dem Modell berücksichtigt werden.

45. Darüber hinaus sollten die ORKBn von Fall zu Fall bewerten, ob die Maßnahmen, die der für die Verarbeitung Verantwortliche ergriffen hat, um die Anonymität eines KI-Modells sicherzustellen und nachzuweisen, angemessen und wirksam sind.

---

[32] Urteil des EuGH vom 19. Oktober 2016, Rechtssache C-582/14, *Breyer/Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), Randnr. 43.

[33] Dazu gehören Merkmale wie die Einzigartigkeit der Datensätze in den Trainingsdaten, die Genauigkeit der Informationen, die Aggregation, die Randomisierung und insbesondere die Frage, wie sich diese auf die Anfälligkeit für eine Identifizierung auswirken.

[34] Dazu gehören auch kontextbezogene Elemente, wie die Beschränkung des Zugangs auf bestimmte Personen und rechtliche Garantien.

[35] Urteil des EuGH vom 7. März 2024, Rechtssache C-479/22 P, *OC gegen Europäische Kommission* (ECLI:EU:C:2024:215), Randnummer 50.

[36] Urteil des EuGH vom 7. März 2024, Rechtssache C-479/22 P, *OC gegen Europäische Kommission* (ECLI:EU:C:2024:215), Randnummer 50.

[37] Urteil des EuGH vom 19. Oktober 2016, Rechtssache C-582/14, *Breyer/Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), Randnr. 46, und Urteil des EuGH vom 7. März 2024, Rechtssache C-479/22 P, *OC/Europäische Kommission* (ECLI:EU:C:2024:215), Randnr. 51.

46. Insbesondere könnte die Schlussfolgerung der Bewertung einer ORKB unterschiedlich ausfallen, wenn es sich um ein öffentlich zugängliches KI-Modell handelt, zu dem eine unbekannte Anzahl von Personen mit einer unbekannten Bandbreite von Methoden Zugang hat, um zu versuchen, personenbezogene Daten zu extrahieren, oder wenn es sich um ein internes KI-Modell handelt, zu dem nur die Mitarbeiter Zugang haben. Während die für die Verarbeitung Verantwortlichen in beiden Fällen überprüfen sollten, ob sie ihrer Rechenschaftspflicht gemäß Artikel 5 Absatz 2 und Artikel 24 DSGVO nachgekommen sind, können sich die "*Mittel, die nach vernünftigem Ermessen von* anderen Personen *verwendet werden können*", auf das Spektrum und die Art der möglichen Szenarien auswirken, die zu berücksichtigen sind. Je nach dem Kontext der Entwicklung und des Einsatzes des Modells können die ORKB daher unterschiedliche Stufen der Prüfung und der Widerstandsfähigkeit gegen Angriffe in Betracht ziehen.

47. In diesem Zusammenhang stellt der EDSB im Folgenden eine nicht präskriptive und nicht erschöpfende Liste möglicher Elemente zur Verfügung, die von den für die Verarbeitung Verantwortlichen bei der Bewertung der Anonymitätsbehauptung eines für die Verarbeitung Verantwortlichen berücksichtigt werden können. Andere Ansätze können möglich sein, wenn sie ein gleichwertiges Schutzniveau bieten, insbesondere unter Berücksichtigung des Stands der Technik.

48. Das Vorhandensein oder Fehlen der unten aufgeführten Elemente ist kein schlüssiges Kriterium für die Bewertung der Anonymität eines KI-Modells.

3.2.2.1 AI-Modellentwurf

49. Im Hinblick auf die Gestaltung von KI-Modellen sollten die ORKB die von den Fluglotsen in der Entwicklungsphase verfolgten Ansätze bewerten. Die Anwendung und Wirksamkeit von vier Schlüsselbereichen (siehe unten) sollte in diesem Zusammenhang berücksichtigt werden.

Auswahl der Quellen

50. Der erste Bewertungsbereich umfasst die Prüfung der Auswahl der Quellen, die zum Training des KI-Modells verwendet werden. Dazu gehört die Bewertung aller Schritte, die zur Vermeidung oder Einschränkung der Erhebung personenbezogener Daten unternommen wurden, durch die ORKB, einschließlich u. a. (i) der Angemessenheit der Auswahlkriterien, (ii) der Relevanz und Angemessenheit der ausgewählten Quellen im Hinblick auf den/die beabsichtigten Zweck(e) und (iii) der Frage, ob ungeeignete Quellen ausgeschlossen wurden.

Datenaufbereitung und -minimierung

51. Der zweite Bereich der Bewertung bezieht sich auf die Aufbereitung der Daten für die Ausbildungsphase. Die ORKB sollten insbesondere Folgendes prüfen: (i) ob die Verwendung anonymer und/oder pseudonymisierter personenbezogener Daten in Betracht gezogen wurde; und (ii) wenn entschieden wurde, solche Maßnahmen nicht zu verwenden, die Gründe für diese Entscheidung unter Berücksichtigung des beabsichtigten Zwecks; (iii) die Strategien und Techniken zur Datenminimierung, die eingesetzt wurden, um den Umfang der in den Trainingsprozess einbezogenen personenbezogenen Daten zu begrenzen; und (iv) etwaige Datenfilterungsprozesse, die vor dem Modelltraining eingesetzt wurden, um irrelevante personenbezogene Daten zu entfernen.

Methodische Entscheidungen für die Ausbildung

52. Der dritte Bereich der Bewertung betrifft die Auswahl robuster Methoden bei der Entwicklung von KI-Modellen. SAs sollten methodische Entscheidungen bewerten, die die Identifizierbarkeit signifikant reduzieren oder eliminieren können, unter : (i) ob diese Methodik Regularisierungsmethoden verwendet, um die Modellgeneralisierung zu verbessern und die Überanpassung zu reduzieren; und, entscheidend, (ii) ob der Controller geeignete und wirksame Techniken zur Wahrung der Privatsphäre implementiert hat (z.B. differentielle Privatsphäre).

Maßnahmen bezüglich der Outputs des Modells

53. Der letzte Bewertungsbereich betrifft alle Methoden oder Maßnahmen, die dem KI-Modell selbst hinzugefügt werden und die sich zwar nicht auf das Risiko einer direkten Extraktion personenbezogener Daten für das Modell durch eine Person auswirken, die direkt darauf zugreift, aber die Wahrscheinlichkeit verringern könnten, dass personenbezogene Daten im Zusammenhang mit Trainingsdaten aus Abfragen gewonnen werden.

3.2.2.2 AI-Modell-Analyse

54. Damit die ORKB die Robustheit des entworfenen KI-Modells in Bezug auf die Anonymisierung beurteilen können, muss in einem ersten Schritt sichergestellt werden, dass der Entwurf wie geplant entwickelt wurde und einer wirksamen technischen Steuerung unterliegt. Die ORKB sollten bewerten, ob die für die Verarbeitung Verantwortlichen dokumentengestützte Prüfungen (intern oder extern) durchgeführt haben, die eine Bewertung der gewählten Maßnahmen und ihrer Auswirkungen zur Begrenzung der Wahrscheinlichkeit einer Identifizierung beinhalten. Dies könnte die Analyse von Berichten über Code-Reviews sowie eine theoretische Analyse umfassen, die die Angemessenheit der Maßnahmen dokumentiert, die zur Verringerung der Wahrscheinlichkeit einer erneuten Identifizierung des betreffenden Modells gewählt wurden.

3.2.2.3 Prüfung von KI-Modellen und Widerstand gegen Angriffe

55. Schließlich sollten die ORKB den Umfang, die Häufigkeit, die Quantität und die Qualität der Tests berücksichtigen, die der Kontrolleur an dem Modell durchgeführt hat. Insbesondere sollten die ORKBn berücksichtigen, dass erfolgreiche Tests, die weithin bekannte, dem Stand der Technik entsprechende Angriffe abdecken, nur ein Beweis für die Resistenz gegen diese Angriffe sein können. Zum Zeitpunkt dieser Stellungnahme könnte dies unter anderem strukturierte Tests gegen (i) Attribut- und Zugehörigkeitsinferenz, (ii) Exfiltration, (iii) Regurgitation von Trainingsdaten, (iv) Modellinversion oder (v) Rekonstruktionsangriffe umfassen.

3.2.2.4 Dokumentation

56. Gemäß den Artikeln 5, 24, 25 und 30 DSGVO und in Fällen, in denen ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zu erwarten ist, gemäß Artikel 35 DSGVO, müssen die für die Verarbeitung Verantwortlichen ihre Verarbeitungsvorgänge angemessen dokumentieren. Dies gilt auch für jede Verarbeitung, die das Training eines KI-Modells beinhaltet, selbst wenn das Ziel der Verarbeitung die Anonymisierung ist. Die Aufsichtsbehörden sollten eine solche Dokumentation und eine regelmäßige Bewertung der Folgerisiken für die von den für die Verarbeitung Verantwortlichen durchgeführten Verarbeitungen in Betracht ziehen, da dies grundlegende Schritte sind, um nachzuweisen, dass keine personenbezogenen Daten verarbeitet werden.

57. **Der EDSB ist der Ansicht, dass die ORKBn die Dokumentation berücksichtigen sollten, wenn die Behauptung der Anonymität eines bestimmten KI-Modells zu bewerten ist. Der EDSB stellt fest, dass, wenn eine ORKB nach der Bewertung der Anonymitätsbehauptung, auch im Lichte der Dokumentation, nicht bestätigen kann, dass wirksame Maßnahmen zur Anonymisierung des KI-Modells ergriffen wurden, die ORKB in der Lage wäre, davon auszugehen, dass der für die Verarbeitung Verantwortliche seinen Rechenschaftspflichten gemäß Artikel 5 Absatz 2 DSGVO nicht nachgekommen ist. Daher sollte auch die Einhaltung anderer Bestimmungen der DSGVO geprüft werden.**

58. Idealerweise sollten die SAs überprüfen, ob die Dokumentation des Kontrolleurs Folgendes enthält:

    a. alle Informationen im Zusammenhang mit der Datenschutzfolgenabschätzung, einschließlich aller Bewertungen und Entscheidungen, die eine Datenschutzfolgenabschätzung als nicht notwendig erachten;

    b. Ratschläge oder Rückmeldungen des **behördlichen** Datenschutzbeauftragten (sofern ein Datenschutzbeauftragter bestellt wurde oder hätte bestellt werden sollen);

    c. Informationen über die technischen und organisatorischen Maßnahmen, die bei der Entwicklung des KI-Modells getroffen wurden, um Wahrscheinlichkeit einer Identifizierung zu verringern, einschließlich des Bedrohungsmodells und der Risikobewertungen, auf die sich diese Maßnahmen stützen. Dazu sollten die spezifischen Maßnahmen für jede Quelle von Trainingsdatensätzen gehören, einschließlich relevanter Quell-URLs und Beschreibungen der getroffenen (oder bereits von Drittanbietern von Datensätzen getroffenen) Maßnahmen;

    d. die technischen und organisatorischen Maßnahmen, die in allen Phasen des Lebenszyklus des Modells ergriffen wurden und die entweder dazu beigetragen haben, dass keine personenbezogenen Daten im Modell enthalten sind, oder dies bestätigt haben;

    e. die Dokumentation, die die theoretische Widerstandsfähigkeit des KI-Modells gegenüber Re-Identifizierungsverfahren belegt, sowie die Kontrollen, mit denen der Erfolg und die Auswirkungen der wichtigsten Angriffe (Regurgitation, Membership-Inference-Angriffe, Exfiltration usw.) begrenzt oder bewertet werden sollen. Dies kann beinhalten, in

insbesondere: (i) das Verhältnis zwischen der Menge der Trainingsdaten und der Anzahl der Parameter im Modell, einschließlich der Analyse ihrer Auswirkungen auf das Modell[38]; (ii) Metriken zur Wahrscheinlichkeit einer erneuten Identifizierung auf der Grundlage des aktuellen Stands der Technik; (iii) Berichte darüber, wie das Modell getestet wurde (von wem, wann, wie und in welchem Umfang) und (iv) die Ergebnisse der Tests;

f. die Dokumentation, die dem/den für die Verarbeitung Verantwortlichen, der/die das Modell einsetzt/einsetzen, und/oder den betroffenen Personen zur Verfügung gestellt wird, insbesondere die Dokumentation zu den Maßnahmen, die ergriffen wurden, um die Wahrscheinlichkeit einer Identifizierung zu verringern, und zu den möglichen Restrisiken.

3.3 Zur Angemessenheit des berechtigten Interesses als Rechtsgrundlage für die personenbezogener Daten im Zusammenhang mit der Entwicklung und dem Einsatz von KI Modellen

59. Zur Beantwortung der Fragen 2 und 3 des Ersuchens wird der EDSB zunächst allgemeine Anmerkungen zu einigen wichtigen Aspekten machen, die die für die Verarbeitung Verantwortlichen unabhängig von der Rechtsgrundlage für die Verarbeitung berücksichtigen sollten, wenn sie beurteilen, wie die für die Verarbeitung Verantwortlichen die Einhaltung der DSGVO im Rahmen von KI-Modellen nachweisen können. Aufbauend auf den Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO[39] wird der EDSB dann die drei Schritte betrachten, die für die Bewertung des berechtigten Interesses im Zusammenhang mit der Entwicklung und dem Einsatz von KI-Modellen erforderlich sind.

3.3.1 Allgemeine Beobachtungen

60. Der EDSB erinnert daran, dass die Datenschutz-Grundverordnung keine Hierarchie zwischen den verschiedenen Rechtsgrundlagen in Artikel 6 Absatz 1 der Datenschutz-Grundverordnung [40].

61. Artikel 5 DSGVO legt die Grundsätze für die Verarbeitung personenbezogener Daten fest. Der EDSB hebt diejenigen hervor, die für diese Stellungnahme von Bedeutung sind und von den ORKB bei der Bewertung spezifischer KI-Modelle zumindest berücksichtigt werden sollten, sowie die wichtigsten Anforderungen aus anderen Bestimmungen der DSGVO unter Berücksichtigung des Anwendungsbereichs dieser Stellungnahme.

62. **Grundsatz der Rechenschaftspflicht** (Artikel 5 Absatz 2 DSGVO) - Dieser Grundsatz sieht vor, dass der für die Verarbeitung Verantwortliche für die Einhaltung der DSGVO verantwortlich ist und dies auch nachweisen kann. In diesem Zusammenhang sollten die Aufgaben und Zuständigkeiten der Parteien, die personenbezogene Daten im Zusammenhang mit der Entwicklung oder dem Einsatz eines KI-Modells verarbeiten, vor der Verarbeitung bewertet werden, um die Pflichten der für die Verarbeitung Verantwortlichen oder der gemeinsam für die Verarbeitung Verantwortlichen sowie der Auftragsverarbeiter (falls vorhanden) von Anfang an festzulegen.

63. **Grundsätze der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben und der Transparenz** (Artikel 5 Absatz 1 Buchstabe a DSGVO) - Bei der Beurteilung der Rechtmäßigkeit der Verarbeitung im Zusammenhang mit KI-Modellen hält es der EDSB im Lichte von Artikel 6 Absatz 1 DSGVO für sinnvoll, die verschiedenen Phasen der Verarbeitung personenbezogener Daten zu unterscheiden[41]. Der Grundsatz der Verarbeitung nach Treu und Glauben, der eng mit dem Grundsatz der Transparenz zusammenhängt, verlangt, personenbezogene Daten nicht mit unlauteren Mitteln, durch Täuschung oder in einer Weise verarbeitet werden, die "*ungerechtfertigt nachteilig, unrechtmäßig oder unzulässig*" ist.

---

[38] Ricciato F., *A Cautionary Reflection on (Pseudo-)Synthetic Data from Deep Learning on Personal Data*, Privacy in Statistical Databases conference (PSD 2024), Antibes, France, September 2024, Folien verfügbar unter: https://cros.ec.europa.eu/system/files/2024-10/20240926_PSD2024_Ricciato_v6_1.pdf und Belkin M., Hsu D., Ma S., & Mandal S. (2019), *Reconciling modern machine-learning practice and the classical bias-variance trade- off*. Proceedings of the National Academy of Sciences, 24. Juli 2019, 116(32) 15849-15854, verfügbar unter: https://www.pnas.org/doi/10.1073/pnas.1903070116

[39] Siehe EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024.

[40] Ebd., Absatz 1.

[41] EDPB-Bericht über die Arbeit der ChatGPT-Taskforce, angenommen am 23. Mai 2024, Absatz 14.

diskriminierend, unerwartet oder irreführend für die betroffene Person"[42]. In Anbetracht der Komplexität der beteiligten Technologien sollten die Informationen über die Verarbeitung personenbezogener Daten im Rahmen von KI-Modellen daher in zugänglicher, verständlicher und benutzerfreundlicher Form bereitgestellt werden[43]. Zur Transparenz der Verarbeitung personenbezogener Daten gehört insbesondere die Einhaltung der Informationspflichten gemäß Artikel 12 bis 14 DSGVO[44], die im Falle einer automatisierten Entscheidungsfindung, einschließlich Profiling, auch aussagekräftige Informationen über die zugrunde liegende Logik sowie über die Bedeutung und die voraussichtlichen Folgen der Verarbeitung für die betroffene Person verlangen[45]. In Anbetracht der Tatsache, dass in den Entwicklungsphasen von KI-Modellen große Datenmengen aus öffentlich zugänglichen Quellen (z. B. durch Web-Scraping-Techniken) erhoben werden können, ist die Inanspruchnahme der Ausnahmeregelung nach Artikel 14 Absatz 5 Buchstabe b DSGVO streng auf die Fälle beschränkt, in denen die Anforderungen dieser Vorschrift vollständig erfüllt sind[46].

64. **Zweckbindung und Grundsätze der Datenminimierung** (Artikel 5 Absatz 1 Buchstaben b und c DSGVO) - Gemäß dem Grundsatz der Datenminimierung ist es für die Entwicklung und den Einsatz von KI-Modellen erforderlich, dass personenbezogene Daten dem Zweck angemessen, dafür erheblich und notwendig sind. Dies kann die Verarbeitung personenbezogener Daten einschließen, um die Risiken potenzieller Verzerrungen und Fehler zu vermeiden, wenn dies im Rahmen des Zwecks klar und deutlich angegeben wird und die personenbezogenen Daten für diesen Zweck erforderlich sind (z. B. wenn sie nicht durch die Verarbeitung anderer Daten, einschließlich synthetischer oder anonymisierter Daten, effektiv erreicht werden können)[47]. Die WP29 hat bereits betont, dass "der *Zweck der Erhebung klar und deutlich angegeben werden muss* [...]"[48]. Bei der Beurteilung der Frage, ob der verfolgte Zweck rechtmäßig, spezifisch und eindeutig ist und ob die Verarbeitung mit dem Grundsatz der Datenminimierung im Einklang steht, sollte zunächst festgestellt werden, um welche Verarbeitungstätigkeit es geht. Insbesondere können die verschiedenen Phasen innerhalb der Entwicklungs- oder Einführungsphase dieselben oder unterschiedliche Verarbeitungstätigkeiten darstellen und mehrere für die Verarbeitung Verantwortliche oder gemeinsam Verantwortliche nach sich ziehen. In einigen Fällen ist es möglich, den Zweck, der mit dem Einsatz des KI-Modells verfolgt wird, bereits in einem frühen Entwicklungsstadium zu bestimmen. Selbst wenn dies nicht der Fall ist, sollte ein gewisser Kontext für diesen Einsatz bereits klar sein, und es sollte daher geprüft werden, wie dieser Kontext den Zweck der Entwicklung beeinflusst. Bei der Überprüfung des Zwecks der Verarbeitung in einem bestimmten Entwicklungsstadium sollten die ORKB von dem/den für die Verarbeitung Verantwortlichen ein gewisses Maß an Detailinformationen und eine Erklärung darüber erwarten, wie diese Details den Zweck der Verarbeitung erklären. Dazu können beispielsweise Informationen über die Art des entwickelten KI-Modells, seine erwarteten Funktionalitäten und andere relevante Zusammenhänge gehören, die in diesem bereits bekannt sind. Der Kontext des Einsatzes könnte zum Beispiel auch beinhalten, ob ein Modell für den internen Einsatz entwickelt wird, ob der für die Verarbeitung Verantwortliche beabsichtigt

[42] EDPB-Bericht über die Arbeit der ChatGPT-Taskforce, angenommen am 23. Mai 2024, Absatz 23; EDPB-Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen, Version 2.0, angenommen am 20. Oktober 2020, Absatz 69; Leitlinien der Artikel-29-Datenschutzgruppe zur Transparenz im Rahmen der Verordnung (EU) 2016/679, überarbeitet und angenommen am 11. April 2018, gebilligt vom EDPB am 25. Mai 2018, Absatz 2.

[43] Leitlinien der Artikel-29-Datenschutzgruppe zur Transparenz im Rahmen der Verordnung (EU) 2016/679, überarbeitet und angenommen am 11. April 2018, gebilligt durch den EDSB am 25. Mai 2018, Absatz 5.

[44] Siehe auch Erwägungsgrund 39 der Datenschutz-Grundverordnung, in dem es heißt, dass es "*für natürliche Personen transparent sein sollte, dass sie betreffende personenbezogene Daten erhoben, verwendet, abgefragt oder auf andere Weise verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden oder werden sollen [...]*".

[45] Artikel 13 Absatz 2 Buchstabe f der Datenschutz-Grundverordnung und Artikel 14 Absatz 2 Buchstabe g der Datenschutz-Grundverordnung.

[46] EDPB-Bericht über die Arbeit der ChatGPT-Taskforce, angenommen am 23. Mai 2024, Absatz 27.

[47] Darüber hinaus sieht Artikel 10 Absatz 5 des Gesetzes über künstliche Intelligenz besondere Vorschriften für die Verarbeitung besonderer Kategorien personenbezogener Daten in Bezug auf KI-Systeme mit hohem Risiko vor, um die Aufdeckung und Korrektur von Verzerrungen zu gewährleisten.

[48] Stellungnahme der Artikel-29-Datenschutzgruppe 03/2013 zur Zweckbindung (WP203), S. 15-16.

das Modell nach seiner Entwicklung an Dritte zu verkaufen oder zu vertreiben, einschließlich der Frage, ob das Modell in erster Linie für die Forschung oder für kommerzielle Zwecke eingesetzt werden soll.

65. **Rechte der betroffenen Person** (Kapitel III DSGVO) - Ungeachtet der Notwendigkeit, dass die Aufsichtsbehörden sicherstellen, dass alle Rechte der betroffenen Person bei der Entwicklung und dem Einsatz von KI-Modellen durch die für die Verarbeitung Verantwortlichen beachtet werden, erinnert der EDSB daran, dass immer dann, wenn sich ein für die Verarbeitung Verantwortlicher auf ein berechtigtes Interesse als Rechtsgrundlage beruft, das Widerspruchsrecht gemäß Artikel 21 der DSGVO gilt und gewährleistet werden sollte[49].

3.3.2 Überlegungen zu den drei Schritten der Bewertung des berechtigten Interesses im Zusammenhang mit der Entwicklung und dem Einsatz von KI-Modellen

66. Um festzustellen, ob eine bestimmte Verarbeitung personenbezogener Daten auf Artikel 6 Absatz 1 Buchstabe f DSGVO gestützt werden kann, sollten die ORKB überprüfen, ob die für die Verarbeitung Verantwortlichen sorgfältig geprüft und dokumentiert haben, ob die drei folgenden kumulativen Bedingungen erfüllt sind: (i) die Verfolgung eines berechtigten Interesses durch den für die Verarbeitung Verantwortlichen oder einen Dritten; (ii) die Verarbeitung ist zur Verfolgung des berechtigten Interesses erforderlich; und (iii) das berechtigte Interesse wird nicht durch die Interessen oder Grundrechte und -freiheiten der betroffenen Personen überlagert[50].

3.3.2.1 Erster Schritt - Verfolgung eines berechtigten Interesses durch den für die Verarbeitung Verantwortlichen oder durch einen Dritten

67. Ein Interesse ist das umfassendere Interesse oder der Vorteil, den ein für die Verarbeitung Verantwortlicher oder ein Dritter an einer bestimmten Verarbeitungstätigkeit haben kann[51]. Während die Datenschutz-Grundverordnung und der EuGH mehrere Interessen als legitim anerkennen[52], sollte die Bewertung der Legitimität eines bestimmten Interesses das Ergebnis einer Einzelfallanalyse sein.

68. Wie der EDSB in seinen Leitlinien zum berechtigten Interesse[53] in Erinnerung ruft, kann ein Interesse als berechtigt angesehen werden, wenn die folgenden drei Kriterien kumulativ erfüllt sind:

a. Das Interesse ist rechtmäßig[54];

---

[49] Legt eine betroffene Person Gründen, die sich aus ihrer besonderen Situation ergeben, Widerspruch gegen Verarbeitung sie betreffender personenbezogener Daten ein, so darf der für die Verarbeitung Verantwortliche die personenbezogenen Daten nicht mehr verarbeiten, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Die beiden Aspekte, die von den ORKB zu berücksichtigen sind, sind daher, ob der für die Verarbeitung Verantwortliche in der Lage ist, solche zwingenden, vorrangigen berechtigten Gründe nachzuweisen, und ob das Recht auf Widerspruch ausgeübt werden kann.

[50] EuGH, Urteil vom 4. Juli 2023, Rechtssache C-252/21, *Meta gegen Bundeskartellamt* (ECLI:EU:C:2023:537), Rn. 106; EuGH, Urteil vom 11. Dezember 2019, Rechtssache C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), Rn. 40. Siehe auch EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 12 und ff. Wie in diesen Leitlinien angemahnt, *sollte* diese *"Bewertung zu Beginn der Verarbeitung unter Einbeziehung des Datenschutzbeauftragten (DSB) (falls benannt) erfolgen und von dem für die Verarbeitung Verantwortlichen im Einklang mit dem in Artikel 5 Absatz 2 DSGVO festgelegten Grundsatz der Rechenschaftspflicht dokumentiert werden*".

[51] EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 14.

[52] EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 16.

[53] EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 17.

[54] EuGH, Urteil vom 4. Oktober 2024, Rechtssache C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), Randnummer 49, in der der EuGH betont, dass ein berechtigtes Interesse nicht Widerspruch zum Gesetz stehen darf. In diesem Zusammenhang betont der EDSB, dass bei der Beurteilung der Rechtmäßigkeit eines bestimmten Interesses gegebenenfalls der rechtliche Rahmen berücksichtigt werden sollte. Siehe zum Beispiel: Artikel 26 Absatz 3 und Artikel 28 der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt

b. Das Interesse ist klar und präzise formuliert; und

c. Das Interesse ist real und gegenwärtig, nicht spekulativ.

69. Vorbehaltlich der beiden anderen Schritte, die für die Bewertung des berechtigten Interesses erforderlich sind, können die folgenden Beispiele ein berechtigtes Interesse im Zusammenhang mit KI-Modellen darstellen: (i) Entwicklung des Dienstes eines Gesprächsagenten zur Unterstützung der Nutzer; (ii) Entwicklung eines KI-Systems zur Erkennung betrügerischer Inhalte oder Verhaltensweisen; und (iii) Verbesserung der Erkennung von Bedrohungen in einem Informationssystem.

3.3.2.2 Zweiter Schritt - Analyse der Notwendigkeit der Verarbeitung zur Verfolgung des berechtigten Interesses

70. Der zweite Schritt der Bewertung besteht in der Feststellung, ob die Verarbeitung personenbezogener Daten zur Wahrung der berechtigten Interessen erforderlich ist([55]) ("Erforderlichkeitsprüfung").

71. In Erwägungsgrund 39 der DSGVO wird klargestellt, dass "*personenbezogene Daten nur dann verarbeitet werden sollten, wenn der Zweck Verarbeitung vernünftigerweise nicht mit anderen Mitteln erreicht werden kann"*. Nach dem EuGH und früheren Leitlinien des EDSB sollte die Bedingung bezüglich der Notwendigkeit der Verarbeitung im Lichte der Grundrechte und -freiheiten der betroffenen Personen und in Verbindung mit dem in Artikel 5 Absatz 1 Buchstabe c DSGVO verankerten Grundsatz der Datenminimierung geprüft werden[56].

72. Die vom EuGH angeführte Methode berücksichtigt den Kontext der Verarbeitung die Auswirkungen auf den für die Verarbeitung Verantwortlichen und auf die betroffenen Personen. Die Beurteilung der Erforderlichkeit umfasst daher zwei Elemente: (i) ob die Verarbeitungstätigkeit die Verfolgung des Zwecks ermöglicht[57] und (ii) ob es keine weniger in die Privatsphäre eingreifende Möglichkeit gibt, diesen Zweck zu verfolgen[58].

---

für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) ("DSA") über verbotene gezielte Werbung an Minderjährige; Artikel 5 Absatz 1 und 2 des KI-Gesetzes über verbotene KI-Praktiken (manipulative Praktiken und unter der Schwelle des Bewusstseins); Verarbeitung unter Verletzung von Rechten des geistigen Eigentums und der Bestimmungen der Richtlinie (EU) 2019/790 über Urheberrecht und verwandte Schutzrechte im digitalen Binnenmarkt.

[55] EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absätze 28-30.

[56] EuGH, Urteil vom 4. Juli 2023, Rechtssache C-252/21, *Meta gegen Bundeskartellamt* (ECLI:EU:C:2023:537), Rn. 108 und 109, auch unter Verweis auf EuGH, Urteil vom 11. Dezember 2019, Rechtssache C-708/18, *Asociaţia de Proprietari bloc M5A- ScaraA* (ECLI:EU:C:2019:1064), Rn. 48; EuGH, Urteil vom 9. November 2010, verbundene Rechtssachen C-92/09 und C- 93/09, Volker und Markus Schecke (ECLI:EU:C:2010:662), Randnrn. 85 und 86; EuGH, Urteil vom 22. Juni 2021, Rechtssache C-439/19, *Latvijas Republikas Saeima* (ECLI:EU:C:2021:504), Randnrn. 98, 109, 110, 113. Siehe zum Beispiel auch: EDPB-Leitlinien 3/2019 über die Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0, angenommen am 29. Januar 2020, Rdnrn. 24-26 und 73; EDPB-Leitlinien 2/2019 über die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Version 2.0, angenommen am 8. Oktober 2019, Rdnrn. 23-25; EDPB-Stellungnahme 11/2024 über die Verwendung von Gesichtserkennung zur Rationalisierung des Passagierflusses an Flughäfen, Version 1.1, angenommen am 23. Mai 2024, Rdnr. 27.

[57] Siehe EuGH, Urteil vom 16. Dezember 2008, Rechtssache C-524/06, *Heinz Huber gegen Bundesrepublik Deutschland* (ECLI:EU:C:2008:724), Randnr. 66. Vgl. in derselben Rechtssache auch die Schlussanträge von Generalanwalt Poiares Maduro in der Rechtssache C-524/06, *Heinz Huber/Bundesrepublik Deutschland* (ECLI:EU:C:2008:194), Randnr. 16, in denen es heißt: "*Das richtige Kriterium ist das der Wirksamkeit, und es ist Sache des nationalen Gerichts, es anzuwenden. Es muss sich die Frage stellen, ob es andere Möglichkeiten der Datenverarbeitung gibt, mit denen die Einwanderungsbehörden die Vorschriften über den Aufenthaltsstatus durchsetzen könnten. Bejaht es diese Frage, ist die zentrale Speicherung und Verarbeitung der Daten von Unionsbürgern für rechtswidrig zu erklären. Es ist nicht erforderlich, dass das alternative System das wirksamste oder geeignetste ist; es reicht aus, dass es eine angemessene Leistung erbringen kann. Anders ausgedrückt: Selbst wenn das Zentralregister wirksamer oder zweckmäßiger oder benutzerfreundlicher ist als seine Alternativen (wie die dezentralen, lokalen Register), sind letztere eindeutig vorzuziehen, wenn sie zur Angabe des Aufenthaltsstatus von Unionsbürgern verwendet werden können"*.

[58] Siehe EuGH, Urteil vom 27. September 2017, Rechtssache C-73/16, *Peter Puškár* (ECLI:EU:C:2017:725), Randnr. 113: *"Es ist daher Sache des nationalen Gerichts, zu prüfen, ob die Erstellung der angefochtenen Liste und die Aufnahme der Namen der betroffenen Personen in ein solches Register geeignet sind, die damit verfolgten Ziele zu erreichen und*

73. So muss beispielsweise der mit dem KI-Modell beabsichtigte Umfang an personenbezogenen Daten im Hinblick auf weniger einschneidende Alternativen bewertet werden, die vernünftigerweise zur Verfügung stehen könnten, um den Zweck des verfolgten berechtigten Interesses ebenso wirksam zu erreichen. Wenn die Verfolgung des Zwecks auch durch ein KI-Modell möglich ist, das keine Verarbeitung personenbezogener Daten erfordert, sollte die Verarbeitung personenbezogener Daten als nicht erforderlich angesehen werden. Dies ist insbesondere für die Entwicklung von KI-Modellen relevant. Bei der Beurteilung, ob die Bedingung der Erforderlichkeit erfüllt ist, sollten die ORKB besonders darauf achten, wie viele personenbezogene Daten verarbeitet werden und ob die Verarbeitung zur Verfolgung des berechtigten Interesses verhältnismäßig ist, auch im Hinblick auf den Grundsatz der Datenminimierung.

74. Bei der Beurteilung der Erforderlichkeit sollte auch der breitere Kontext der beabsichtigten Verarbeitung personenbezogener Daten berücksichtigt werden. Ob es Mittel gibt, die weniger stark in die Grundrechte und -freiheiten der betroffenen Personen eingreifen, kann davon abhängen, ob der für die Verarbeitung Verantwortliche eine direkte Beziehung zu den betroffenen Personen hat (Erstdaten) oder nicht (Drittdaten). Der EuGH hat einige Erwägungen angestellt, die bei der Analyse der Notwendigkeit der Verarbeitung von Erstdaten zum Zwecke der Verfolgung berechtigter Interessen zu berücksichtigen sind (wenn auch im Zusammenhang mit der Weitergabe solcher Daten an Dritte)[59].

75. Die Umsetzung technischer Garantien zum Schutz personenbezogener Daten kann ebenfalls dazu beitragen, die Erforderlichkeitsprüfung zu erfüllen. Dazu könnte beispielsweise die Umsetzung von Maßnahmen wie den in Abschnitt 3.2.2 genannten gehören, die zwar keine Anonymisierung bewirken, aber dennoch die Identifizierung der betroffenen Personen erschweren. Der EDSB stellt fest, dass einige dieser Maßnahmen, auch wenn sie nicht erforderlich sind, um der DSGVO zu entsprechen, zusätzliche Garantien darstellen können, wie im Unterabschnitt "Abschwächende Maßnahmen" in Abschnitt 3.3.2.3[60] näher analysiert wird.

3.3.2.3 Dritter Schritt - Auswuchtungstest

76. Der dritte Schritt der Bewertung des berechtigten Interesses ist die "**Abwägung**" (in diesem Dokument auch als "**Abwägungstest**" bezeichnet)[61]. Dieser Schritt besteht darin, die verschiedenen gegensätzlichen Rechte und Interessen, die auf dem Spiel stehen, zu ermitteln und zu beschreiben[62], d. h. auf der einen Seite die Interessen, Grundrechte und Freiheiten der betroffenen Personen und auf der anderen Seite die Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten. Die besonderen Umstände des Falles sollten dann geprüft werden, um nachzuweisen, dass das berechtigte Interesse eine angemessene Rechtsgrundlage für die fraglichen Verarbeitungstätigkeiten ist[63].

Siehe auch die Schlussanträge des Generalanwalts Rantos in der Rechtssache C-252/21, *Meta gegen Bundeskartellamt*, ECLI:EU:C:2022:704, Randnr. 61, in denen es heißt: *"[...] Es ist daher erforderlich, dass ein enger Zusammenhang zwischen der Verarbeitung und dem verfolgten Interesse besteht, sofern keine datenschutzfreundlicheren Alternativen zur Verfügung stehen, da es nicht ausreicht, dass die Verarbeitung für den für die Verarbeitung Verantwortlichen lediglich von Nutzen ist"*.

[59] EuGH, Urteil vom 4 Oktober 2024, Rechtssache C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), Randnrn. 51-53.

[60] Siehe EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 57.

[61] Siehe EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absätze 31 bis 60.

[62] Siehe EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 32.

[63] Siehe EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Randnummer 32, auch unter Bezugnahme auf EuGH, Urteil vom 4. Juli 2023, Rechtssache C-252/21, *Meta gegen Bundeskartellamt* (ECLI:EU:C:2023:537), Randnummer 110.

Interessen, Grundrechte und Freiheiten der betroffenen Personen

77. Artikel 6 Absatz 1 Buchstabe f DSGVO sieht vor, dass der für die Verarbeitung Verantwortliche bei der Bewertung der verschiedenen Komponenten im Rahmen der Abwägungsprüfung die Interessen, Grundrechte und Freiheiten der betroffenen Personen berücksichtigen sollte. Die Interessen der betroffenen Personen sind diejenigen, die von der Verarbeitung betroffen sein können. Im Zusammenhang mit der Entwicklungsphase eines KI-Modells können dies unter anderem Interesse an der Selbstbestimmung und der Beibehaltung der Kontrolle über die eigenen personenbezogenen Daten (z. B. die für die Entwicklung des Modells erhobenen Daten) sein. Im Zusammenhang mit dem Einsatz eines KI-Modells können die Interessen der betroffenen Personen unter anderem das Interesse daran umfassen, die Kontrolle über die eigenen personenbezogenen Daten zu behalten (z. B. die Daten, die nach dem Einsatz des Modells verarbeitet werden), finanzielle Interessen (z. B. wenn ein KI-Modell von der betroffenen Person zur Erzielung von Einnahmen oder von einer Person im Rahmen ihrer beruflichen Tätigkeit verwendet wird), persönliche Vorteile (z. B. wenn ein KI-Modell zur Verbesserung der Zugänglichkeit zu bestimmten Dienstleistungen verwendet wird) oder sozioökonomische Interessen (z. B. wenn ein KI-Modell den Zugang zu einer besseren Gesundheitsversorgung ermöglicht oder die Ausübung eines Grundrechts wie des Zugangs zu Bildung erleichtert)[64].

78. Je genauer ein Interesse im Hinblick auf den beabsichtigten Zweck der Verarbeitung definiert wird, desto besser lässt sich die Realität der Vorteile und Risiken, die bei der Abwägung zu berücksichtigen sind, klar erkennen.

79. In Bezug auf die Grundrechte und -freiheiten der betroffenen Personen kann die Entwicklung und der Einsatz von KI-Modellen schwerwiegende Risiken für die durch die EU-Grundrechtecharta (die "**EU-Charta**") geschützten Rechte mit sich bringen, einschließlich, aber nicht beschränkt auf das Recht auf Privat- und Familienleben (Artikel 7 der EU-Charta) und das Recht auf Schutz personenbezogener Daten (Artikel 8 der EU-Charta). Diese Risiken können in der Entwicklungsphase auftreten, beispielsweise wenn personenbezogene Daten gegen den Willen der betroffenen Personen oder ohne deren Wissen abgegriffen werden. Diese Risiken können auch in der Einführungsphase auftreten, z. B. wenn personenbezogene Daten durch das Modell (oder als Teil des Modells) in einer Weise verarbeitet werden, die gegen die Rechte der betroffenen Personen verstößt, oder wenn es möglich ist, zufällig oder durch Angriffe (z. B. Ableitung von Zugehörigkeiten, Extraktion oder Modellumkehrung) darauf zu schließen, welche personenbezogenen Daten in der Lerndatenbank enthalten sind. Solche Situationen stellen ein Risiko für die Privatsphäre der betroffenen Personen dar, deren Daten in der Einsatzphase des KI-Systems auftauchen könnten (z. B. Reputationsrisiko, Identitätsdiebstahl oder Betrug, Sicherheitsrisiko je nach Art der Daten).

80. Je nach Fall kann es auch Risiken für andere Grundrechte geben. So kann beispielsweise eine groß angelegte und wahllose Datenerhebung durch KI-Modelle in der Entwicklungsphase bei den betroffenen Personen ein Gefühl der Überwachung hervorrufen, insbesondere wenn man bedenkt, wie schwierig es ist, zu verhindern, dass öffentliche Daten abgegriffen werden. Dies kann den Einzelnen zur Selbstzensur veranlassen und birgt die Gefahr, dass sein Recht auf freie Meinungsäußerung untergraben wird (Artikel 11 der EU-Charta). In der Einführungsphase bestehen ebenfalls Risiken für die Meinungsfreiheit, wenn KI-Modelle verwendet werden, um die Veröffentlichung von Inhalten durch betroffene Personen zu blockieren. Darüber hinaus kann ein KI-Modell, das gefährdeten Personen ungeeignete Inhalte empfiehlt, Risiken für deren psychische Gesundheit bergen (Artikel 3 Absatz 1 der EU-Charta). In anderen Fällen kann der Einsatz von KI-Modellen auch nachteilige Auswirkungen auf das Recht des Einzelnen auf Arbeit haben (Artikel 15 der EU-Charta), beispielsweise wenn Bewerbungen mithilfe eines KI-Modells vorausgewählt werden. Ebenso könnte ein KI-Modell Risiken für das Recht auf Nichtdiskriminierung (Artikel 21) bergen, wenn es Personen aufgrund bestimmter persönlicher Merkmale (wie Nationalität oder Geschlecht) diskriminiert. Außerdem ist die

[64] Siehe EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 38.

Der Einsatz von KI-Modellen kann auch Risiken für die Sicherheit des Einzelnen (z. B. wenn das KI-Modell in böser Absicht eingesetzt wird) sowie Risiken für seine körperliche und geistige Unversehrtheit bergen[65].

81. Der Einsatz von KI-Modellen kann sich auch positiv auf bestimmte Grundrechte auswirken, z. B. kann das Modell das Recht auf geistige Unversehrtheit der Person (Artikel 3 der Charta) unterstützen, etwa wenn ein KI-Modell verwendet wird, um schädliche Online-Inhalte zu identifizieren; oder das Modell kann den Zugang zu bestimmten wesentlichen Diensten oder die Ausübung von Grundrechten erleichtern, wie den Zugang zu Informationen (Artikel 11 der EU-Charta) oder den Zugang zu Bildung (Artikel 14 der EU-Charta).

Auswirkungen der Verarbeitung auf die betroffenen Personen

82. Die Verarbeitung personenbezogener Daten, die während der Entwicklung und des Einsatzes von KI-Modellen stattfindet, kann sich auf unterschiedliche Weise auf die betroffenen Personen auswirken, die positiv oder negativ sein kann[66]. Wenn eine Verarbeitungstätigkeit beispielsweise Vorteile für die betroffene Person mit sich bringt, können diese bei der Abwägungsprüfung berücksichtigt werden. Das Vorhandensein solcher Vorteile kann zwar dazu führen, dass eine OR zu dem Schluss kommt, dass die Interessen für die Verarbeitung Verantwortlichen oder eines die Interessen, Grundrechte und Freiheiten der betroffenen Personen nicht überwiegen, doch kann eine solche Schlussfolgerung nur das Ergebnis einer Einzelfallanalyse sein, bei der alle geeigneten Faktoren berücksichtigt werden.

83. Die Auswirkungen der Verarbeitung auf die betroffenen Personen können beeinflusst werden durch (i) die Art der Daten, die durch die Modelle verarbeitet werden, (ii) den Kontext der Verarbeitung und (iii) die weiteren Folgen, die die Verarbeitung haben kann[67].

84. In Bezug auf die **Art der verarbeiteten Daten** sei daran erinnert, dass - abgesehen von besonderen Kategorien personenbezogener Daten und Daten über strafrechtliche Verurteilungen und Straftaten, die nach Artikel 9 bzw. 10 DSGVO zusätzlichen Schutz genießen - die Verarbeitung einiger anderer Kategorien personenbezogener Daten erhebliche Folgen für die betroffenen Personen haben kann. In diesem Zusammenhang sollte die Verarbeitung bestimmter Arten personenbezogener Daten, die sehr private Informationen offenlegen (z. B. Finanzdaten oder Standortdaten) für die Entwicklung und den Einsatz eines KI-Modells als möglicherweise mit schwerwiegenden Folgen für die betroffenen Personen verbunden angesehen werden. In der Einführungsphase können die Folgen einer solchen Verarbeitung für die betroffenen Personen beispielsweise wirtschaftlicher Art sein (z. B. Diskriminierung im Beschäftigungskontext) und/oder den Ruf schädigen (z. B. Diffamierung).

85. In Bezug auf den **Kontext der Verarbeitung** müssen zunächst die Elemente ermittelt werden, die Risiken für die betroffenen Personen schaffen könnten (z. B. die Art und Weise, in der das Modell entwickelt wurde, die Art und Weise, in der das Modell eingesetzt werden kann, und/oder ob die Sicherheitsmaßnahmen zum Schutz der personenbezogenen Daten angemessen sind). Die Art des Modells und die beabsichtigten betrieblichen Verwendungszwecke spielen eine Schlüsselrolle bei der Ermittlung solcher potenziellen Ursachen.

86. Es ist auch erforderlich, die Schwere dieser Risiken für die betroffenen Personen zu bewerten. Dabei kann unter anderem berücksichtigt werden, wie die personenbezogenen Daten verarbeitet werden (z. B. wenn sie mit anderen Datensätzen kombiniert werden), welchen Umfang die Verarbeitung und die Menge der verarbeiteten personenbezogenen Daten haben[68] (z. B. das Gesamtdatenvolumen, das Datenvolumen pro betroffene Person, die Anzahl der Personen)[69], die

[65] Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 46.
[66] Siehe EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 39.
[67] Siehe EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 32.
[68] Siehe EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 43.
[69] EuGH, Urteil vom 4. Juli 2023, Rechtssache C-252/21, *Meta gegen Bundeskartellamt* (ECLI:EU:C:2023:537), Randnummer 116.

Status der betroffenen Person (z. B. Kinder oder andere schutzbedürftige Personen) und ihre Beziehung zu dem für die Verarbeitung Verantwortlichen (z. B. wenn die betroffene Person ein Kunde ist). So kann beispielsweise der Einsatz von Web Scraping in der Entwicklungsphase - bei Fehlen ausreichender Garantien - aufgrund des großen Volumens der erhobenen Daten, der großen Zahl der betroffenen Personen und der wahllosen Erhebung personenbezogener Daten zu erheblichen Auswirkungen auf den Einzelnen führen.

87. **Die weiteren Folgen**, **die** die Verarbeitung haben kann, sollten bei der Bewertung Auswirkungen der Verarbeitung auf die betroffenen Personen ebenfalls berücksichtigt werden. Sie sollten von den ORKB Fall zu Fall unter Berücksichtigung der vorliegenden spezifischen Fakten bewertet werden.

88. Zu diesen Folgen kann auch (aber nicht nur) das Risiko einer Verletzung Grundrechte der betroffenen Personen gehören, wie im vorhergehenden Unterabschnitt beschrieben[70]. Die Risiken können nach Wahrscheinlichkeit und Schweregrad variieren und können sich aus der Verarbeitung personenbezogener Daten ergeben, die zu physischen, materiellen oder immateriellen Schäden führen könnte, insbesondere wenn die Verarbeitung zu Diskriminierung führen kann[71].

89. Wenn der Einsatz eines KI-Modells die Verarbeitung personenbezogener Daten sowohl i) von betroffenen Personen, deren personenbezogene Daten in dem in der Entwicklungsphase verwendeten Datensatz enthalten sind, als auch ii) von betroffenen Personen, deren personenbezogene Daten in der Einsatzphase verarbeitet werden, mit sich bringt, sollten die ORKB bei der Überprüfung der von einem für die Verarbeitung Verantwortlichen durchgeführten Abwägungsprüfung die Risiken für die Interessen, Rechte und Freiheiten jeder dieser Kategorien von betroffenen Personen unterscheiden und berücksichtigen.

90. **Schließlich sollte bei der Analyse der möglichen weiteren Folgen der Verarbeitung auch die Wahrscheinlichkeit des Eintretens dieser weiteren Folgen berücksichtigt werden**. Die Bewertung dieser Wahrscheinlichkeit sollte unter Berücksichtigung der bestehenden technischen und organisatorischen Maßnahmen und der besonderen Umstände des Falles erfolgen. So kann die ORKB beispielsweise prüfen, ob Maßnahmen ergriffen wurden, um einen möglichen Missbrauch des KI-Modells zu verhindern. Bei KI-Modellen, die für eine Vielzahl von Zwecken eingesetzt werden können, wie z. B. generative KI, kann dies Kontrollen umfassen, die ihre Verwendung für schädliche Praktiken so weit wie möglich einschränken, z. B. die Erstellung von Deepfakes, Chatbots, die für Desinformation, Phishing und andere Arten von Betrug verwendet werden, und manipulative KI/AI-Agenten (insbesondere wenn sie anthropomorph sind oder irreführende Informationen liefern).

Angemessene Erwartungen der betroffenen Personen

91. Gemäß Erwägungsgrund 47 der Datenschutz-Grundverordnung *"müsste in jedem Fall das Vorliegen eines berechtigten Interesses sorgfältig geprüft werden, einschließlich der Frage, ob die betroffene Person zum Zeitpunkt und im Zusammenhang mit der Erhebung der personenbezogenen Daten vernünftigerweise erwarten kann, dass eine Verarbeitung zu diesem Zweck erfolgen kann. Die Interessen und Grundrechte der betroffenen Person könnten insbesondere dann Vorrang vor dem Interesse des für die Verarbeitung Verantwortlichen haben, wenn personenbezogene Daten unter Umständen verarbeitet werden, unter denen die betroffenen Personen vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen können"*[72].

92. Angemessene Erwartungen spielen eine Schlüsselrolle bei der Abwägungsprüfung, nicht zuletzt aufgrund der Komplexität der in KI-Modellen verwendeten Technologie und der Tatsache, dass es für die betroffenen Personen schwierig sein kann, die

[70] Siehe Unterabschnitt "Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen" oben.
[71] Siehe Abschnitt 2.3 der EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024. Siehe auch Erwägungsgrund 75 der DSGVO für weitere Beispiele.
[72] Siehe auch EuGH, Urteil vom 4. Juli 2023, Rechtssache C-252/21, *Meta v. Bundeskartellamt* (ECLI:EU:C:2023:537), Randnr. 112; EuGH, Urteil vom 11. Dezember 2019, Rechtssache C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), Randnr. 58; EuGH, Urteil vom 4. Oktober 2024, Rechtssache C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), Randnr. 55.

die Vielfalt der möglichen Verwendungszwecke eines KI-Modells und die damit verbundene Datenverarbeitung[73]. Zu diesem Zweck können die den betroffenen Personen zur Verfügung gestellten Informationen berücksichtigt werden, um zu beurteilen, ob die betroffenen Personen vernünftigerweise erwarten können, dass ihre personenbezogenen Daten verarbeitet werden. Zwar kann das Fehlen von Informationen dazu beitragen, dass die betroffenen Personen nicht mit einer bestimmten Verarbeitung rechnen, doch reicht die bloße Erfüllung der in der Datenschutz-Grundverordnung festgelegten Transparenzanforderungen allein nicht aus, um davon auszugehen, dass die betroffenen Personen vernünftigerweise bestimmte Verarbeitung erwarten können[74]. Darüber hinaus bedeutet die Tatsache, dass Informationen über die Entwicklungsphase eines KI-Modells in den Datenschutzrichtlinien des für die Verarbeitung Verantwortlichen enthalten sind, nicht zwangsläufig, dass die betroffenen Personen vernünftigerweise erwarten können, dass dies geschieht; vielmehr sollte dies von den für die Verarbeitung Verantwortlichen anhand der spezifischen Umstände des Einzelfalls und unter Berücksichtigung aller relevanten Faktoren analysiert werden.

93. Bei der Bewertung der berechtigten Erwartungen der betroffenen Personen in Bezug auf die Verarbeitung in der Entwicklungsphase ist es wichtig, die in den Leitlinien des EDSB zum berechtigten Interesse[75] genannten Elemente zu berücksichtigen. Darüber hinaus ist es im Rahmen des Gegenstands dieser Stellungnahme wichtig, den weiteren Kontext der Verarbeitung zu berücksichtigen. Dazu gehören unter anderem die Frage, ob die personenbezogenen Daten öffentlich zugänglich waren, die Art Beziehung zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen (und ob eine Verbindung zwischen den beiden besteht), die Art des Dienstes, der Kontextin dem die personenbezogenen Daten erhoben wurden, die Quelle, aus der die Daten stammen (z. B. die Website oder der Dienst, auf der/dem die personenbezogenen Daten erhoben wurden, und die Datenschutzeinstellungen), die potenzielle weitere Verwendung des Modells und die Frage, ob die betroffenen Personen überhaupt wissen, dass ihre personenbezogenen Daten online sind.

94. In der Entwicklungsphase des Modells können die berechtigten Erwartungen der betroffenen Personen unterschiedlich sein, je nachdem, ob die zur Entwicklung des Modells verarbeiteten Daten von den betroffenen Personen veröffentlicht werden oder nicht. Darüber hinaus können die berechtigten Erwartungen auch davon abhängen, ob sie dem für die Verarbeitung Verantwortlichen die Daten direkt zur Verfügung gestellt haben (z. B. im Rahmen ihrer Nutzung des Dienstes) oder ob der für die Verarbeitung Verantwortliche sie aus einer anderen Quelle erhalten hat (z. B. über einen Dritten oder durch Scraping). In beiden Fällen sollten die Schritte, die unternommen wurden, um die betroffenen Personen über die Verarbeitungstätigkeiten zu informieren, bei der Bewertung der berechtigten Erwartungen berücksichtigt werden.

95. In der Einführungsphase des KI-Modells ist es ebenso wichtig, die angemessenen Erwartungen der betroffenen Personen im Zusammenhang mit den spezifischen Fähigkeiten des Modells zu berücksichtigen. Bei KI-Modellen, die sich an die bereitgestellten Eingaben anpassen können, kann es beispielsweise relevant sein, zu prüfen, ob den betroffenen Personen bewusst war, dass sie personenbezogene Daten bereitgestellt hatten, damit das KI-Modell seine Antworten auf ihre Bedürfnisse abstimmen konnte und sie maßgeschneiderte Dienstleistungen erhalten konnten. Ferner kann es relevant sein zu prüfen, ob sich diese Verarbeitungstätigkeit nur auf den den betroffenen Personen angebotenen Dienst auswirkt (z. B. die Personalisierung von Inhalten für einen bestimmten Nutzer) oder ob sie zur Änderung des allen Kunden angebotenen Dienstes verwendet wird (z. B. zur allgemeinen Verbesserung des Modells). Wie in der Entwicklungsphase kann es auch hier besonders wichtig sein, zu prüfen, ob eine direkte Verbindung zwischen den betroffenen Personen und dem für die Verarbeitung Verantwortlichen besteht. Eine solche direkte Verbindung kann es dem für die Verarbeitung Verantwortlichen zum Beispiel ermöglichen

[73] In seinem Urteil vom 4. Juli 2023 in der Rechtssache C-252/21, *Meta gegen Bundeskartellamt* (ECLI:EU:C:2023:537), Randnummer 123, stellte der EuGH zwar fest, dass die "Produktverbesserung" nicht grundsätzlich als berechtigtes Interesse ausgeschlossen werden kann, aber auch, dass es "*zweifelhaft ist, ob [...] das Ziel der 'Produktverbesserung' angesichts des Umfangs dieser Verarbeitung und ihrer erheblichen Auswirkungen auf den Nutzer sowie der Tatsache, dass der Nutzer vernünftigerweise nicht erwarten kann, dass diese Daten verarbeitet werden, [...] die Interessen und Grundrechte eines solchen Nutzers überwiegen kann, insbesondere wenn dieser Nutzer ein Kind ist*".

[74] Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 53.

[75] Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absätze 50-54.

den betroffenen Personen auf einfache Weise Informationen über die Verarbeitungstätigkeit und das Modell zur Verfügung zu stellen, die dann die berechtigten Erwartungen der betroffenen Personen beeinflussen könnten.

Abschwächende Maßnahmen

96. Wenn die Interessen, Rechte und Freiheiten der betroffenen Personen die von dem für die Verarbeitung Verantwortlichen oder einem Dritten verfolgten berechtigten Interessen zu überwiegen scheinen, kann der für die Verarbeitung Verantwortliche die Einführung von Abhilfemaßnahmen in Erwägung ziehen, um die Auswirkungen der Verarbeitung auf diese betroffenen Personen zu begrenzen. Mildernde Maßnahmen sind Schutzmaßnahmen, die auf die Umstände des Einzelfalls zugeschnitten sein sollten und von verschiedenen Faktoren abhängen, unter anderem von der beabsichtigten Verwendung des KI-Modells. Diese abmildernden Maßnahmen sollen sicherstellen, dass die Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten nicht überwiegen, so dass sich der für die Verarbeitung Verantwortliche auf diese Rechtsgrundlage berufen kann.

97. Wie in den Leitlinien des EDSB zum berechtigten Interesse ausgeführt, sollten mildernde Maßnahmen nicht mit den Maßnahmen verwechselt werden, die der für die Verarbeitung Verantwortliche ohnehin rechtlich ergreifen muss, um die Einhaltung der DSGVO zu gewährleisten, unabhängig davon, ob die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f DSGVO beruht[76]. Dies ist besonders wichtig für Maßnahmen, die beispielsweise die Einhaltung von Grundsätzen der Datenschutz-Grundverordnung wie dem Grundsatz der Datenminimierung erfordern.

98. Die nachstehende Liste von Maßnahmen ist nicht erschöpfend und nicht präskriptiv, und die Umsetzung der Maßnahmen sollte von Fall zu Fall geprüft werden. Während einige der nachstehenden Maßnahmen je nach den Umständen erforderlich sein können, um bestimmte Verpflichtungen der DSGVO zu erfüllen, können sie, wenn dies nicht der Fall ist, als zusätzliche Schutzmaßnahmen in Betracht gezogen werden. Darüber hinaus beziehen sich einige der unten genannten Maßnahmen auf Bereiche, die einer raschen Entwicklung und neuen Entwicklungen unterworfen sind, und sollten von den ORKB bei der Bearbeitung eines konkreten Falles berücksichtigt werden.

99. **In Bezug auf die Entwicklungsphase von KI-Modellen** können verschiedene Maßnahmen ergriffen werden, um die Risiken zu mindern, die sich aus der Verarbeitung von Daten sowohl von Erstanbietern als auch von Dritten ergeben (einschließlich der Risiken im Zusammenhang mit Web-Scraping-Verfahren). Auf der Grundlage der obigen Ausführungen liefert der EDSB einige Beispiele für Maßnahmen, die zur Minderung der im Rahmen der Abwägungsprüfung ermittelten Risiken ergriffen werden können und von den ORKB bei der Bewertung spezifischer KI-Modelle auf Einzelfallbasis berücksichtigt werden sollten.

100. **Technische Maßnahmen:**

a. Die in Abschnitt 3.2.2 genannten Maßnahmen, die geeignet sind, die Risiken mindern, sofern diese Maßnahmen nicht zu einer Anonymisierung des Modells führen und nicht erforderlich sind, um anderen Verpflichtungen aus der DSGVO oder der Erforderlichkeitsprüfung (zweiter Schritt der Bewertung des berechtigten Interesses) nachzukommen.

101. Zusätzlich zu diesen Maßnahmen können weitere relevante Maßnahmen hinzukommen:

b. Pseudonymisierungsmaßnahmen: Dies könnte z. B. Maßnahmen umfassen, die jegliche Kombination von Daten auf der Grundlage individueller Identifikatoren verhindern. Diese Maßnahmen sind möglicherweise nicht angemessen, wenn die ORKB der Ansicht ist, dass der für die Verarbeitung Verantwortliche die begründete Notwendigkeit nachgewiesen hat, für die Entwicklung des betreffenden KI-Systems oder -Modells verschiedene Daten über eine bestimmte Person zu erfassen.

c. Maßnahmen zur Maskierung personenbezogener Daten oder zu ihrer Ersetzung durch gefälschte personenbezogene Daten im Trainingssatz (z. B. Ersetzung von Namen und E-Mail-Adressen durch gefälschte Namen und gefälschte E-Mails)

[76] Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 57.

Adressen). Diese Maßnahme kann besonders geeignet sein, wenn der tatsächliche materielle Inhalt der Daten für die Gesamtverarbeitung nicht relevant ist (z. B. bei der LLM-Ausbildung).

102. **Maßnahmen, die die Ausübung der Rechte des Einzelnen erleichtern:**

a. Einhaltung eines angemessenen Zeitraums zwischen der Erhebung eines Schulungsdatensatzes und seiner Verwendung. Diese zusätzliche Schutzmaßnahme kann es den betroffenen Personen ermöglichenihre Rechte während dieses Zeitraums auszuüben, wobei der angemessene Zeitraum je nach den Umständen des Einzelfalls zu beurteilen ist.

b. Vorschlag eines bedingungslosen "Opt-out" von Anfang an, z. B. durch die Gewährung eines Widerspruchsrechts für die betroffenen Personen vor der Verarbeitung, um die Kontrolle des Einzelnen über seine Daten zu stärken, was über Bedingungen von Artikel 21 DSGVO[77] hinausgeht.

c. Ermöglichung der Ausübung des Rechts auf Löschung durch die betroffenen Personen, auch wenn die in Artikel 17 Absatz 1 DSGVO aufgeführten besonderen Gründe nicht zutreffen[78].

d. Ermöglichung des Einreichens von Behauptungen über die Wiederholung oder Speicherung personenbezogener Daten durch die betroffenen Personen sowie der Umstände und Mittel, mit denen die Behauptungen reproduziert werden können, damit die für die Verarbeitung Verantwortlichen die entsprechenden Techniken zum Verlernen der Behauptungen reproduzieren und bewerten können.

103. **Transparenzmaßnahmen:** In einigen könnten zu den Abhilfemaßnahmen Maßnahmen gehören, die für mehr Transparenz bei der Entwicklung des KI-Modells sorgen. Einige Maßnahmen können zusätzlich zur Einhaltung der Verpflichtungen der Datenschutz-Grundverordnung dazu beitragen, die Informationsasymmetrie zu überwinden und den betroffenen Personen ein besseres Verständnis der Verarbeitung in der Entwicklungsphase zu ermöglichen:

a. Veröffentlichung von öffentlichen und leicht zugänglichen Mitteilungen, die über die in Artikel 13 oder 14 DSGVO geforderten Informationen hinausgehen, z. B. durch zusätzliche Angaben zu den Erfassungskriterien und allen verwendeten Datensätzen, wobei der besondere Schutz von Kindern und schutzbedürftigen Personen zu berücksichtigen ist.

b. Alternative Formen der Information der betroffenen Personen, z. B.: Medienkampagnen mit verschiedenen Medien zur Information der betroffenen Personen, Informationskampagne per E-Mail, Verwendung von grafischen Darstellungen, häufig gestellte Fragen, Transparenzetiketten und Modellkarten, deren Systematisierung die Präsentation von Informationen über KI-Modelle strukturieren könnte, sowie jährliche Transparenzberichte auf freiwilliger Basis.

104. **Spezifische Abhilfemaßnahmen im Zusammenhang mit Web Scraping:** In Anbetracht der Tatsache, dass Web Scraping, wie oben erwähnt, besondere Risiken birgt[79], könnten in diesem Zusammenhang besondere Maßnahmen zur Risikominderung festgelegt werden. Sie können von den Aufsichtsbehörden bei der Untersuchung von für die Verarbeitung Verantwortlichen, die Web-Scraping durchführen, gegebenenfalls zusätzlich zu den oben genannten Maßnahmen zur Risikominderung in Betracht gezogen werden.

105. Spezifische Maßnahmen können sich als nützlich erweisen, um das Risiko im Zusammenhang mit Web-Scraping zu mindern, auch wenn sie nach dem zweiten Schritt der Bewertung des berechtigten Interesses nicht erforderlich sind. Dazu können **technische Maßnahmen** gehören, wie z. B:

[77] Ebd.

[78] Ebd.

[79] Diese Praktiken können auch weitere Fragen aufwerfen, die in dieser Stellungnahme nicht behandelt werden, siehe z. B. Pagallo U., Ciani Sciolla J., *Anatomy of web data scraping: ethics, standards, and the troubles of the law.* European Journal of Privacy Law & Technologies, (2023) 2 S. 1 - 19, verfügbar unter: https://doi.org/10.57230/EJPLT232PS.

a. Ausschluss von Dateninhalten aus Veröffentlichungen, die personenbezogene Daten enthalten könnten, die Risiken für bestimmte Personen oder Personengruppen mit sich bringen (z. B. Personen, die bei einer Veröffentlichung der Informationen Missbrauch, Vorurteilen oder sogar körperlichen Schäden ausgesetzt sein könnten).

b. Sicherstellung, dass bestimmte Datenkategorien nicht erhoben werden oder dass bestimmte Quellen von der Datenerhebung ausgeschlossen werden; dazu könnten beispielsweise bestimmte Websites gehören, die aufgrund der Sensibilität ihres Themas besonders aufdringlich sind.

c. Ausschluss der Sammlung von Websites (oder Teilen von Websites), die sich eindeutig gegen Web-Scraping und die Wiederverwendung ihrer Inhalte für den Aufbau von KI-Trainingsdatenbanken aussprechen (z. B. durch Einhaltung von robots.txt- oder ai.txt-Dateien oder anderen anerkannten Mechanismen, die den Ausschluss von automatisiertem Crawling oder Scraping zum Ausdruck bringen).

d. Auferlegung anderer relevanter Beschränkungen für die Erhebung, möglicherweise einschließlich Kriterien auf der Grundlage von Zeiträumen.

106. Im Zusammenhang mit Web-Scraping können Beispiele für spezifische Maßnahmen **zur Erleichterung der Ausübung der Rechte des Einzelnen und der Transparenz** folgende sein: Erstellung einer von dem für die Verarbeitung Verantwortlichen verwalteten Opt-out-Liste, die es den betroffenen Personen ermöglicht, der Erhebung ihrer Daten auf bestimmten Websites oder Online-Plattformen zu widersprechen, indem sie Informationen zur Verfügung stellen, die sie auf diesen Websites identifizieren, auch bevor die Datenerhebung stattfindet[80].

107. **Spezifische Erwägungen zu Abhilfemaßnahmen in der Errichtungsphase:** Während einige der oben genannten Maßnahmen je nach den Umständen auch für die Errichtungsphase von Bedeutung sein können, enthält der EDPB im Folgenden eine nicht erschöpfende zusätzlicher unterstützender Maßnahmen, die durchgeführt werden können und von den NHB von Fall zu Fall bewertet werden sollten.

a. So können beispielsweise **technische Maßnahmen ergriffen** werden, um Speicherung, Wiederverwendung oder Generierung personenbezogener Daten zu verhindern, insbesondere im Zusammenhang mit generativen KI-Modellen (z. B. Output-Filter), und/oder um das Risiko einer unrechtmäßigen Wiederverwendung durch KI-Modelle für allgemeine Zwecke zu verringern (z. B. digitale Wasserzeichen für KI-generierte Outputs).

b. **Maßnahmen, die die Ausübung der Rechte des Einzelnen** in der Einführungsphase über das gesetzlich vorgeschriebene Maß hinaus **erleichtern oder beschleunigen**, insbesondere, aber nicht ausschließlich, die Ausübung des Rechts auf Löschung personenbezogener Daten aus den Modellausgabedaten oder die Deduplizierung sowie Nachschulungstechniken, die versuchen, personenbezogene Daten zu entfernen oder zu unterdrücken.

108. Bei der Untersuchung des Einsatzes eines bestimmten KI-Modells sollten die ORKB prüfen, ob der für die Verarbeitung Verantwortliche die von ihm durchgeführte Abwägungsprüfung veröffentlicht hat, da dies die Transparenz und Fairness erhöhen kann. Wie in den Leitlinien des EDSB zum berechtigten Interesse erwähnt, können andere Maßnahmen in Betracht gezogen werden, um den betroffenen Personen Informationen aus der Abwägungsprüfung vor der Erhebung personenbezogener Daten zur Verfügung zu stellen[81]. Der EDSB bekräftigt auch[82], dass ein zu berücksichtigendes Element darin besteht, ob der für die Verarbeitung Verantwortliche gegebenenfalls den DSB einbezogen hat.

[80] Es sei denn, der für die Verarbeitung Verantwortliche kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die der Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen dienen. [81] EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 68.
[82] EDPB-Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO, Version 1.0, angenommen am 8. Oktober 2024, Absatz 12.

3.4 Zu den möglichen Auswirkungen einer rechtswidrigen Verarbeitung bei der Entwicklung eines KI-Modells auf die Rechtmäßigkeit der nachfolgenden Verarbeitung oder des Betriebs des KI-Modells

109. Dieser Abschnitt der Stellungnahme befasst sich mit Frage 4 des Ersuchens. Mit dieser Frage soll geklärt werden, welche Auswirkungen eine unrechtmäßige Verarbeitung in der Entwicklungsphase auf die nachfolgende Verarbeitung (z. B. in der Einführungsphase des KI-Modells) oder auf den Betrieb des Modells haben kann. Die Frage bezieht sich sowohl auf die Situation, in der ein solches KI-Modell personenbezogene Daten verarbeitet, die in dem Modell gespeichert werden (Frage 4(i) der Anfrage), als auch auf die Situation, in der bei der Einführung des KI-Modells keine Verarbeitung personenbezogener Daten mehr stattfindet (d.h. das Modell ist anonym) (Frage 4(ii) der Anfrage).

110. Bevor auf bestimmte spezifische Szenarien eingegangen wird, stellt der EDPB die folgenden allgemeinen Überlegungen an.

111. Zunächst konzentrieren sich die Erläuterungen in diesem Abschnitt auf die Verarbeitung personenbezogener Daten in der Entwicklungsphase, die unter Missachtung des Grundsatzes der Rechtmäßigkeit gemäß Artikel 5 Absatz 1 Buchstabe a DSGVO und insbesondere Artikel 6 DSGVO (im Folgenden "**Rechtswidrigkeit**") erfolgt[83]. Dementsprechend konzentrieren sich die Überlegungen des EDSB auf die Auswirkungen der Rechtswidrigkeit der Verarbeitung in der Entwicklungsphase auf die Rechtmäßigkeit (d. h. die Einhaltung von Artikel 5 Absatz 1 Buchstabe a DSGVO und Artikel 6 DSGVO) der anschließenden Verarbeitung oder des Betriebs des Modells. Der EDSB weist jedoch darauf hin, dass die in der Entwicklungsphase durchgeführte Verarbeitung auch zu Verstößen gegen andere Bestimmungen der DSGVO führen kann, wie z. B. mangelnde Transparenz gegenüber den betroffenen Personen oder Datenschutz durch Technik und/oder Voreinstellungen, die in dieser Stellungnahme nicht untersucht werden.

112. Zweitens spielt bei der Beantwortung dieser Frage der Grundsatz der Rechenschaftspflicht eine wichtige Rolle, wonach die für die Verarbeitung Verantwortlichen *unter anderem* für die Einhaltung von Artikel 5 Absatz 1 DSGVO und Artikel 6 DSGVO[84] verantwortlich sind und dies auch nachweisen müssen. Dies gilt auch für die Notwendigkeit, zu beurteilen, welche Organisation der für die betreffende Verarbeitungstätigkeit Verantwortliche ist und ob Situationen gemeinsamer Verantwortlichkeit entstehen (da sie untrennbar miteinander verbunden sein können)[85]. In Anbetracht der Bedeutung faktischen Umstände jedes einzelnen Falles, auch im Hinblick auf die Rolle, die jede an der Verarbeitung beteiligte Partei spielt, sollten die Überlegungen des EDSB als allgemeine Beobachtungen verstanden werden, die von den ORKB von Fall zu Fall bewertet werden sollten.

113. Drittens unterstreicht der EDSB, dass die ORKB gemäß Artikel 51 Absatz 1 DSGVO "*für die Überwachung der Anwendung [der DSGVO] verantwortlich sind, um die Grundrechte und Grundfreiheiten natürlicher Personen in Bezug auf die Verarbeitung zu schützen und den freien Verkehr personenbezogener Daten in der Union zu erleichtern*". Es liegt daher in der Zuständigkeit der Aufsichtsbehörden, die Rechtmäßigkeit der Verarbeitung zu bewerten und die ihnen durch die DSGVO übertragenen Befugnisse im Einklang mit ihrem nationalen Rahmen auszuüben[86]. In solchen Fällen verfügen die Aufsichtsbehörden über einen Ermessensspielraum, um die mögliche(n) Verletzung(en) zu bewerten und geeignete, notwendige

[83] EuGH, Urteil vom 4. Mai 2023, Rechtssache C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), Randnrn. 55-57.
[84] EuGH, Urteil vom 4. Mai 2023, Rechtssache C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), Randnummer 53.
[85] EDPB-Leitlinien 07/2020 zu den Begriffen des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters in der Datenschutz-Grundverordnung, Version 2.1, angenommen am 7. Juli 2021, Absatz 55.
[86] Unter Umständen sind besondere nationale Vorschriften zu berücksichtigen. Siehe z. B. Artikel 2-decies des italienischen Datenschutzgesetzes (Gesetzesdekret 196/2003), in dem festgelegt ist, dass Daten, die unter Verstoß gegen die Datenschutzvorschriften verarbeitet werden, nicht verwendet werden dürfen. Dies gilt unbeschadet anderer einzelstaatlicher Rechtsvorschriften, wie etwa des Strafrechts.

und verhältnismäßige Maßnahmen, die zu den in Artikel 58 DSGVO genannten gehören, unter Berücksichtigung der Umstände jedes Einzelfalls[87].

114. **Wird ein Verstoß festgestellt, können die Aufsichtsbehörden Abhilfemaßnahmen anordnen, z. B. indem sie die für die Verarbeitung Verantwortlichen anweisen, unter Berücksichtigung der Umstände des Einzelfalls Maßnahmen zu ergreifen, um die Rechtswidrigkeit der ursprünglichen Verarbeitung zu beheben**. Dazu kann beispielsweise die Verhängung einer Geldbuße, die vorübergehende Einschränkung der Verarbeitung, die Löschung eines Teils des unrechtmäßig verarbeiteten Datensatzes oder, wenn dies nicht möglich ist, je nach und unter Berücksichtigung der Verhältnismäßigkeit der Maßnahme, die Löschung des gesamten für die Entwicklung des KI-Modells verwendeten Datensatzes und/oder des KI-Modells selbst gehören. Bei der Bewertung der Verhältnismäßigkeit der geplanten Maßnahme können die Aufsichtsbehörden Maßnahmen berücksichtigen, die von dem für die Verarbeitung Verantwortlichen ergriffen werden können, um die Rechtswidrigkeit der ursprünglichen Verarbeitung zu beheben (z. B. Umschulung).

115. Der EDSB weist auch darauf hin, dass betroffene Personen bei einer unrechtmäßigen Verarbeitung personenbezogener Daten unter den in Artikel 17 DSGVO festgelegten Bedingungen die Löschung ihrer personenbezogenen Daten beantragen können und dass die ORKB die Löschung der personenbezogenen Daten *von Amts wegen* anordnen können[88].

116. Bei der Beurteilung, ob eine Maßnahme geeignet, erforderlich und verhältnismäßig ist, können die ORKB unter anderem die Risiken für die betroffenen Personen, die Schwere des Verstoßes, die technische und finanzielle Durchführbarkeit der Maßnahme sowie den Umfang der betroffenen personenbezogenen Daten berücksichtigen.

117. Schließlich weist der EDSB darauf hin, dass die von den Aufsichtsbehörden im Rahmen der DSGVO ergriffenen Maßnahmen unbeschadet der Maßnahmen gelten, die von den zuständigen Behörden im Rahmen des AI-Gesetzes und/oder anderer geltender Rechtsrahmen (z. B. Rechtsvorschriften zur zivilrechtlichen Haftung) ergriffen werden.

118. In den folgenden Abschnitten befasst sich der EDSB mit drei Szenarien, die unter Frage 4 des Antrags fallen und bei denen die Unterschiede darin bestehen, ob die zur Entwicklung des Modells verarbeiteten personenbezogenen Daten in dem Modell gespeichert werden und/oder ob die anschließende Verarbeitung von demselben oder einem anderen für die Verarbeitung Verantwortlichen vorgenommen wird.

3.4.1 Szenario 1. Ein für die Verarbeitung Verantwortlicher verarbeitet unrechtmäßig personenbezogene Daten, um das Modell zu entwickeln, die personenbezogenen Daten werden in dem Modell gespeichert und anschließend von demselben für die Verarbeitung Verantwortlichen verarbeitet (z. B. im Zusammenhang mit dem Einsatz des Modells)

119. Dieses Szenario bezieht sich auf Frage 4(i) der Anfrage, in der Situation, in der ein für die Verarbeitung Verantwortlicher unrechtmäßig personenbezogene Daten verarbeitet (d.h. durch Nichtbeachtung von Artikel 5 Absatz 1(a) GDPR und Artikel 6 GDPR), um ein KI-Modell zu entwickeln, das KI-Modell Informationen über eine bestimmte oder bestimmbare natürliche Person enthält und somit nicht anonym ist. Personenbezogene Daten werden dann später von demselben für die Verarbeitung Verantwortlichen verarbeitet (beispielsweise im Zusammenhang mit dem Einsatz des Modells). In Bezug auf dieses Szenario enthält der EDPB die folgenden Überlegungen.

[87] Siehe hierzu Erwägungsgrund 129 DSGVO sowie EuGH, Urteil vom 26. September 2024, Rechtssache C-768-21, *TR gegen Land Hessen* (ECLI:EU:C:2024:785), Randnr. 37; EuGH, Urteil vom 7. Dezember 2023, verbundene Rechtssachen C-26/22 und C-64/22, SCHUFA Holding (Libération de reliquat de dette) (ECLI:EU:C:2023:958), Randnr. 57; und EuGH, Urteil vom 14. März 2024, Rechtssache C-46/23, Újpesti *Polgármesteri Hivatal* (ECLI:EU:C:2024:239), Randnr. 34.

[88] Diesbezüglich Stellungnahme 39/2021 des EDSB zu der Frage, ob Artikel 58 Absatz 2 Buchstabe g DSGVO als Rechtsgrundlage dafür dienen kann, dass eine Aufsichtsbehörde von Amts wegen die Löschung personenbezogener Daten anordnet, wenn die betroffene Person keinen entsprechenden Antrag gestellt hat, Absatz 28. Siehe in diesem Zusammenhang auch EuGH, Urteil vom 14. März 2024, Rechtssache C-46/23, Újpesti *Polgármesteri Hivatal* (ECLI:EU:C:2024:239), Randnr. 42.

120. Die Befugnis der ORKB, Abhilfemaßnahmen für die ursprüngliche Verarbeitung zu verhängen (wie unter den Ziffern 113, 114 und 115 erläutert), würde sich grundsätzlich auf die nachfolgende Verarbeitung auswirken (wenn die ORKB beispielsweise anordnet, dass der für die Verarbeitung Verantwortliche die unrechtmäßig verarbeiteten personenbezogenen Daten löscht, würden solche Abhilfemaßnahmen es ihm nicht erlauben, die personenbezogenen Daten, die Gegenstand der Maßnahmen waren, später zu verarbeiten).

121. Im Hinblick auf die Auswirkungen der unrechtmäßigen Verarbeitung in der Entwicklungsphase auf die nachfolgende Verarbeitung (z. B. in der Errichtungsphase) erinnert der EDSB daran, dass es Sache der ORKB ist, eine Einzelfallanalyse durchzuführen, die die besonderen Umstände jedes einzelnen Falles berücksichtigt.

122. **Ob die Entwicklungs- und die Einführungsphase getrennte Zwecke verfolgen (und somit getrennte Verarbeitungstätigkeiten darstellen) und inwieweit sich das Fehlen einer Rechtsgrundlage für die erste Verarbeitungstätigkeit auf die Rechtmäßigkeit der nachfolgenden Verarbeitung auswirkt, sollte von Fall zu Fall und je nach Kontext des Falles beurteilt werden.**

123. Wenn beispielsweise die nachfolgende Verarbeitung auf einem berechtigten Interesse beruht, sollte die Tatsache, dass die ursprüngliche Verarbeitung rechtswidrig war, bei der Bewertung des berechtigten Interesses berücksichtigt werden (z. B. im Hinblick auf die Risiken für die betroffenen Personen oder die Tatsache, dass die betroffenen Personen eine solche nachfolgende Verarbeitung möglicherweise nicht erwarten), insbesondere im Hinblick auf die Rechtsgrundlage von Artikel 6 Absatz 1 Buchstabe f DSGVO. In diesen Fällen kann die Rechtswidrigkeit der Verarbeitung in der Entwicklungsphase Auswirkungen auf die Rechtmäßigkeit der nachfolgenden Verarbeitung haben.

3.4.2 Szenario 2. Ein für die Verarbeitung Verantwortlicher verarbeitet unrechtmäßig personenbezogene Daten, um das Modell zu entwickeln, die personenbezogenen Daten werden in dem Modell gespeichert und von einem anderen für die Verarbeitung Verantwortlichen im Zusammenhang mit dem Einsatz des Modells verarbeitet

124. Dieses Szenario bezieht sich auf Frage 4(i) des Ersuchens. Es unterscheidet sich von Szenario 1 (in Abschnitt 3.4.1 dieser Stellungnahme), da personenbezogene Daten anschließend von einem anderen für die Verarbeitung Verantwortlichen im Zusammenhang mit der Einführung des KI-Modells verarbeitet werden.

125. Der EDSB weist darauf hin, dass die Bestimmung der Rollen, die diesen verschiedenen Akteuren im Rahmen des Datenschutzes zugewiesen werden, ein wesentlicher Schritt ist, um festzustellen, welche Verpflichtungen nach der DSGVO gelten und wer für diese Verpflichtungen verantwortlich ist, und dass bei der Bewertung der Verantwortlichkeiten der einzelnen Parteien nach der auch Situationen der gemeinsamen Kontrolle berücksichtigt werden sollten. Daher sollten die nachstehenden Bemerkungen als allgemeine Elemente betrachtet werden, die von den ORKB gegebenenfalls berücksichtigt werden sollten. Zu diesem Szenario 2 stellt der EDSB die folgenden Überlegungen an.

126. Zunächst sei daran erinnert, dass gemäß Artikel 5 Absatz 1 Buchstabe a DSGVO im Lichte von Artikel 5 Absatz 2 DSGVO jeder für die Verarbeitung Verantwortliche die Rechtmäßigkeit der von ihm durchgeführten Verarbeitung sicherstellen und nachweisen können muss. Daher sollten die ORKB die Rechtmäßigkeit der Verarbeitung durch i) den für die Verarbeitung Verantwortlichen, der das KI-Modell ursprünglich entwickelt hat, und ii) den für die Verarbeitung Verantwortlichen, der das KI-Modell erworben hat und die personenbezogenen Daten selbst verarbeitet, bewerten.

127. Zweitens sind die Überlegungen unter den Nummern 113, 114 und 115 in diesem Fall relevant, die Befugnis der ORKB betrifft, in Bezug auf die Erstverarbeitung einzugreifen. Artikel 17 Absatz 1 Buchstabe d der Datenschutz-Grundverordnung (Löschung unrechtmäßig verarbeiteter Daten) und Artikel 19 der Datenschutz-Grundverordnung (Meldepflicht für die Berichtigung oder Löschung personenbezogener Daten oder die Einschränkung der Verarbeitung) können je nach den Umständen des Falles in diesem Zusammenhang ebenfalls relevant sein, beispielsweise in Bezug auf die Meldung, die der für die Verarbeitung Verantwortliche, der das Modell entwickelt, gegenüber dem für die Verarbeitung Verantwortlichen, der das einsetzt, vornehmen sollte.

128. Was drittens die möglichen Auswirkungen der Rechtswidrigkeit der ursprünglichen Verarbeitung auf die nachfolgende Verarbeitung durch einen anderen für die Verarbeitung Verantwortlichen anbelangt, so sollte eine solche Bewertung von den internationalen Kontrollinstanzen von Fall zu Fall vorgenommen werden.

129. **Die ORKB sollten berücksichtigen, ob der für die Verarbeitung Verantwortliche, der das Modell einsetzt, im Rahmen seiner Rechenschaftspflicht[89] zum Nachweis der Einhaltung von Artikel 5 Absatz 1 Buchstabe a und Artikel 6 DSGVO eine angemessene Bewertung durchgeführt hat, um sich zu vergewissern, dass das KI-Modell nicht durch eine unrechtmäßige Verarbeitung personenbezogener Daten entwickelt wurde.** Bei einer solchen Bewertung durch die für die Verarbeitung Verantwortlichen sollte berücksichtigt werden, ob der für die Verarbeitung Verantwortliche einige nicht erschöpfende Kriterien bewertet hat, wie z. B. die Quelle der Daten und ob das KI-Modell das Ergebnis eines Verstoßes gegen die DSGVO ist, insbesondere wenn dies von einer für die Verarbeitung Verantwortlichen oder einem Gericht festgestellt wurde, so dass der für die Verarbeitung Verantwortliche, der das Modell einsetzt, nicht ignorieren konnte, dass die ursprüngliche Verarbeitung unrechtmäßig war.

130. Der für die Verarbeitung Verantwortliche sollte beispielsweise berücksichtigen, ob die Daten aus einer Verletzung des Schutzes personenbezogener Daten stammen oder ob die Verarbeitung Gegenstand einer Feststellung eines Verstoßes durch eine ORKB oder ein Gericht war. **Der Grad der Bewertung durch den für die Verarbeitung Verantwortlichen und der von den ORKB erwartete Detaillierungsgrad können in Abhängigkeit von verschiedenen Faktoren variieren, einschließlich der Art und des Ausmaßes der Risiken, die durch die Verarbeitung im KI-Modell während seiner Einführung in Bezug auf die betroffenen Personen, deren Daten zur Entwicklung des Modells verwendet wurden, entstehen.**

131. Der EDSB stellt fest, dass das KI-Gesetz von Anbietern von KI-Systemen mit hohem Risiko verlangt, eine EU-Konformitätserklärung[90] zu erstellen, und dass diese Erklärung eine Aussage darüber enthält, dass das betreffende KI-System mit den EU-Datenschutzgesetzen übereinstimmt[91]. Der EDSB stellt fest, dass eine solche Selbsterklärung keine abschließende Feststellung der Einhaltung der Datenschutzgrundverordnung darstellt. Sie kann jedoch von den Aufsichtsbehörden bei der Untersuchung eines bestimmten KI-Modells berücksichtigt werden.

132. Dieselben Erwägungen, die unter Punkt 123 angestellt wurden, sind auch in diesem Fall relevant. Wenn die ORKB prüfen, ob und wie der für die Verarbeitung Verantwortliche die Angemessenheit des berechtigten Interesses als Rechtsgrundlage für die von ihm durchgeführte Verarbeitung bewertet hat, sollte die Rechtswidrigkeit der ursprünglichen Verarbeitung als Teil der Bewertung des berechtigten Interesses berücksichtigt werden, indem beispielsweise die potenziellen Risiken bewertet werden, die sich für die betroffenen Personen ergeben können, deren personenbezogene Daten zur Entwicklung des Modells unrechtmäßig verarbeitet wurden. Im Rahmen der Abwägungsprüfung sind verschiedene Aspekte technischer Art (z. B. das Vorhandensein von Filtern oder Zugangsbeschränkungen während Entwicklung des Modells, die der spätere für die Verarbeitung Verantwortliche nicht umgehen oder beeinflussen kann und die den Zugang zu oder die Offenlegung von personenbezogenen Daten verhindern könnten) oder rechtlicher Art (z. B. Art und Schwere der Rechtswidrigkeit der ursprünglichen Verarbeitung) angemessen zu berücksichtigen.

3.4.3 Szenario 3. Ein für die Verarbeitung Verantwortlicher verarbeitet unrechtmäßig personenbezogene Daten, um das Modell zu entwickeln, und sorgt dann dafür, dass das Modell anonymisiert wird, bevor derselbe oder ein anderer für die Verarbeitung Verantwortlicher ( ) eine weitere Verarbeitung personenbezogener Daten im Zusammenhang mit dem Einsatz einleitet

133. Dieses Szenario bezieht sich auf Frage 4 Ziffer ii des Antrags und bezieht sich auf einen Fall, in dem ein für die Verarbeitung Verantwortlicher unrechtmäßig personenbezogene Daten verarbeitet, um das KI-Modell zu entwickeln, dies aber in einer Weise tut, die sicherstellt, dass personenbezogene Daten anonymisiert werden, bevor derselbe oder ein anderer für die Verarbeitung Verantwortlicher eine weitere Verarbeitung personenbezogener Daten im Zusammenhang mit dem Einsatz einleitet. Erstens erinnert der EDSB daran, dass die ORKB befugt sind und die Befugnis haben, in Bezug auf die Verarbeitung im Zusammenhang mit der Anonymisierung des Modells sowie auf die Verarbeitung während der Entwicklungsphase einzugreifen. So können die ORKB je nach den spezifischen

[89] Artikel 5 Absatz 2 DS-GVO und Artikel 24 DS-GVO.
[90] Artikel 16 Buchstabe g und Artikel 47 AI-Gesetz.
[91] Anhang V, Punkt 5 AI-Gesetz.

unter den Umständen des Falles Berichtigungsmaßnahmen für diese Erstverarbeitung anordnen (wie unter den Ziffern 113, 114 und 115 erläutert)

134. Wenn nachgewiesen werden kann, dass der spätere Betrieb des KI-Modells keine Verarbeitung personenbezogener Daten mit sich bringt, ist der EDSB der Ansicht, dass die DSGVO nicht anwendbar ist[92]. Die Rechtswidrigkeit ursprünglichen Verarbeitung sollte keine Auswirkungen auf den späteren Betrieb des Modells haben. Der EDSB betont jedoch, dass die bloße Behauptung der Anonymität des Modells nicht ausreicht, um es von der Anwendung der Datenschutz-Grundverordnung auszunehmen, und weist darauf hin, dass die ORKB dies im Einzelfall unter Berücksichtigung der vom EDSB zur Beantwortung von Frage 1 des Ersuchens angestellten Überlegungen bewerten sollten.

135. **Wenn die für die Verarbeitung Verantwortlichen anschließend personenbezogene Daten verarbeiten, die während der Errichtungsphase erhoben wurden, nachdem das Modell anonymisiert wurde, würde die DSGVO in Bezug auf diese Verarbeitungstätigkeiten gelten. In diesen Fällen sollte die Rechtmäßigkeit der in der Errichtungsphase durchgeführten Verarbeitung nicht durch die Rechtswidrigkeit der ursprünglichen Verarbeitung beeinträchtigt werden.**

4 Schlussbemerkungen

136. Diese Stellungnahme ist an alle ORKB gerichtet und wird gemäß Artikel 64 Absatz 5 Buchstabe b) DSGVO veröffentlicht.

Für den Europäischen Datenschutzausschuss Der

Vorsitzende

Anu Talus

[92] Erwägungsgrund 26 GDPR.