



THUR. LANDTAG POST
22.05.2026 13:31
15722/2026

BfDI | Postfach 1468 | 53004 Bonn

Thüringer Landtag
Ausschuss für Inneres, Kommunales und
Landesentwicklung

nur per E-Mail:
poststelle@thueringer-landtag.de

Den Mitgliedern des AfIKL

Thüringer Landtag
Z u s c h r i f t
8/558
zu Drs. 8/2478

**Prof. Dr. Louisa
Specht-Riemenschneider**
Die Bundesbeauftragte

Telefon: +49 228 997799 5000

E-Mail: bfdi@bfdi.bund.de

Aktenz.: SI2-640/001#0725
(bitte immer angeben)

Dok.: 55515/2026

Anlage:

Bonn, 22.05.2026

Zweites Gesetz zur Änderung des Polizeiaufgabengesetzes (Drucksache 8/2478)

Ihr Schreiben vom 17. März 2026

Sehr geehrte Damen und Herren Abgeordnete,

für die Gelegenheit zur Stellungnahme zum Entwurf eines zweiten Gesetzes zur Änderung des Polizeiaufgabengesetzes Thüringen (PAG-E) bedanke ich mich. Aufgrund zahlreicher aktueller Gesetzgebungsvorhaben in Bund und Ländern beschränke ich meine Ausführungen auf die vorgesehenen Vorschriften zur Automatisierten Datenanalyse in § 40a PAG-E und zum biometrischen Abgleich mit Daten aus dem Internet in § 43a PAG-E.

Zu § 40a PAG-E (Automatisierte Datenanalyse)

Alle derzeit vorliegenden Gesetzentwürfe zu diesem Thema beachten meines Erachtens nicht hinreichend die Vorgaben, die sich aus der jüngeren Verfassungsrechtsprechung ergeben.

Abzulehnen ist jede Form von „**Super-Datenbanken**“, wie sie hier durch „automatisiertes zusammenführen“ geplant oder zumindest vorausgesetzt werden.

„Der Staat darf nicht etwa alle Daten, die er rechtmäßig erhoben oder geschaffen hat, über den primären Zweck hinaus mit der Begründung vorsorgend speichern, die Daten könnten künftig noch einmal benötigt werden und der gebotene Schutz könne in die Ausgestaltung der zulässigen künftigen Nutzung verlagert werden. Unzulässig wäre es daher, unabhängig von solchen Zweckbestimmungen einen Datenvorrat zu schaffen, dessen Nutzung je nach Bedarf und politischem Ermessen der späteren Entscheidung verschiedener staatlicher Instanzen überlassen bleibt. Die Bereitstellung eines solchen seiner Zwecksetzung nach offenen Datenvorrats würde den notwendigen Zusammenhang zwischen Speicherung und Speicherungszweck aufheben und damit auch die zentrale datenschutzrechtliche Freiheitssicherung durch die Zweckbindung. Auch wäre die Tragweite für die Bürgerinnen und Bürger nicht vorhersehbar.“¹

Das Bundesverfassungsgericht hat in seiner Entscheidung zur automatisierten Datenanalyse ein **zweistufiges Vorgehen** des Gesetzgebers vorgezeichnet². Auf der ersten Stufe kann der Gesetzgeber die Eingriffsintensität der Datenanalyse steuern. In der zweiten Stufe kann er anschließend daran angepasste Eingriffsschwellen festlegen. Begrenzt er die Tiefe des mit der Analyse verbundenen Grundrechtseingriffs, kann er Analysen unter niedrigeren Schwellen zulassen. Tut er das nicht, sind automatisierte Datenanalysen auf der Gefahrenabwehrseite nur zum Schutz höchststrangiger Rechtsgüter zulässig. Daraus folgt für repressive Befugnisse, dass die Ermittlungsbehörden damit nur besonders schwere Straftaten verfolgen dürfen.

Auffällig ist, dass in allen bislang vorliegenden Vorschlägen für Rechtsgrundlagen weitgehend darauf verzichtet wird, diesen vom Gericht vorgezeichneten und aus meiner Sicht äußerst sinnvollen und differenzierten Weg zu gehen. So könnten etwa Datenanalysen auf die Daten beschränkt werden, die in den polizeilichen Systemen für Zwecke der Vorsorge gespeichert sind. Für bestimmte Fälle könnte der Gesetzgeber den Kreis der Daten stufenweise und in verhältnismäßiger Weise erweitern. Stattdessen werden pauschal sehr weitreichende Datenanalysen vorgesehen, die zu intensiven Grundrechtseingriffen führen. Auf ein gestuftes Vorgehen wird verzichtet, obwohl dies mit einer moderneren Datenverarbeitung möglich wäre.

Bundesweite Modernisierung

Statt auf einzelne und grundrechtlich fragwürdige Analysesysteme zu setzen, wäre es zielführender, die polizeiliche Datenverarbeitung **grundlegend zu modernisieren**. Analysesysteme, wie sie mit dem in diesem Entwurf vorgeschlagenen § 40a PAG-E eingeführt werden, sind dann notwendig, wenn die vorliegenden polizeilichen Daten mit geringer Qualität und unstrukturiert vorliegen. Gerade dieses Problem wird aber mit dem bundesweiten

¹ BVerfG, NVwZ 2024, 1736 (1750), Rn. 183.

² BVerfG, NJW 2023, 1196 (1202), Rn. 71.

Programm P20 angegangen. Dies bietet aufgrund der besseren Datenstruktur die Chance, stärkere Rücksicht auf die Zweckbindung der Daten zu nehmen. Dann wäre keine Vorschrift notwendig, die pauschal die Analyse einer Vielzahl von Daten erlaubt, auch zu Zeugen, Opfern und Unbeteiligten. Vielmehr könnten mit stärker begrenzten Befugnissen ebenfalls gute Ergebnisse erzielt werden, die dann nur in bestimmten Fällen gestuft erweitert werden müssten.

Umgekehrt können allerdings Befugnisse, die die datenschutzrechtliche Zweckbindung in polizeilichen Dateien weitgehend aushebeln, die polizeiliche Datenverarbeitung in einem modernisierten Datenhaus in weiten Teilen unverhältnismäßig werden lassen. Das gefährdet dann sogar solch wichtige Projekte wie das genannte Programm P20. Denn die Modernisierung der polizeilichen Datenverarbeitung und die – auch grundrechtliche – Rechtsbindung der Verwaltung müssen Hand in Hand gehen.

Im Programm P20 erfolgt durch Bund und Länder gemeinsam die Neukonzeption der polizeilichen Informationsordnung insgesamt. Zielbild ist ein Datenhaus, in dem alle Datenbestände der Polizeien von Bund und Ländern strukturiert und technisch mandantengetreunt abgelegt werden. Kern von P20 ist nicht nur eine zentralisierte Datenhaltung. Erklärtes Ziel von P20 ist ebenfalls, diesen Datenbestand von Anfang an auswertbar und analysiefähig auszurichten. In welchem Umfang und mit welchen Anbieterlösungen oder Eigenentwicklungen innerhalb von P20 Auswertungen- und Analysetools eingesetzt werden sollen, ist nach meinem aktuellen Kenntnisstand noch nicht abschließend geklärt. Der Bedarf an einer Analyse von strukturierten Daten wird nach meiner Einschätzung dabei jedoch nicht im Vordergrund stehen. Denn innerhalb des Projekts werden derzeit Suchfunktionalitäten (die P20-Suche) entwickelt, die eine Suche in internen und externen Datenquellen bündeln und rechtskonform ermöglichen kann. In dieser Konsequenz kann ein großer Bereich potentiell zu analysierender Daten bereits mit der P20-Suche abgedeckt werden ohne dass entsprechende auf dem Markt bekannte Produkte flächendeckend bezogen werden müssten. Die P20-Suche ist nach meinem Verständnis jedoch nicht dazu geeignet, unstrukturierte Daten, bzw. „Schmutzdaten“ zu durchsuchen (z. B. aus sichergestellten Asservaten). Dieser – deutlich eingrenzbarere Bereich – kann einen zusätzlichen Bedarf für auf dem Markt verfügbare Produkte begründen. Die mit P20 angestrebte Datenhaltung und die geplanten Suchfunktionalitäten verbunden mit für einzelne Bereiche klar definierten Analysefunktionen wären nachvollziehbar und deutlich grundrechtsschonender. Ich befinde mich mit der Projektgruppe P20 im BMI seither in einem andauernden Beratungsprozess.

In seiner Entscheidung vom 1. Oktober 2024 hat das Bundesverfassungsgericht klargestellt, dass bereits die vorsorgende Speicherung personenbezogener Daten ein eigenständiger Grundrechtseingriff von erheblichem Gewicht ist.³ Deshalb dürfen Daten im polizeilichen Informationsverbund für Zwecke der Vorsorge nur unter engen Bedingungen und nur befristet gespeichert werden.⁴

Danach dürfen Daten, die für die Erfüllung der primären Aufgabe in den **Vorgangsbearbeitungssystemen** gespeichert sind, nicht pauschal und vorsorgend für Zwecke der künftigen Nutzung vorgehalten werden. Es ist eine polizeiinterne Zwecktrennung vorzusehen. Diese muss differenzieren zwischen

1. primärer Aufgabenerfüllung (z. B. § 29 Absatz 1 Satz 1 BPolG)
2. Dokumentation polizeilichen Handelns (z. B. § 29 Absatz 5 Satz 1 BPolG) und
3. vorsorgender Speicherung (z. B. §§ 18, 30a BKAG).

Insbesondere die Vorgangsbearbeitungssysteme der Polizeibehörden müssen deshalb die Daten nach den oben genannten Zwecken trennen.⁵ Die Zugriffsregeln müssen dann so gestaltet werden, dass die Daten nur für ihren jeweiligen Zweck genutzt werden können.

Speichert man jedoch alle Daten pauschal in einer Analyseplattform, dann unterläuft dies die Grenzen, die verfassungsrechtlich für die vorsorgende Speicherung gelten. Einbezogen sind dann nicht nur Beschuldigte, sondern ebenso Zeuginnen und Zeugen sowie unbeteiligte Dritte. Dies schließt biometrische Daten oder besonders sensible Inhalte von Zeugenaussagen ein, etwa der Opfer von Sexualstraftaten. Zudem kann dies dann etwa Daten aus Ordnungswidrigkeitenverfahren betreffen, allgemeine Verkehrsunfallaufnahmen und alle sonstigen niedrigschwellig erhobenen polizeilichen Informationen.

Die geplante Vorschrift will meinem Verständnis nach jedoch diese Daten nicht nur für die Analyse im Einzelfall freigeben, sondern dauerhaft zusammenführen, um dann anlassbezogen schnell für Analysezwecke darauf zugreifen zu können.

Betroffener Personenkreis

Maßgebend für die Verhältnismäßigkeit der Norm im engeren Sinne ist unter anderem, wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben.⁶

³ BVerfG, NVwZ 2024, 1736 (1748 ff.), Rn. 155 ff., 181.

⁴ BVerfG, NVwZ 2024, 1736 (1750), Rn. 183.

⁵ BfDI, 28. Tätigkeitsbericht 2019, Nr. 6.7.3, Seite 55 f. (zu den in der Folge erreichten Lösungen siehe BfDI, 32. Tätigkeitsbericht 2023, Nr. 12.2, S. 152 f.).

⁶ BVerfGE 156, 11 (48 f.), Rn. 96.

Eingriffsmildernd würde wirken, wenn lediglich Daten Verwendung finden würden, die sich auf Personen beziehen, bezüglich derer die Polizei tatsächliche Anhaltspunkte besitzt, dass diese selbst in Straftaten verfangen sind oder dass sie Kontaktperson zu einer solchen Person sind.⁷

Keine wesentliche Begrenzung der in die Analyse einzubeziehenden Daten

Für die Eingriffsintensität ist hier insbesondere maßgeblich, dass offensichtlich Daten aus den Vorgangsbearbeitungssystemen pauschal in die Analyse einbezogen werden dürfen.⁸ Ausschlüsse bestimmter Daten gelten nur für bestimmte Konstellationen, vgl. § 40a Absatz 1 Satz 2, Absatz 2 Satz 2, Absatz 3 Satz 1 PAG-E. Daten aus anderen eingriffsintensiven Ermittlungsmaßnahmen, die zur Verfolgung schwerer Straftaten zulässig sind, dürfen hingegen grundsätzlich verwendet werden. Unbeschränkt ist beispielsweise die Nutzung von Verkehrsdaten, die zu einer sehr hohen Eingriffsintensität führen, wie etwa die vom Bundesverfassungsgericht als Beispiel angeführten **Funkzellendateien** zeigen.⁹

Sogar Daten aus Asservaten können einbezogen werden. Diese können ihrerseits eine Vielzahl von Daten unbeteiligter Dritter enthalten. Denkbar wäre es beispielsweise, auch beschlagnahmte **größere Datenbestände** von Unternehmen oder Anwaltskanzleien einzubeziehen.

Die Dateiformate, die in die Analyse einbezogen werden können, wie etwa Bilder oder Videos, können eingriffsverstärkend oder -mildernd wirken.¹⁰ Zu diesem Faktor ist in der Norm selbst nichts zu finden. Eine Einschränkung hinsichtlich der in Art. 9 DSGVO und § 32 Nr. 14 ThürDSG als besondere Kategorien definierte Arten von personenbezogenen Daten ist nicht ersichtlich. Praktisch bedeutsam dürften insbesondere zur eindeutigen Identifizierung geeignete biometrische Daten aus Bild- oder Videodateien sein. Dies dürfte in der Praxis in erster Linie Daten von asservierten Datenträgern betreffen. Auf entsprechenden Festplatten, Smartphones oder Kameras können sich jede erdenkliche Art von Daten befinden. Als Beispiel seien nur Aufnahmen von Sexualpartnern genannt. Die eingriffsverstärkende Wirkung drängt sich insofern meines Erachtens auf.

Der Entwurf sieht also eine Gesamtmenge an einzubeziehenden Daten vor, die zu einer sehr hohen Eingriffsintensität der Analyse führen.

Aufbewahrungsfristen und Löschungspflichten

Nicht geregelt ist, wie lange die Daten in der Analysedatenbank vorgehalten werden dürfen. Das erhöht die Eingriffstiefe nochmals. Denn die Datenmenge wird auch durch Regelungen über Aufbewahrungsfristen und Löschungspflichten bestimmt¹¹.

⁷ BVerfG, NJW 2023, 1196 (1203), Rn. 84.

⁸ Vgl. BVerfG, NJW 2023, 1196 (1209 f.), Rn. 134 ff.

⁹ BVerfG, NJW 2023, 1196 (1210), Rn. 142; siehe dazu BfDI, 30. Tätigkeitsbericht 2021, Nr. 8.2.4, Seite 90.

¹⁰ BVerfG NJW 2023, 1196 (1204), Rn. 87.

¹¹ BVerfG NJW 2023, 1196 (1203), Rn. 85.

Meines Erachtens fehlt eine Regelung, die die Speicherung des in die Analyseplattform „kopierten“ Datensatzes an das Bestehen der Speicherung des Ausgangsdatensatzes bindet und sehr kurze Speicherfristen vorsieht. Denn zum einen muss für eine Legitimierung der automatisierten Datenanalyse die Legitimität der einbezogenen Datensätze fortwährend Bestand haben. Zum anderen wäre es ansonsten möglich, die Erforderlichkeit der weiteren Speicherung in der Analyseplattform auf den Zweck der automatisierten Datenanalyse selbst zu beziehen und nicht auf den ursprünglichen Speicherzweck (vgl. den Wortlaut von § 40a Absatz 1 Satz 1 „...zur Gewinnung neuer Erkenntnisse...“). Dann könnten Daten aber ohne zeitliche Begrenzung in der Analyseplattform verbleiben, denn auch aus alten und für den ursprünglichen Zweck nicht mehr erforderlichen Daten können noch möglicherweise interessante Erkenntnisse gewonnen werden, zumindest für statistische Zwecke. Eine solche, auf potentielle Ewigkeit angelegte Speicherung ist gesetzgeberisch zu unterbinden.¹² Da die vom ursprünglichen Zweck losgelöste Speicherung einen erheblichen Grundrechtseingriff darstellt, müssten für die Speicherung zur Analyse als eigenem Zweck sehr kurze Fristen gesetzlich festgelegt sein.

b) *Mitziehung alter Speicherungen*

Für die Datenbestände der thüringischen Polizeibehörden gilt die sog. Mitziehung gemäß § 40 Absatz 6 Satz 1 PAG. Sobald eine neue Speicherung zum Datensatz einer Person hinzukommt, gilt für alle Speicherungen die Prüf- oder Löschfrist, die als letzte abläuft.

Mit einer solchen Regelung können personenbezogene Daten betroffener Personen letztlich über einen sehr langen Zeitraum – wenn nicht sogar unbegrenzt – gespeichert werden, sofern regelmäßig neue „Erkenntnisse“ über eine Person gespeichert werden. Alte Speicherungen werden dann „mitgezogen“ und nicht gelöscht. Dies stellt meines Erachtens einen erheblichen Grundrechtseingriff dar, für den es keine Rechtfertigung gibt. Die ohne Prüfung der Erforderlichkeit fortwährende Speicherung potentiell sehr alter Erkenntnisse ist unverhältnismäßig. Selbst wenn eine Negativprognose vorliegt, verliert diese mit der Zeit ihre Wirkung und Belastbarkeit.¹³ Diese „Mitziehautomatik“ halte ich angesichts der zitierten aktuellen Rechtsprechung des Bundesverfassungsgerichts – unabhängig von der Datenanalyse – für verfassungsrechtlich nicht mehr tragfähig.

Zusätzlich ist fraglich, wie sich das Hinzutreten der automatisierten Datenanalyse hier auswirkt. Eine gesetzliche Regelung ist nicht vorhanden. Denkbar wäre daher nach dem Gesetzeswortlaut, dass jede durch die automatisierte Datenanalyse neu hervorgebrachte Erkenntnis zu einer Person abgespeichert wird. Dies beträfe auch nicht vorwerfbar zurechenbare Veranlassungen, etwa die Anwesenheit in einer Funkzelle in der Erfurter Innenstadt zu zwei verschiedenen Erhebungszeitpunkten oder die bloße Mitgliedschaft in verschiede-

¹² vgl. BVerfG, NVwZ 2024, 1736 (1750), Rn. 183 ff.

¹³ BVerfG, NVwZ 2024, 1736 (1751), Rn. 189.

nen offenen Facebook-Gruppen. Durch die automatisierte Datenanalyse könnte der Datenbestand zu einer Person also – je nachdem welche Daten einbezogen und auf welche Weise diese analysiert werden – beständig vergrößert und erhalten werden. Dies verschärft die Problematik der Mitziehung meines Erachtens erheblich und steigert dementsprechend die nochmals Eingriffsintensität.

Methode der Analyse oder Auswertung

Die möglichen Suchergebnisse werden nicht durch die Regelungen in § 40a PAG-E eingeschränkt. Es finden sich keine Regelungen zur Vermeidung von Diskriminierungen. Ebenfalls finden sich keine Regelungen zur Nachvollziehbarkeit der Tatsachenfeststellungen. Eine Eingriffsmilderung ist nicht erkennbar¹⁴.

Auch die zugelassene Weiterverwendung der Analyseergebnisse wird durch die Norm nicht eingeschränkt. Insbesondere ist festzustellen, dass auch hinsichtlich unbeteiligter Personen jegliche erzielten Analyseergebnisse ohne Einschränkung weiterverarbeitet werden können. Dies ist meines Erachtens als die Eingriffsintensität erhöhend anzusehen.¹⁵

Zu § 43a PAG-E (Biometrischer Abgleich mit Daten aus dem Internet),

Der vorliegende Gesetzesentwurf des § 43a PAG-E ist aufgrund des hohen Eingriffsgewichts sowie der zu pauschalen und undifferenzierten Ausgestaltung des Abgleichs biometrischer Daten meines Erachtens mit den verfassungsrechtlichen Vorgaben nicht vereinbar. Insbesondere für die Grundrechte unbeteiligter Personen besteht ein sehr hohes Risiko. Jeder biometrische Abgleich birgt ein Fehlerkennungsrisiko in sich. Umso größer die abgegliche Datenmenge ist, desto häufiger sind Fehlerkennungen. Jede Fehlerkennung im Bereich polizeilicher Maßnahmen kann aber zu mitunter auch dauerhaften erheblichen Einschränkungen der Lebensführung sowie gesellschaftlichen und beruflichen Nachteilen führen.

Die Vorschrift grenzt den **Personenkreis** für die zum Abgleich bereitgestellten Daten nicht weiter ein. Betroffen können Beschuldigte, Zeugen oder auch bloße Passanten sein. Wird zum Beispiel eine Tatbegehung auf einem Volksfest angekündigt, könnten pauschal alle Besucher der Veranstaltung biometrisch erfasst und dem Abgleich unterzogen werden. Dieser Abgleich könnte auf der anderen Seite theoretisch mit den Daten fast aller Menschen erfolgen, da biometrische Daten (Fotos, Videos) von fast jedem Menschen potentiell im Internet verfügbar sind. Positiv hervorzuheben ist, dass durch die Formulierung „öffentlich frei zugängliche“ Daten anscheinend kommerzielle Anbieter ausgeschlossen werden sollen.

Grundlage des Datenabgleichs gemäß § 43a PAG-E sind Gesichter und Stimmen, die die Polizei „zur Erfüllung ihrer Aufgaben weiterverarbeitet oder für die sie eine Berechtigung

¹⁴ vgl. BVerfG NJW 2023, 1196 (1205), Rn. 96 f., 102.

¹⁵ vgl. BVerfG NJW 2023, 1196 (1205), Rn. 99.

zum Abruf hat“. Der Wortlaut lässt insofern den Zugriff auf alle bei den Polizeibehörden gespeicherten Gesichts- und Stimmdateien aus (irgend-) einem Vorgang zu. Dazu gehören nicht nur vereinzelte Lichtbilder oder Stimmprofile. Vielmehr können darüber hinaus etwa **umfangreiche Sammlungen von sichergestellten Videoaufnahmen** herangezogen werden, die z. B. in einem weiten Umkreis um Tatorte in Ladengeschäften oder öffentlichen Verkehrsmitteln aufgenommen wurden.¹⁶ Vor allem in der Kombination mit anderen Vorschriften zur Datenanalyse wie z. B. § 40a PAG-E ergeben sich hier weitreichende Möglichkeiten. Denn es sind potentiell auch biometrische Daten erfasst, die eine Anwendung zur automatisierten Datenanalyse zuvor aus einer Vielzahl von weiteren Datenbeständen als mögliche relevante Person vorgeschlagen hat.

Nach derzeitigem Stand der Technik ist für den Abgleich größerer Mengen biometrischer Daten die Erstellung einer zumindest temporären **Datenbank** erforderlich.¹⁷ Der Gesetzesentwurf enthält keine Regelungen dazu. Sofern entsprechende Datenbanken mittels KI erstellt werden, ist Art. 5 Absatz 1 Unterabsatz 1 Buchst. e der VO (EU) 2024/1689 (KI-VO) zu beachten. Danach ist die Verwendung von KI-Systemen verboten, die Datenbanken zur Gesichtserkennung durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern. Das Verbot umfasst auch temporäre Datenbanken.¹⁸

Durch den biometrischen Abgleich ist nicht nur der einzubeziehende Datenbestand, sondern auch die Analyseverfahren für sich betrachtet eingriffsintensiv. Umfangreiche **Bewegungs- und Verhaltensprofile** sind nicht ausgeschlossen.¹⁹ Denn die Vorschrift dient ausdrücklich *nicht nur* dazu, eine Person zu finden, nach der gezielt gefahndet wird.

Insgesamt handelt es sich daher um einen intensiven Grundrechtseingriff.²⁰

Verfahrenssicherungen

Die in § 43a Absatz 5 PAG-E vorgesehene Protokollierung umfasst nicht die abgeglichenen Daten und ermöglicht deshalb keine datenschutzrechtliche Kontrolle.

Positiv zu werten ist der vorgesehene Richtervorbehalt.

¹⁶ Vgl. dazu etwa den Bericht des Hamburgischen Datenschutzbeauftragten über die „Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg, abrufbar unter: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/Pruefbericht_Gesichtserkennungssoftware.pdf, zuletzt abgerufen am 15.5.2026.

¹⁷ Vgl. Gutachten des Wissenschaftlichen Dienstes des Bundestages vom 22.1.2026 <https://www.bundestag.de/resource/blob/1149732/EU-6-074-25-WD-5-105-25.pdf> zuletzt abgerufen am 15.5.2026.

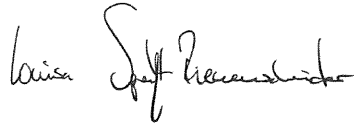
¹⁸ Vgl. Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-VO), Rn. 226 <https://ec.europa.eu/newsroom/dae/redirection/document/118661> zuletzt abgerufen am 15.5.2026.

¹⁹ Vgl. BVerfG, NJW 2023, 1196 (1202 f.), Rn. 77.

²⁰ BVerfG, NJW 2023, 1196 (1202 f.), Rn. 77.

§ 43a Abs. 4 PAG-E bezieht sich nur auf die unverzügliche Löschung von Daten ohne konkreten Ermittlungsgrundsatz. Überwiegende schutzwürdige Interessen der betroffenen Person im Einzelfall werden nicht mehr berücksichtigt. Das steht nicht im Verhältnis zur Eingriffsintensität der Maßnahme.

Mit freundlichen Grüßen



Prof. Dr. Louisa Specht-Riemenschneider