Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Stellungnahme der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin

Eine umfassende Stellungnahme der BlnBDI war vor dem Hintergrund der kurzfristigen Übersendung des Änderungsantrages nicht möglich. Die BlnBDI nimmt daher nur zu ausgewählten Punkten des Änderungsantrages Stellung:

I. § 28a ASOG – Nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

Der durch den Änderungsantrag der Fraktionen modifizierte § 28a ASOG soll u.a. den Anwendungsbereich auf Kontakt- und Begleitpersonen ausweiten.

Der Änderungsantrag erweitert den Satzteil vor Nr. 1 in Abs. 1 Satz 1 des § 28a ASOG. Die Polizei soll biometrische Daten zu Gesichtern und Stimmen nicht nur der in den Nr. 1 bis 3 genannten Personen, sondern auch deren Kontakt- und Begleitpersonen mittels automatisierter Anwendungen zum Zweck der Identifizierung und der Ermittlung des Aufenthaltsortes biometrisch mit öffentlich zugänglichen Daten aus dem Internet abgleichen. Zudem werde die Zweckbestimmung präzisiert: Der Abgleich dürfe nur dazu dienen, eine Person zu identifizieren und ihren Aufenthaltsort zu ermitteln.

Die ausdrückliche Einbeziehung von Kontakt- und Begleitpersonen erweitert den Personenkreis der Betroffenen erheblich. Der biometrische Abgleich mit öffentlich zugänglichen Internetdaten stellt bereits für gefahrenverantwortliche Personen einen intensiven Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar. Durch die Erweiterung auf Kontakt- und Begleitpersonen wird die bereits sehr große Streubreite der Maßnahme weiter erhöht. Bei diesen Personen handelt es sich nicht zwingend um Verdächtige oder Gefahrverantwortliche. Auch die neue Definition in § 18 Abs. 2 Nr. 1 Buchst. b ASOG eröffnet einen erheblichen Beurteilungsspielraum und birgt das Risiko, dass Personen einbezogen werden, die tatsächlich in keiner Weise an der

Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI)
Alt-Moabit 59-61, 10555 Berlin
Eingang: Alt-Moabit 60

Telefon: 030 13889-0
Telefax: 030 215 50 50
Sprechzeiten: Mo., Di., Fr. 10–12 Uhr,
Mi., Do. 13–15 Uhr und nach Vereinbarung

E-Mail: mailbox@datenschutz-berlin.de
Website: www.datenschutz-berlin.de

Straftatenbegehung beteiligt sind. Im Kontext der biometrischen Fernidentifizierung, die bereits aufgrund der Nutzung künstlicher Intelligenz und der Vielzahl durchsuchter Internetquellen eine hohe Streubreite aufweist, führt dies zu einer Potenzierung der Grundrechtsbeeinträchtigungen unbeteiligter Personen.

Zwar sieht § 28a Abs. 1 Satz 2 ASOG eine Subsidiaritätsklausel vor, wonach die Maßnahme nur zulässig ist, wenn die Abwehr der Gefahr oder die Verhütung der Straftat auf andere Weise aussichtslos oder wesentlich erschwert wäre. Bei Kontakt- und Begleitpersonen ist die Verbindung zur Gefahr oder die Nähe zur Straftat jedoch regelmäßig bedeutend weniger eng als bei der gefahrverantwortlichen Person selbst. Die Einbeziehung von Kontakt- und Begleitpersonen erscheint damit nicht verhältnismäßig.

In meiner bisherigen Stellungnahme vom 29. September 2025 habe ich bereits darauf hingewiesen, dass vor dem Hintergrund der sehr großen Streubreite der Maßnahme und der Eingriffe in die Grundrechte vieler unbeteiligter Personen die Eingriffsschwellen erhöht werden müssen. Ich hatte u.a. empfohlen, die Subsidiaritätsklausel zu verschärfen. Die nunmehr vorgesehene Erweiterung auf Kontakt- und Begleitpersonen verstärken diese Bedenken erheblich.

Ich empfehle, den Anwendungsbereich des § 28a ASOG nicht auf Kontakt- und Begleitpersonen zu erstrecken. Die Maßnahme sollte auf die polizeirechtlich verantwortlichen Personen beschränkt bleiben. Der Satzteil „und deren Kontakt- und Begleitpersonen“ in § 28a Abs. 1 Satz 1 ASOG sollte daher gestrichen werden.

II. § 42d ASOG – Training und Testung von KI-Systemen

Die Regelungen des Änderungsantrags in § 42d bleiben nach kursorischer Prüfung unklar und führen nicht dazu, die Bedenken gegen diese Vorschrift insbesondere im Hinblick auf die Anforderungen der hypothetischen Datenneuerhebung auszuräumen. Ich halte die Vorschrift nach wie vor nicht für verfassungskonform.

II. § 47a ASOG – Automatisierte Anwendung zur Analyse vorhandener Daten

Mit dem vorliegenden Änderungsantrag wird die Regelung zur automatisierten Datenanalyse in § 47a ASOG grundlegend überarbeitet. Die wesentliche Änderung besteht da-

rin, dass der ursprüngliche Entwurf, der den Einsatz selbstlernender Systeme noch ausdrücklich ausschloss, nun für derartige Systeme geöffnet wird. Zugleich werden Schutzmechanismen gegen diskriminierende Algorithmen eingeführt.

a) Zweckbestimmung für die Zusammenführung, Aufbereitung und Verknüpfung von Daten

In § 47a Abs. 1 Satz 1 ASOG sollen nach dem Wort „Daten“ die Wörter „ausschließlich zur Vorbereitung der automatisierten Datenanalyse“ eingefügt werden. Diese Änderung bezweckt nach der Begründung die Klarstellung, dass die Zusammenführung, Verknüpfung und Aufbereitung der Daten ausschließlich der Vorbereitung der automatisierten Datenanalyse dienen. Für eine Auswertung dieser Daten zu einem anderen Zweck gebe es keine Rechtsgrundlage (vgl. S. 42 der Begründung des Entwurfes).

Diese Klarstellung ist grundsätzlich zu begrüßen, da sie einer zweckwidrigen Verwendung der zusammengeführten Daten entgegenwirkt. Allerdings greift die Änderung das in meiner Stellungnahme vom 29. September 2025 aufgeworfene grundsätzliche Problem nicht auf. Ich hatte darauf hingewiesen, dass bereits die Zusammenführung, Verknüpfung und Aufbereitung eine zweckändernde Verarbeitung darstellen, die unter den Vorbehalt von Eingriffsschwellen zu stellen ist (vgl. S. 25 meiner Stellungnahme vom 29. September 2025). Die nunmehr eingefügte Klarstellung ändert nichts daran, dass § 47a Abs. 1 Satz 1 ASOG nach wie vor die voraussetzungslose Zusammenführung gespeicherter personenbezogener Daten erlaubt. Erst wenn in einem weiteren Schritt nach § 47a Abs. 1 Satz 2 ASOG die zusammengeführten Daten im Rahmen der automatisierten Datenanalyse verarbeitet werden, müssen nach dem Entwurf die Voraussetzungen der Eingriffsschwellen gegeben sein. Dies entspricht auch nicht den diesbezüglichen Bestimmungen in Hessen und Hamburg, an denen sich der ursprüngliche Entwurf ausweislich der Begründung orientieren soll. Die Verweisung auf § 42a Abs. 1 bis 4, § 42b und § 42c Abs. 1 in § 47a Abs. 2 Satz 6 ASOG führt zwar zur Anwendung der Regelungen über zweckwahrende und zweckändernde Datenverarbeitung, gilt aber nicht bereits für die zweckändernde Zusammenführung nach § 47a Absatz 1 Satz 1 ASOG. Dies ist mit den verfassungsrechtlichen Vorgaben weiterhin nicht vereinbar.

Ich empfehle daher weiterhin, auch für die Zusammenführung, Verknüpfung und Aufbereitung in § 47a Abs. 1 Satz 1 ASOG eine Eingriffsschwelle vorzusehen, wie dies in den Vergleichsregelungen in Hessen und Hamburg der Fall ist.

b) Erweiterung der Eingriffsschwellen

In § 47a Abs. 1 Satz 2 Nr. 2 ASOG wird die Voraussetzung der konkretisierten Gefahr der Begehung einer Straftat nach § 100a Absatz 2 StPO um die Alternative terroristische Straftat ergänzt. Allerdings wurde meine Kritik an der Verweisungstechnik nicht aufgegriffen. In meiner Stellungnahme vom 29. September 2025 hatte ich bemängelt, dass der Entwurf in eine derzeit defekte Norm des § 100a Absatz 2 StPO verweist, ohne die im Einzelfall betroffenen Schutzgüter zu benennen (BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 180/23, Trojaner II). Der Landesgesetzgeber sollte hier einen eigenen, am Schutzgut orientierten Katalog entwickeln.

c) Öffnung für selbstlernende Systeme und erhöhte Eingriffsschwellen

Die zentrale Änderung des Antrags betrifft den bisherigen § 47a Absatz 1 Satz 4 ASOG. Der ursprüngliche Entwurf sah vor, dass die automatisierte Datenanalyse regelbasiert nach einer von Menschen definierten Abfolge von Verarbeitungsschritten erfolgt. Die Begründung führte hierzu aus, dies schließe den Einsatz selbstlernender künstlicher Intelligenz aus, da dieser zwar nicht von vornherein unzulässig sei, aber „wegen des besonderen Eingriffsgewichts außerordentlich restriktiven Voraussetzungen" unterliege (BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100f.), „die sich für die aktuelle Gesetzgebung noch nicht klar genug abzeichnen" (vgl. S. 332 der Begründung des ursprünglichen Entwurfes). Mit dem Änderungsantrag wird diese Beschränkung aufgehoben, um „ein breiteres Spektrum von Anbietern für Systeme der automatisierten Datenanalyse zu ermöglichen und dem Grundsatz der europäischen digitalen Souveränität besser Rechnung zu tragen" (vgl. S. 42 der Begründung des Änderungsentwurfes).

Zugleich wird die Zulässigkeit selbstlernender Systeme abgestuft. Nach dem neuen Satz 5 ist die Nutzung unter den Voraussetzungen von Satz 2 Nummer 1 und 3 zulässig. Für den Fall von Satz 2 Nummer 2 wird die Eingriffsschwelle deutlich angehoben: Hier ist die Nutzung nur bei konkretisierter Gefahr einer terroristischen Straftat oder einer in § 100b Absatz 2 StPO genannten besonders schwerwiegenden Straftat zulässig.

Diese Öffnung für selbstlernende Systeme wirft trotz Anhebung der Eingriffsschwellen erhebliche verfassungsrechtliche Fragen auf. Das Bundesverfassungsgericht hat in seinem Urteil vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20, Rn. 100f.) ausgeführt, dass

der Einsatz selbstlernender Systeme außerordentlich restriktiven Voraussetzungen unterliegt, denn „deren Mehrwert, zugleich aber auch ihre spezifischen Gefahren liegen darin, dass nicht nur von den einzelnen Polizistinnen und Polizisten aufgegriffene kriminologisch fundierte Muster Anwendung finden, sondern solche Muster automatisiert weiterentwickelt oder überhaupt erst generiert und dann in weiteren Analysestufen weiter verknüpft werden. [...] So könnten besonders weitgehende Informationen und Annahmen über eine Person erzeugt werden, deren Überprüfung spezifisch erschwert sein kann. Denn komplexe algorithmische Systeme könnten sich im Verlauf des maschinellen Lernprozesses immer mehr von der ursprünglichen menschlichen Programmierung lösen, und die maschinellen Lernprozesse und die Ergebnisse der Anwendung könnten immer schwerer nachzuvollziehen sein [...]. Dann droht zugleich die staatliche Kontrolle über diese Anwendung verloren zu gehen." Das Gericht hat diese Voraussetzungen allerdings nicht abschließend konkretisiert. Der nun vorliegende Änderungsantrag nimmt die Öffnung vor, ohne sich in der erforderlichen Weise mit der verfassungsrechtliche Rechtslage auseinanderzusetzen:

Der neue Satz 8 verlangt zwar, dass die Ergebnisse nachvollziehbar und nachprüfbar bleiben. Der neue Satz 9 konkretisiert zudem, dass nicht Schlussfolgerungen des Systems, sondern die Ausgangsdaten selbst Grundlage weiterer Maßnahmen sein dürfen. Diese Regelungen sind auch von zentraler Bedeutung für den Grundrechtsschutz, denn das Bundesverfassungsgericht hat in seinem Urteil vom 16. Februar 2023 hervorgehoben, dass gänzlich automatisierte Entscheidungsfindungen unzulässig sind (BVerfG, a.a.O., Rn. 108f.). Allerdings stellt sich die Frage, ob diese Anforderungen bei selbstlernenden Systemen praktikabel und vor allem umsetzbar sind. Je komplexer ein System ist, desto schwieriger wird es, seine Ergebnisse vollständig nachzuvollziehen. Es besteht die Gefahr, dass die Nachvollziehbarkeitsanforderung zu einer bloßen Formalität wird. Die Begründung schweigt zu der Frage, wie bei selbstlernenden Systemen die Nachvollziehbarkeit praktisch sichergestellt werden soll.

Ich empfehle, die Anforderungen zu konkretisieren und technische Mindeststandards für die Erklärbarkeit festzulegen. Zudem sollte klargestellt werden, dass bei Systemen, deren Entscheidungswege nicht hinreichend nachvollziehbar gemacht werden können, von deren Einsatz abzusehen ist.

d) Schutz vor Diskriminierung

Der neue Satz 6 regelt, dass durch geeignete Maßnahmen sicherzustellen ist, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Diese Regelung ist grundsätzlich zu begrüßen, bleibt aber zu unbestimmt. Es wird lediglich gefordert, dass „geeignete Maßnahmen" zu ergreifen sind, ohne dass diese konkretisiert werden. Dies ist problematisch, weil selbstlernende Systeme im Lernprozess Verzerrungen aus den Trainingsdaten übernehmen und verstärken können. In meiner Stellungnahme vom 29. September 2025 hatte ich auf empirisch belegte Diskriminierungsrisiken hingewiesen (vgl. S. 14). Die bloße Forderung nach „geeigneten Maßnahmen" genügt dem verfassungsrechtlichen Bestimmtheitsgebot nicht.

Ich empfehle, die Anforderungen zu konkretisieren, etwa durch die Festlegung regelmäßiger Bias-Tests, der Dokumentation der Trainingsdaten und deren Repräsentativität sowie fortlaufender Überwachung hinsichtlich diskriminierender Ergebnisse.

e) Verwendung von Nutzungsdaten

Mit der Änderung in § 47a Absatz 2 Satz 1 ASOG wird geregelt, dass Nutzungsdaten wie Verkehrsdaten nur in den Fällen des § 47a Absatz 1 Satz 2 Nummer 1 ASOG in die automatisierte Datenanalyse einbezogen werden dürfen (vgl. S. 42 der Begründung des Entwurfes). Dies bedeutet, dass Nutzungsdaten nur bei konkreter Gefahr für höchstrangige Rechtsgüter verwendet werden dürfen, nicht aber bei konkretisierter Gefahr der Begehung schwerer oder terroristischer Straftaten nach Nummer 2 und 3.

Diese Beschränkung ist zu begrüßen, da sie dem besonderen Eingriffsgewicht der Einbeziehung von Nutzungsdaten Rechnung trägt. Nutzungsdaten ermöglichen weitreichende Rückschlüsse auf das Kommunikationsverhalten und damit auf persönliche Beziehungen und Lebensumstände. Ihre Einbeziehung in die automatisierte Datenanalyse erhöht das Eingriffsgewicht erheblich. Es ist daher sachgerecht, diese Daten nur bei konkreter Gefahr für höchstrangige Rechtsgüter zu verwenden. Allerdings bleibt unklar, warum diese Beschränkung nicht auch für den Einsatz selbstlernender Systeme nach dem neuen Satz 5 gilt. Das erhöhte Eingriffsgewicht selbstlernender Systeme in Verbindung mit der Einbeziehung sensibler Nutzungsdaten erfordert, wie bereits dargelegt, zusätzliche Einschränkungen.

f) Benachrichtigungspflicht

Der neue § 47a Absatz 3 Satz 6 ASOG regelt eine Benachrichtigungspflicht gegenüber Personen, gegen die nach einer automatisierten Datenanalyse weitere Maßnahmen getroffen wurden. Diese Regelung ist zu begrüßen, entspricht den verfassungsgerichtlichen Vorgaben (BVerfG, a.a.O., Rn. 109) und ermöglicht Rechtsschutz. Allerdings ist die Beschränkung auf Personen, gegen die weitere Maßnahmen getroffen wurden, zu eng.

Ich empfehle, die Benachrichtigungspflicht auf alle Personen auszudehnen, deren Daten in erheblichem Umfang einbezogen wurden.

g) Periodische Kontrollverpflichtung

Mit der Ergänzung im neuen Satz 7 des § 47a Absatz 3 ASOG werden Kontrollen durch die behördliche Datenschutzbeauftragte spätestens alle zwei Jahre vorgeschrieben. Ein Intervall von zwei Jahren erscheint für eine so eingriffsintensive Maßnahme, insbesondere beim Einsatz selbstlernender Systeme, zu lang. Selbstlernende Systeme können sich im Laufe der Zeit verändern und diskriminierende Muster entwickeln.
Ich empfehle, das Kontrollintervall auf jährliche Kontrollen zu verkürzen und beim Einsatz selbstlernender Systeme halbjährliche Kontrollen vorzuschreiben.

h) Fazit

Der Änderungsantrag versucht, dem erhöhten Eingriffsgewicht selbstlernender Systeme durch verschiedene Schutzmechanismen Rechnung zu tragen: Anhebung der Eingriffsschwelle in bestimmten Fällen, Schutz vor diskriminierenden Algorithmen, Nachvollziehbarkeitsanforderungen, erhöhte Anordnungsbefugnisse und verstärkte Kontrollen. Diese Schutzmechanismen sind grundsätzlich zu begrüßen, sind jedoch in ihrer derzeitigen Ausgestaltung nicht ausreichend, um den verfassungsrechtlichen Anforderungen zu genügen. Insbesondere bleiben zentrale Fragen ungeklärt, etwa wie bei selbstlernenden Systemen die Nachvollziehbarkeit praktisch sichergestellt werden soll, welche konkreten Maßnahmen zur Verhinderung diskriminierender Algorithmen zu ergreifen sind und welche Anforderungen an die Trainingsdaten zu stellen sind.

Die Neuregelung bedarf einer grundlegenden Überarbeitung, um den verfassungsrechtlichen Anforderungen an den Einsatz selbstlernender Systeme bei der automatisierten Datenanalyse zu genügen.