Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 27.02.2024

Datenschutzrechtliche Grundlagen beim Einsatz von Künstlicher Intelligenz (KI) im Bereich der Sicherheitsbehörden des Bundes

Handreichung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Version: 1.0

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Inhalt

1. Einleitung 3

1.1. Gegenstand und Zweck des Dokuments 3

1.2. Verordnung über künstliche Intelligenz 3

1.3. Begriff von KI 5

2. Differenzierung einzelner Verarbeitungsschritte 5

3. Rechtsgrundlagen 7

4. Kriterien zur Beurteilung der Eingriffsintensität 8

5. Verteilung von Verantwortlichkeiten 11

6. Rechenschaftspflicht 12

6.1. Grundlegendes Pflichtenprogramm (Auswahl) 12

6.2. Dokumentation und Protokollierung 14

7. Wahrung der Betroffenenrechte 16

1. Einleitung

KI ist nicht nur Gegenstand von Forschungsprojekten, sondern mittlerweile auch Teil der behördlichen Praxis im Sicherheitsbereich. Mit dem KI-Campus der Polizei z. B. fördert die Bundesregierung den Wissenstransfer zwischen den Polizeibehörden in Deutschland zur Entwicklung und zum Einsatz von KI-Anwendungen.[1] Im Fokus der Bemühungen stehen dabei insbesondere die Rechtmäßigkeit und die ethische Vertretbarkeit bestimmter KI-Lösungen.[2]

Für die Nachrichtendienste und Polizeibehörden dient die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) unter anderem als Drehscheibe für Forschung und Wissensaufbau bei KI für Anwendungen bei den Sicherheitsbehörden. Dort sind diverse Aktivitäten zu KI-Entwicklungssprojekten gebündelt, was eine zunehmende Priorität dieses Handlungsfelds erkennbar macht.

Gerade die datenschutzrechtliche Bewertung von KI-basierten Datenverarbeitungen erfordert eine sorgfältige Prüfung unter Berücksichtigung aller Umstände des Einzelfalls.

1.1. Gegenstand und Zweck des Dokuments

Die nachfolgende Handreichung dient der Unterstützung der Verantwortlichen in den Sicherheitsbehörden. Sie erhebt keinen Anspruch auf Vollständigkeit und ist als eine erste Orientierungshilfe bei grundlegenden Fragen und Fallkonstellationen im Zusammenhang mit der Entwicklung und dem Einsatz von KI-Anwendungen konzipiert.

Die Handreichung enthält sich jeglicher Aussage darüber, ob und wann der Einsatz oder das Training von KI durch die Sicherheitsbehörden sinnvoll oder angezeigt ist. Gegenstand der Handreichung sind vielmehr ausgewählte datenschutzrechtliche Aspekte, die bei einer geplanten Verarbeitung personenbezogener Daten zu beachten sind.

1.2. Verordnung über künstliche Intelligenz

[1] https://www.ki-strategie-deutschland.de/tile-7-4-ki-campus-der-polizei.html.
[2] Vgl. z. B. auch ZITiS zum Forschungsprojekt KISTRA, abrufbar unter: https://www.zitis.bund.de/DE/WerWirSind/werwirsind_node.html#forschungsprojekte.

Einen wichtigen Bestandteil des künftigen Rechtsrahmens, innerhalb dessen die Sicherheitsbehörden KI-Systeme nutzen dürfen, stellt die am 21. Mai 2024 verabschiedete Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Verordnung über künstliche Intelligenz) dar.[3] Für den Bereich der nachrichtendienstlichen Arbeit findet dieses als EU-Rechtsakt (grundsätzlich) keine Anwendung, so dass dessen Rechtsgedanken allenfalls im Einzelfall analog angewendet werden können.

Nach dieser Verordnung könnten bestimmte KI-Systeme nicht oder nur eingeschränkt zu Zwecken der Strafverfolgung[4] eingesetzt werden. Eine Reihe von KI-Systemen, die zu Strafverfolgungszwecken eingesetzt werden, wird nach der Verordnung über künstliche Intelligenz als hochriskant eingestuft.[5] Für Hochrisiko-KI-Systeme enthält die Verordnung über künstliche Intelligenz besondere Anforderungen. Diese betreffen beispielsweise folgende Bereiche:

- Risikomanagementsystem (Art. 9),
- Daten und Daten-Governance (Art. 10),
- Technische Dokumentation (Art. 11),
- Aufzeichnungspflichten (Art. 12).

Aus der Tatsache, dass ein KI-System die Vorgaben der Verordnung über künstliche Intelligenz erfüllen muss, kann nicht die Schlussfolgerung gezogen werden, dass der geplante KI-Einsatz datenschutzrechtlich zulässig ist. Vielmehr muss der Einsatz auf einer unionsrechtlichen oder nationalgesetzlichen Regelung beruhen. Die Verordnung über künstliche Intelligenz selbst legt außerdem bestimmte verbotene Praktiken im Bereich künstliche Intelligenz fest, welche grundsätzlich unzulässig sind (Art. 5). Dies gilt insbesondere für die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, außer wenn und insoweit dies im Hinblick auf eines der im Gesetz festgelegten Ziele unbedingt erforderlich ist. Darüber hinaus sind auch die einschlägigen datenschutzrechtlichen Vorgaben zu beachten.

---

[3] Die nachfolgenden Ausführungen zur Verordnung über künstliche Intelligenz basieren auf der Fassung vom 14.5.2024, abrufbar unter: https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/de/pdf.
[4] Der Zweck Strafverfolgung in diesem Sinne (engl. „law enforcement“) umfasst hier auch die Gefahrenabwehr.
[5] Art. 6 und Anhang III Nr. 6 Verordnung über künstliche Intelligenz.

1.3. Begriff von KI

Für die Zwecke des vorliegenden Dokuments wird kein bestimmter Begriff von KI zugrunde gelegt. Das geltende Datenschutzrecht bezieht sich auf die Verarbeitung von personenbezogenen Daten und ist insofern technologieneutral formuliert. Im Vordergrund steht hier die Reichweite der datenverarbeitenden Befugnisse der Sicherheitsbehörden. Verarbeitungen erfolgen jedenfalls dann mithilfe von KI, wenn sie der Verordnung über künstliche Intelligenz unterfallen.[6] Auch andere automatisierte Anwendungen zur Datenanalyse oder -auswertung können als KI-Systeme einzuordnen sein.

2. Differenzierung einzelner Verarbeitungsschritte

Sollen mittels KI personenbezogene Daten verarbeitet werden, ist das Datenschutzrecht anwendbar und in jeder Lebenszyklusphase einer KI-Anwendung – von dem Design des KI-Systems über das Training bis hin zum Einsatz – zu beachten. Beispielsweise kann zwischen vier[7] Phasen unterschieden werden. Die Lebenszyklusphasen können je nach Anwendung unterschiedlich ausgestaltet sein.

Für die datenschutzrechtliche Bewertung ist dabei die Unterscheidung zwischen einzelnen Schritten der Datenverarbeitung – ggfls. auch innerhalb einer Lebenszyklusphase – elementar wichtig.
So kann beispielsweise das Training von KI mittels personenbezogener Daten einem anderen Datenschutzrechtsregime unterliegen als der Einsatz von KI zum Zweck der Aufgabenerfüllung.[8]

Beispiel: Testet eine Polizeibehörde eine KI-Anwendung im Hinblick auf ihre Fehlerfreiheit, richtet sich die damit verbundene Verarbeitung personenbezogener Daten nach der DS-GVO.[9] Für den Einsatz dieser KI-Anwendung – im Produktivbetrieb – zum Zweck der Strafverfolgung oder der Gefahrenabwehr ist

[6] Gemäß Art. 3 Nr. 1 der Verordnung über künstliche Intelligenz ist ein KI-System „ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“.
[7] OECD, Abbildung 1.5., abrufbar unter: https://www.oecd-ilibrary.org/sites/64ae49f7-de/index.html?itemId=/content/component/64ae49f7-de.
[8] Vgl. Kelber/Bortnikov, NJW 2023, 2000 Rn. 24 ff.
[9] Vgl. ausführlich Kelber/Bortnikov, NJW 2023, 2000 Rn. 24 ff.

hingegen das jeweils für die betreffende Behörde anwendbare Fachrecht maßgeblich.

Auch die datenschutzrechtliche Verantwortlichkeit kann bei unterschiedlichen Verarbeitungsschritten divergieren.[10] Möglich ist auch, dass einzelne Verarbeitungsschritte im Einzelfall datenschutzrechtlich unterschiedlich zu bewerten sind.

Beispiel: Wird eine KI-Anwendung mithilfe einer Vielzahl von – auch sensiblen[11] – personenbezogenen Daten trainiert, ist die Eingriffsintensität der damit verbundenen Datenverarbeitung höher als beim nachfolgenden Testen der KI-Anwendung, wenn diese Tests lediglich mit wenigen Testdaten durchgeführt werden.[12] Vorbehaltlich der weiteren Rahmenbedingungen wären in diesem Fall an die Rechtsgrundlage für das Testen der KI-Anwendung geringere Anforderungen zu stellen als an das Training.

Beispiel: Eine KI-Anwendung, die automatisiert (Audio-)Material übersetzt, ist weniger eingriffsintensiv als eine, die in einem zweiten Schritt den Inhalt auf mögliche „Code"-Worte durchsucht, die Aufschluss auf verfassungsfeindliche Inhalte oder sogar über mögliche strafbare Inhalte analysiert und den Sprecher daraufhin als (besonders) beobachtungsbedürftig einstuft.

Beispiel: Informationsbezogene Maßnahmen bauen in der Regel auf einander auf, sodass zwischen Erhebung, Speicherung und Verwendung von Daten zu unterscheiden ist.[13] So kann z. B. die anlasslose *Erfassung* des Innenraums und des Kennzeichens eines Fahrzeugs zwecks Feststellung eines Handy-Verstoßes nicht auf die Vorschriften der Strafprozessordnung (in Verbindung mit § 46 Abs. 1 Ordnungswidrigkeitengesetz) gestützt werden, da zum Zeitpunkt dieser Datenerhebung noch kein Anfangsverdacht vorliegt und damit erst festgestellt werden soll.[14] Werden Bilder in einem Trefferfall gespeichert, kommen für

[10] Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 4 Nr. 7 DS-GVO Rn. 22.
[11] Vgl. insbesondere „besondere Kategorien personenbezogener Daten" im Sinne von § 46 Nr. 14 BDSG, Art. 9 Abs. 1 DS-GVO.
[12] Zur Auswirkungen der Eingriffsintensität auf die Wahl einer Rechtsgrundlage vgl. sogleich unter 3.
[13] BVerfG, Beschluss vom 27.5.2020 – 1 BvR 1873/13, 1 BvR 2618/13, NJW 2020, 2699, Rn. 93.
[14] AG Trier, Urteil vom 02.03.2023 – 2 OWi 8113 Js 1906/23 (2), juris, Rn. 42 ff.

diese *Speicherung* hingegen die Vorschriften der Strafprozessordnung in Frage.[15]

3. Rechtsgrundlagen

Jede Verarbeitung personenbezogener Daten muss sich auf eine Rechtsgrundlage stützen. Für die Wahl der richtigen Rechtsgrundlage ist der mit der konkreten Datenverarbeitung verfolgte Zweck maßgeblich. Die in Frage kommenden Normen sind gegebenenfalls verfassungskonform auszulegen und anzuwenden.[16] Eine verfassungskonforme Auslegung ist umso eher geboten, je offener die fragliche Rechtsgrundlage formuliert ist.[17] Denn die verfassungsrechtlichen Anforderungen an die Normbestimmtheit und Normklarheit steigen mit zunehmender Eingriffsintensität.[18] Mit den Regelungen, mit denen der Gesetzgeber durch Art und Umfang der Daten und durch Begrenzung der Auswertungsmethode die Eingriffsintensität gesteuert hat, korrespondieren die verfassungsrechtlichen Anforderungen an die Eingriffsvoraussetzungen.[19] Grundsätzlich können generalklauselartig formulierte Normen nur Datenverarbeitungen mit geringer Eingriffsintensität rechtfertigen,[20] wie z. B. KI-gestützte Übersetzungen. Im Einzelfall kann die verfassungskonforme Auslegung deshalb dazu führen, dass in Frage kommende Rechtsgrundlagen für die konkrete Datenverarbeitung nicht hinreichend spezifisch sind und die fragliche Datenverarbeitung nicht rechtfertigen können.

Beispiel: Die anlasslose Verkehrsüberwachung mittels der MonoCam kann nicht auf die Datenerhebungsgeneralklausel gemäß § 29 Abs. 2 S. 1 POG RLP[21] gestützt werden.[22] Diese Norm setzt lediglich voraus, dass die Erhebung zur Erfüllung einer polizeilichen Aufgabe erforderlich ist. Aufgrund der geringen Voraussetzungen, die diese Norm an eine Datenerhebung stellt, genügt sie – trotz der im vorliegen-

[15] AG Trier, Urteil vom 02.03.2023 – 2 OWi 8113 Js 1906/23 (2), juris, Rn. 70 ff.
[16] VGH Mannheim, Urteil vom 22. 7. 2004 - 1 S 2801/03, NJW 2005, 88 (89).
[17] Vgl. VGH Mannheim, Urteil vom 22. 7. 2004 - 1 S 2801/03, NJW 2005, 88 (89).
[18] Vgl. z. B. BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196, 1205, Rn. 71.
[19] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196, 1205, Rn. 103.
[20] Vgl. nur Gola/Heckmann/Starnecker, 3. Aufl. 2022, BDSG § 3 Rn. 13 (in Bezug auf § 3 BDSG); AG Trier, Urt. v. 2.3.2023 – 2 OWi 8113 Js 1906/23 (2), juris, Rn. 55 (in Bezug auf § 29 POG RLP).
[21] Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz.
[22] AG Trier, Urteil vom 02.03.2023 – 2 OWi 8113 Js 1906/23 (2), juris, Rn. 51 ff.

den Fall moderaten Eingriffsintensität – nicht den Bestimmtheitsanforderungen.[23] § 29 POG kann nur Datenerhebungen mit geringer Eingriffsintensität rechtfertigen.[24] „Vielmehr wäre eine Norm erforderlich, die neben der hinreichend bestimmten Festlegung des Anlasses der Kontrollen, des Verwendungszwecks der erfassten Daten sowie der Modalitäten und des Umfangs der Datenerhebung, auch Regelungen zur Speicherung und Verwendung, möglicherweise auch zur Sicherung der erfassten Daten gegen unbefugte Nutzung vorsieht."[25]

Beispiel: Bei verfassungskonformer Auslegung des § 100h Abs. 1 Nr. 2 StPO kann die automatische Kennzeichenerfassung im Aufzeichnungsmodus nicht hierauf gestützt werden.[26] In Anbetracht der hohen Grundrechtssensibilität der Maßnahme bedarf es vielmehr spezieller auf die automatische Kennzeichenerfassung zugeschnittener Ermächtigungsgrundlagen (mit verschärften Voraussetzungen und höherer Regelungsdichte).[27] Der Vorschrift fehlt es an Regelungen zur Datenspeicherung, -löschung und -sicherheit sowie den Zugriffsmöglichkeiten, einem effektiven Richtervorbehalt, und an der Gewährleistung effektiven individuellen Rechtsschutzes und hinreichender Transparenz.[28]

4. Kriterien zur Beurteilung der Eingriffsintensität

Werden – z. B. mithilfe einer KI-Anwendung – personenbezogene Daten verarbeitet, geht damit ein Eingriff in die Grundrechte der betroffenen Personen, insbesondere in das Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG oder in das Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG, einher. Bei der einfachgesetzlichen Rechtsanwendung kann die Eingriffsintensität einer datenverarbeitenden Tätigkeit insbesondere bei der Wahl und bei der verfassungskonformen Anwendung von Rechtsgrundlagen relevant sein.[29] Durch die Ergreifung angemessener technischer und organisatorischer Maßnahmen kann das Eingriffsgewicht gemindert werden.

Im Folgenden werden Kriterien dargestellt, die sich auf die Eingriffsintensität einer datenverarbeitenden Tätigkeit auswirken:

[23] AG Trier, Urteil vom 02.03.2023 – 2 OWi 8113 Js 1906/23 (2), juris, Rn. 54.
[24] AG Trier, Urteil vom 02.03.2023 – 2 OWi 8113 Js 1906/23 (2), juris, Rn. 55.
[25] AG Trier, Urteil vom 02.03.2023 – 2 OWi 8113 Js 1906/23 (2), juris, Rn. 56.
[26] LG Frankfurt (Oder), Beschl. v. 22.07.2022 – 22 Os 40/19, BeckRS 2022, 19483 Rn. 69.
[27] LG Frankfurt (Oder), Beschl. v. 22.07.2022 – 22 Os 40/19, BeckRS 2022, 19483 Rn. 69.
[28] LG Frankfurt (Oder), Beschl. v. 22.07.2022 – 22 Os 40/19, BeckRS 2022, 19483 Rn. 70.
[29] Vgl. oben unter 3.

- **Art und Umfang der Daten**

Das Eingriffsgewicht einer datenverarbeitenden Tätigkeit wird zunächst durch die Art und den Umfang der verarbeiteten Daten bestimmt. Je größer die Menge der verarbeiteten Daten ist und je unterschiedlicher diese Daten sind, desto höher ist das Eingriffsgewicht.[30] Auch die Herkunft der Daten kann Einfluss auf das Eingriffsgewicht haben. Dabei fördert eine Verknüpfung der Analyseeinrichtung mit dem Internet praktisch die Verarbeitung besonders großer Datenmengen und wirkt deshalb eingriffsverstärkend.[31]

Mögliche Maßnahmen zur Reduktion des Eingriffsgewichts:

- Begrenzung des Umfangs der verarbeiteten personenbezogenen Daten, auch bereits auf Ebene der Datenerhebung, etwa durch Verbindung bestimmter Kameraerfassungsbereiche).
- Begrenzung der Verarbeitung auf bestimmte Dateiformate wie etwa Textdateien unter Ausschluss von Bildern, Video- und Audioaufnahmen.[32]
- Ausschluss besonderer Kategorien personenbezogener Daten wie z. B. biometrischer Daten.[33]
- Begrenzung der Analyse auf Daten, die die Behörde selbst oder die eine andere Behörde desselben Rechtsträgers, jedenfalls aber eine andere inländische Behörde erhoben hat.[34]
- Ausschluss von Daten, die aus sozialen Netzwerken erhoben wurden.
- Ausschluss von Daten, die der Privatsphäre und der Intimsphäre zu zuordnen sind.

[30] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 78.
[31] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 88.
[32] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 88.
[33] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 87.
[34] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 79.

- Ausschluss der polizeilichen Verarbeitung von Daten, die ursprünglich von nachrichtendienstlichen Behörden erhoben wurden.[35]

- Ausschluss der Verarbeitung von Daten, die ursprünglich durch (besonders) schwere Grundrechtseingriffe erlangt wurden.[36]

- Begrenzung der Verarbeitung auf solche Daten, die bei der Wahrnehmung bestimmter Aufgaben angefallen sind.[37]

- Begrenzung auf aktuelle Daten oder solche, die nicht ein bestimmtes Alter überschritten haben.

- Nutzung von Stand-Alone-Rechnern (ohne eine Verknüpfung mit dem Internet).

- Händische Hinzuziehung von Dateien für jeden Analysevorgang bzw. Verzicht auf die automatisierte Einbeziehung von Dateien.[38]

- Technisch und organisatorisch gesicherte Beschränkung des Zugriffs auf eine begrenzte Zahl von Mitarbeitenden und eine besondere Qualifizierung dieser Personen.[39]

- **Methode der Datenverarbeitung**

Die Reichweite im hiesigen Kontext relevanter Datenverarbeitungsmethoden reicht von komplexen Formen des automatisierten Datenabgleichs bis hin zu selbstlernenden Systemen. Mit steigender Komplexität, Fehler- und Diskriminierungsanfälligkeit der eingesetzten Datenverarbeitungstechnologie erhöht sich die Intensität der mit ihrem Einsatz verbundenen Grundrechtseingriffe. Die Komplexität des suchenden Vergleichs kann sich z. B. durch eine höhere Zahl an Abgleichschritten und Verknüpfungen erhöhen[40]. Die Eingriffsintensität ist ferner umso höher, je breitere und tiefere Erkenntnisse über Personen dadurch erlangt

[35] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 79.
[36] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 81.
[37] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 82.
[38] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 88.
[39] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 89.
[40] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 92.

werden können.[41] Schließlich erhöht sich das Eingriffsgewicht, wenn die Datenanalyse – ohne hinreichenden Sachverhaltsbezug – darauf zielt, allein statistische Auffälligkeiten in den Datenmengen zu entdecken.[42]

Mögliche Maßnahmen zur Reduktion des Eingriffsgewichts:

- Verwendung einer Methode mit der geringsten Komplexität und der größtmöglichen Nachvollziehbarkeit.[43]

- Reduktion von Verknüpfungsmöglichkeiten durch die Begrenzung der Zahl der vorprogrammierten Abgleichschritte, die sich ohne weiteren, im Einzelfall menschlich veranlassten Anstoß vollziehen könnten.[44]

- Reduktion der Zahl abstrakter Variablen, die von der KI kombiniert, verknüpft und analysiert werden.

- Vorkehrungen zur Entdeckung und Korrektur von Fehlern; Monitoring der Entwicklung der eingesetzten Software[45], sowie Einsatz von Methoden und Techniken zur Verhinderung von Verzerrungen (Bias) und Diskriminierungen. Zu beachten ist dabei, dass Bias aus unterschiedlichen Quellen resultieren kann. Insbesondere können Verzerrungen in den Trainingsdatensätzen enthalten sein, bei der Entwicklung der Algorithmen eingeführt oder bei der Implementierung der Systeme – auch durch die Anwendenden –erzeugt werden.[46]

- Begrenzung der Datenanalyse auf Suchbegriffe, die auf einem erkennbaren Sachverhalt gründen.[47]

5. Verteilung von Verantwortlichkeiten

[41] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 90.
[42] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 93.
[43] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 91, 93.
[44] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 92.
[45] BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 90, 102, 109.
[46] Entschließung des Europäischen Parlaments vom 6.10.2021 zu dem Thema: Künstliche Intelligenz im Strafrecht und ihre Verwendung durch die Polizei und Justizbehörden in Strafsachen (2020/2016(INI)), Ziff. 8.
[47] Vgl. BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 93.

Bei der Beurteilung der Verantwortlichkeit ist strikt nach der jeweiligen Lebenszyklusphase bzw. dem jeweiligen Verarbeitungsschritt zu differenzieren.[48]

Die Einbeziehung von externen Dritten – von Herstellern und Dienstleistern – ist im Zusammenhang mit KI weit verbreitet. „AI as a Service“ (AIaaS) ist ein auf dem Vormarsch befindliches Geschäftsmodell. Für die datenschutzrechtliche Bewertung ist dabei die Verteilung von Verantwortlichkeiten zentral. „Verantwortlicher“ ist, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (§ 46 Nr. 7 BDSG). Da unterschiedliche Formen vertraglicher Beziehungen möglich sind, sind die Rollen der Beteiligten bei jeglicher Einbeziehung Dritter vorab genau festzulegen und die datenschutzrechtliche Verantwortlichkeit zu prüfen.

In den AIaaS-Konstellationen liegt grundsätzlich – vorbehaltlich der gebotenen Gesamtwürdigung im Einzelfall – eine Auftragsverarbeitung nahe, soweit der Dienstleister die personenbezogenen Daten nicht auch zu eigenen Zwecken verarbeitet. Andernfalls käme auch eine gemeinsame Verantwortung in Frage.

Beispiel: Wurde ein KI-Modell mit personenbezogenen Daten allein nach Maßgaben des Herstellers trainiert, trägt die Behörde, die die darauf basierende KI-Anwendung einsetzt, keine Verantwortung für die mit dem Training verbundene Datenverarbeitung.

6. Rechenschaftspflicht

Der Verantwortliche muss die Einhaltung der Grundsätze der Datenverarbeitung sicherstellen (6.1.) und nachweisen (6.2.) können.

6.1. Grundlegendes Pflichtenprogramm (Auswahl)

Ein Pflichtenprogramm des Verantwortlichen lässt sich nicht abschließend bestimmen. Beispielhaft genannt seien folgende Aspekte:

- Der Verantwortliche hat den Zweck der Verarbeitung unverzüglich und eindeutig im Vorfeld festzulegen, damit stets erkennbar ist, zu welchem Zweck

[48] Vgl. schon oben unter 2.

ein bestimmtes Datum verarbeitet wird.[49] Gerade bei multifunktional einsetzbaren KI-Anwendungen kommt der Zweckfestlegung eine besondere Bedeutung zu.

- Es dürfen nur personenbezogene Daten verarbeitet werden, die für das Erreichen des Verarbeitungszwecks erforderlich sind. Kommt beispielsweise eine Software in die nähere Auswahl, die mehr Daten verarbeitet als für die Erfüllung des konkreten Zwecks der verantwortlichen Dienststelle erforderlich ist, sollten entsprechende Anpassungen vorgenommen werden, bevor mit der Software personenbezogene Daten verarbeitet werden.

- Die Erforderlichkeit der Verarbeitung von Daten mit Personenbezug ist stets zu prüfen. Die Datenverarbeitung ist so wenig eingriffsintensiv wie möglich auszugestalten. Beim Testen von KI-Produkten und beim Trainieren von KI beispielsweise sind vorrangig anonymisierte, synthetisch erzeugte oder zumindest pseudonymisierte Daten heranzuziehen.[50]

- Diskriminierende Wirkungen des Einsatzes von KI sind zu verhindern.[51]

- Der Verantwortliche hat regelmäßig zu prüfen, ob die Algorithmen zweckentsprechend funktionieren.[52] Im Hinblick auf sog. Hochrisiko-KI-Systeme formuliert das Gesetz über künstliche Intelligenz Anforderungen an Genauigkeit, Robustheit und Cybersicherheit. Insbesondere müssen diese so konzipiert und entwickelt werden, dass sie ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren.[53]

---

[49] BfDI, Positionspapier zum Grundsatz der Zweckbindung in polizeilichen Informationssystemen vom 6.4.2021, S. 3.
[50] Kelber/Bortnikov, NJW 2023, 2000 Rn. 21.
[51] Vgl. EDSA, Leitlinien 4/2019 zu Artikel 25 „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“, Version 2.0 vom 20.10.2020, Rn. 69 f.; DSK, Hambacher Erklärung zur Künstlichen Intelligenz vom 3.4.2019, S. 3 f.; Art. 4a Abs. 1 Buchst. e) KI-VO.
[52] EDSA, Leitlinien 4/2019 zu Artikel 25 „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“, Version 2.0 vom 20.10.2020, S. 22.
[53] Art. 15 Abs. 1 der Verordnung über künstliche Intelligenz.

- Automatisierte Einzelentscheidungen sind – vorbehaltlich einer gesetzlichen Erlaubnis – zu vermeiden.[54] Ein qualifiziertes menschliches Eingreifen ist sicherzustellen.[55]

- Nach Möglichkeit sind Eigenentwicklungen und kontrollierbare Open-Source-Lösungen den Software-Produkten privater Akteure oder anderer Staaten vorzuziehen.[56]

Beispiel: Die Information, ob eine Person eine doppelte Staatsbürgerschaft besitzt, ist für die Verfolgung und Aufdeckung von Sozialleistungsbetrug nicht erforderlich. Der Klassifikator „doppelte Staatsbürgerschaft" führt zudem zu Diskriminierungen anhand der Nationalität.[57]

6.2. Dokumentation und Protokollierung

Die Rechenschaftspflicht des Verantwortlichen erfordert, dass der Verantwortliche – über die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten[58] hinaus – eine angemessene Dokumentation über all diejenigen Maßnahmen und Vorkehrungen in geeigneter Form vorzuhalten hat, die er zum Zweck der Einhaltung der datenschutzrechtlichen Vorgaben ergriffen oder nicht ergriffen hat.

Beispiel: Ist die verantwortliche Dienststelle der Ansicht, dass der Einsatz einer bestimmten KI-Anwendung keine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge habe und führt sie keine Datenschutz-Folgenabschätzung durch, muss die Begründung für diese Entscheidung dokumentiert werden.[59]

Je höher die Risiken der fraglichen Datenverarbeitung sind, desto höher sind dabei die Anforderungen an die Dokumentationspflicht.

---

[54] Vgl. § 54 BDSG.
[55] Vgl. EDSA, Leitlinien 4/2019 zu Artikel 25 „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen", Version 2.0 vom 20.10.2020, S. 22 (unter Bezugnahme auf Art. 22 DS-GVO).
[56] Kelber/Bortnikov, NJW 2023, 2000 Rn. 17; Kugelmann/Buchmann, GSZ 2024, 1 (6); vgl. BVerfG Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 100.
[57] Das Beispiel ist angelehnt an die sog. „Kindergeldaffäre", vgl. z. B. Dachwitz, Niederlande zahlen Millionenstrafe wegen Datendiskriminierung 29.12.2021, abrufbar unter: https://netzpolitik.org/2021/kindergeldaffaere-niederlande-zahlen-millionenstrafe-wegen-datendiskriminierung/.
[58] Vgl. § 70 BDSG.
[59] Holthausen, NZA 2023, 1489 (1491).

Denn bei jedem staatlichen Eingriff muss jederzeit überprüfbar sein, ob der Eingriff rechtmäßig war. Daher hat jede Behörde die Pflicht zur objektiven Dokumentation des wesentlichen Geschehensablaufs. Dieser Pflicht kommt vor allem bei Maßnahmen ohne Kenntnis der betroffenen Personen und im Bereich der Nachrichtendienste eine besondere Bedeutung zu, da eine Prüfung durch die betroffene Person selbst oder eine von ihr veranlasste gerichtliche Überprüfung in der Regel ausgeschlossen oder wesentlich erschwert ist. Umso wichtiger ist in diesen Fällen die Möglichkeit der datenschutzrechtlichen Kontrolle, die bei fehlender Dokumentation jedoch stark eingeschränkt ist.

Teilweise existieren **spezifische gesetzliche Dokumentationspflichten**.

Beispiel: Jede Verwendung von Hochrisiko-KI-Systemen zur nachträglichen biometrischen Fernfernidentifizierung muss gemäß Art. 26 Abs. 10 der Verordnung über künstliche Intelligenz in der einschlägigen Polizeiakte dokumentiert werden.

Außerdem sind auch beim Einsatz von KI Protokollierungspflichten zu beachten. So müssen bestimmte Systemereignisse für Zwecke der IT-Sicherheit in der IT-Infrastruktur technisch protokolliert werden. Auf der Ebene der Fachanwendung sind zudem die materiell-rechtlichen Vorgaben, insbesondere aus § 76 BDSG,[60] zu beachten.[61]
Da ein wichtiges Anwendungsfeld im Bereich der Sicherheitsbehörden darin liegt, Datenmengen mit einander zu verknüpfen bzw. unterschiedliche Datenbestände in Beziehung zu setzen und zu analysieren, kommt der Pflicht aus § 76 Abs. 1 Nr. 5 BDSG, die „Kombination“ von Daten zu protokollieren, eine große praktische Bedeutung zu.

Beispiel: Dient eine Software dem Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen und der Darstellung in Form von räumlichen und sonstigen Beziehungen zwischen Personen sowie Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen,[62] sind an die Protokollierung besondere Anforderungen zu richten. Protokollierungspflichtig sind alle Verarbeitungsschritte, die

[60] Spezifische Protokollierungspflichten finden sich z. B. in § 6 Abs. 3 BVerfSchG oder § 25c Abs. 1 BVerfSchG
[61] BfDI, Hinweise zu den datenschutzrechtlichen Anforderungen an die Protokollierung nach § 76 Bundesdatenschutzgesetz, S. 1, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Muster_Hinweise_Protokollierung.pdf;jsessionid=AE8DFF8CBFBD5E86AA631820F22C71D8.intranet232?__blob=publicationFile&v=2.
[62] Vgl. Landtag NRW, Drs. 17/16517, S. 18 (Begründung zu § 23 Abs. 6 PolG NRW).

zu der Kombination geführt haben, und das Kombinationsergebnis.[63] Für alle Zusammenführungen (Merging) und Verknüpfungen (Linking) sind mindestens der Ursprung, das Ziel, der Bearbeiter und der Zeitpunkt zu protokollieren.[64]

Auch außerhalb des Anwendungsbereiches spezifischer Protokollierungsvorschriften kann eine Protokollierung als eine technische und organisatorische Maßnahme (vgl. z. B. § 64 BDSG) unter Umständen erforderlich sein.[65]

7. Wahrung der Betroffenenrechte

Die Rechte der betroffenen Personen – z. B. auf Information, Berichtigung, Löschung oder Auskunft – müssen auch im Zusammenhang mit KI gewahrt werden. Zu beachten ist dabei, dass KI-Modelle ggfls. personenbezogene Daten enthalten können, sodass die verantwortliche Stelle in der Lage sein muss, diese z. B. zu berichtigen oder zu löschen, wenn die Daten unrichtig sind bzw. deren Verarbeitung unzulässig ist. Unter Umständen kann ein (Machine) Unlearning erforderlich sein, um die Berichtigungs- oder Löschverpflichtung erfüllen zu können. Angesichts des mit dem Unlearning verbundenen Kosten- und Arbeitsaufwands empfiehlt es sich, die im KI-Modell ggfls. gespeicherten Daten – die Erforderlichkeit der Verarbeitung personenbezogener Daten unterstellt[66] – zu anonymisieren bzw. gleich synthetisch erzeugte Daten zu verwenden. Verantwortliche Stellen müssen bei Anwendung von KI zudem sicherstellen, dass das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gewahrt bleibt. In diesem Zusammenhang ist auf die Entscheidung des EuGH vom 21. Juni 2022 hinzuweisen, in der das Gericht feststellte, dass es zur Wahrung des Rechts aus Art. 47 EU-Grundrechte-Charta wesentlich ist, dass der Grund für das Verarbeitungsergebnis der KI erkennbar ist.[67] Die betroffenen Personen müssen – so führte der EuGH weiter aus – die Funktionsweise des Systems verstehen können, um über die Einlegung von Rechtsbehelfen entscheiden zu können.[68] Auch Verarbeitungen personenbezogener Daten zum Zwecke der Wahrung der Betroffenenrechte sind möglichst grundrechtschonend durchzuführen; es gelten die allgemeinen Grundsätze.

---

[63] BfDI, Hinweise zu den datenschutzrechtlichen Anforderungen an die Protokollierung nach § 76 Bundesdatenschutzgesetz, S. 8.
[64] BfDI, Hinweise zu den datenschutzrechtlichen Anforderungen an die Protokollierung nach § 76 Bundesdatenschutzgesetz, S. 9.
[65] Zum Beispiel in Verbindung mit § 36 Abs. 1 Nr. 2 Sicherheitsüberprüfungsgesetz.
[66] Vgl. oben unter 6.1.
[67] EuGH, C-817/19, Rn. 195.
[68] EuGH, C-817/19, Rn. 210.