bitkom

Stellungnahme

Januar 2026

Gesetz zur Modernisierung des Bundespolizeigesetzes

Zusammenfassung

Mit der Novellierung des Bundespolizeigesetzes (BPolG-E) sollen die rechtlichen Grundlagen für eine moderne, digital unterstützte Polizeiarbeit weiterentwickelt werden. Fortschreitende Digitalisierung, neue technische Möglichkeiten – etwa in der Telekommunikationsüberwachung, bei automatisierten Analysen, Sensorik, Drohnen oder der Verarbeitung von Fluggast- und Grenzdaten – sowie eine zunehmende Vernetzung von Sicherheits- und Infrastruktursystemen erfordern klare, rechtssichere und technisch umsetzbare Regelungen.

Bitkom begrüßt das Ziel, die Leistungsfähigkeit der Bundespolizei zu stärken. Der Gesetzentwurf enthält hierfür wichtige Ansätze, weist aus Sicht der Digitalwirtschaft jedoch noch Klarstellungs- und Nachbesserungsbedarf auf. Neue Befugnisse müssen auf klaren rechtlichen Grundlagen, standardisierten technischen Verfahren und zumutbaren Mitwirkungspflichten beruhen. Fehlende Schnittstellenstandards, unklare Governance, offene Haftungs- und Kostenfragen gefährden Rechts- und Planungssicherheit und erschweren die Zusammenarbeit zwischen Behörden und Unternehmen. Für eine innovationsfreundliche Bundespolizei fehlen zudem bislang eine ausdrückliche, differenzierte Rechtsgrundlage für automatisierte Datenanalysen sowie ein gesetzlich verankertes Innovationslabor, in dem neue Technologien kontrolliert, transparent und grundrechtskonform erprobt werden können.

Eine zukunftsfähige Ausgestaltung des Bundespolizeigesetzes erfordert:

- **Einheitliche, offene und standardisierte Behörden-Schnittstellen mit klarer Governance**
- **Faire Kostenerstattungsregelungen & realistische Übergangsfristen** für verpflichtete Unternehmen
- **Ausdrückliche und differenzierte Rechtsgrundlage für automatisierte Datenanalyse**
- **Ein Innovationslabor für die Bundespolizei**, um neue Technologien kontrolliert, transparent und grundrechtskonform zu erproben

Einleitung

Der Bitkom setzt sich für moderne und digitale Polizeikräfte ein. Fortschreitende Digitalisierung und zunehmende Vernetzung erfordern eine kontinuierliche Anpassung der rechtlichen Rahmenbedingungen. Die Digitalisierung im Polizeikontext muss dabei mit einem hohen Maß an technischer Standardisierung, Datenschutz und Rechtssicherheit erfolgen, um Vertrauen in staatliche Systeme zu gewährleisten. Das neue Bundespolizeigesetz enthält zahlreiche Regelungen, die Chancen für die Telekommunikationsbranche, Betreiber kritischer Infrastrukturen und die Digitalwirtschaft darstellen.

Der Bitkom begrüßt die Bemühungen, die Sicherheit und den Datenschutz zu stärken, sieht jedoch in mehreren Punkten einen konkreten Nachbesserungsbedarf. Für einen sicheren, rechtssicheren und wirtschaftlich tragfähigen Vollzug sind klare Schnittstellenstandards, zumutbare Pflichten, verbindliche Governance-Prozesse und fair verteilte Kosten unerlässlich. Zugleich weist der Bitkom darauf hin, dass neue Befugnisse nur auf der Grundlage klar bestimmter rechtlicher Voraussetzungen, technisch standardisierter Verfahren und zumutbarer Umsetzungsbedingungen eingeführt werden dürfen.

Die folgenden Punkte fassen die aus Sicht der Digitalwirtschaft zentralen Änderungs- und Klarstellungsbedarfe zusammen.

Einheitliche technische Standards und Schnittstellen

Für die Umsetzung der neuen Pflichten nach § 24 (Bestandsdatenauskunft), §25 (Erhebung von Verkehrs- und Nutzungsdaten), § 41 (Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten) und § 52 (Erhebung von Fluggastdaten durch Luftfahrtunternehmen und Übermittlung an die Bundespolizei) BPolG-E sollten einheitliche, offene und dokumentierte Schnittstellenstandards in Form von Behörden-APIs festgelegt werden. Diese Schnittstellen sollten sich an anerkannten europäischen und internationalen Normen, etwa einschlägigen ETSI- und ISO-Standards, orientieren und in einem offenen, maschinenlesbaren Format beschrieben sein, sodass eine automatisierte und sichere Anbindung der beteiligten Systeme möglich ist. Ein solcher Standardansatz gewährleistet Interoperabilität, Transparenz und technologische Neutralität. Er reduziert Implementierungsaufwand und Kosten, insbesondere für kleine und mittelständische Anbieter, und verhindert parallele, inkompatible Lösungen in Bund- und Länderzuständigkeit.

Bitkom empfiehlt, dass die Bundesregierung für diese Schnittstellen eine zentrale Governance-Struktur etabliert, zum Beispiel in Form eines API- und Datenformat-Registers, in dem Spezifikationen, Versionen und Änderungen nachvollziehbar dokumentiert werden. Ergänzend sollten verbindliche Ankündigungs- und Übergangsfristen für technische Änderungen vorgesehen werden, damit Unternehmen technische Anpassungen mit angemessenem Vorlauf umsetzen können, ohne laufende Dienste oder Sicherheitsarchitekturen zu beeinträchtigen. Dies gilt nicht nur für Telekommunikationsanbieter, sondern ebenso für Betreiber von Verkehrs- und

sonstigen Infrastrukturen, die über standardisierte Schnittstellen in Sicherheitsprozesse eingebunden werden.

Rechtssicherheit bei der Telekommunikationsüberwachung

Präventive Eingriffe in Telekommunikations- und Standortdaten nach § 25, § 40 (Überwachung der Telekommunikation) und 41 BPolG-E müssen auf klar bestimmten gesetzlichen Grundlagen beruhen. Aus Sicht der Digitalwirtschaft sind dabei insbesondere die folgenden drei Punkte entscheidend: Erstens sollte jede Maßnahme einem wirksamen Richtervorbehalt unterliegen, um die Rechtmäßigkeit und Verhältnismäßigkeit sicherzustellen. Zweitens sollte der Gesetzgeber präzisieren, ab welcher konkretisierten Gefahr präventive Eingriffe zulässig sind, um Vollzugs- und Auslegungsspielräume zu begrenzen und Rechtsunsicherheiten zu vermeiden. Drittens sind bei der Überwachung von Kommunikationsinhalten, insbesondere im Rahmen der Quellen-Telekommunikationsüberwachung, technische Schutzmechanismen vorzusehen, die höchstpersönliche Kommunikation automatisch erkennen und ausschließen, um den verfassungsrechtlich gebotenen Kernbereichsschutz zu wahren.

Diese Anforderungen setzen die Vorgaben des Bundesverfassungsgerichts um und schaffen zugleich Rechtssicherheit für Unternehmen, die zur Mitwirkung verpflichtet sind. Technische Integrationspflichten sollten nur nach vorheriger Sicherheits- und Datenschutzbewertung auferlegt werden, um IT-Sicherheitsrisiken und Haftungsunsicherheiten zu vermeiden. Aus Sicht der Netzbetreiber ist zudem klarzustellen, dass eine Unterstützung bei Quellen-TKÜ-Maßnahmen nur in engen Grenzen möglich ist. Forderungen, physischen Zugriff auf Netzkomponenten im Feld zu gewähren, etwa auf Outdoor-Netzknoten, um dort behördliche Spezialgeräte zu installieren, sind mit erheblichen betrieblichen, sicherheitstechnischen und wettbewerblichen Risiken verbunden. Gleiches gilt für Überlegungen, über Leitungen der Anbieter behördliche Software in Systeme einzuspielen oder spezielle Firmware auf Kundenendgeräten auszurollen. Solche Ansätze würden gezielt Schwachstellen in Infrastrukturen und Endgeräte einführen und die Verantwortung für staatliche Eingriffe faktisch auf die Unternehmen verlagern. Bitkom sieht hier einen klaren Klarstellungsbedarf: Eingriffe in die Integrität der privaten Netzinfrastruktur sind zu vermeiden. Mitwirkungspflichten müssen sich auf rechtlich klar umrissene, technisch abgesicherte und betrieblich zumutbare Prozesse beschränken.

Im Bereich der Identifizierungs- und Lokalisierungsmaßnahmen nach § 41 BPolG-E erscheint die Umsetzung grundsätzlich unkritisch, sofern diese im Rahmen bereits etablierter Auskunftslösungen erfolgt. Werden bestehende, rechtlich geprüfte und technisch standardisierte Schnittstellen genutzt, können die beschriebenen Maßnahmen ohne zusätzliche tiefgreifende Eingriffe in die Infrastruktur umgesetzt werden. Klarzustellen ist allerdings, dass eine permanente, flächendeckende oder automatisierte Überwachung ohne konkreten Anlass unzulässig ist und die Maßnahmen an konkrete Fälle, richterliche Anordnungen und das Zweckbindungsprinzip nach § 47 (Kennzeichnung) BPolG-E in Verbindung mit Teil 3 BDSG gebunden sind.

Datenschutz und technische Verantwortung bei Sensorik, Drohnen und Biometrie

Für die Erhebung und Verarbeitung von Bild-, Ton- oder biometrischen Daten nach § 32 (Mobile Bild- und Tonaufzeichnungsgeräte), §38 (Einsatz mobiler Sensorträger für Bildaufnahme-, Bildaufzeichnungs-, Tonaufnahme und Tonaufzeichnungsgeräte), §39 (Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme) und §52 BPolG-E sollte der Gesetzgeber eine verbindliche Datenschutz-Folgenabschätzung vorschreiben. Damit können Risiken für die Rechte der Betroffenen frühzeitig identifiziert und geeignete Schutzmaßnahmen festgelegt werden. Zusätzlich sollten »Privacy-by-Design«-Grundsätze unmittelbar im Gesetz verankert werden, um Datenschutz und technische Sicherheit frühzeitig zu verankern. Dazu gehört insbesondere, dass nicht-relevante Bildbereiche automatisiert unkenntlich gemacht werden, dass Tonaufnahmen grundsätzlich deaktiviert sind und nur in begründeten Ausnahmefällen und unter besonderen Voraussetzungen zugeschaltet werden dürfen, dass Zugriffe auf Daten über ein Rollen- und Berechtigungskonzept gesteuert und lückenlos protokolliert werden und dass Lösch- und Sperrfristen so ausgestaltet sind, dass sie dem Grundsatz der Speicherbegrenzung gerecht werden.

Bei automatisierten Entscheidungen, etwa in der Grenz- oder Fluggastdatenverarbeitung, sollte ein »Human-in-the-Loop«-Prinzip vorgesehen werden, um Fehlklassifikationen und unbeabsichtigte Diskriminierungen zu vermeiden und den Anforderungen des Datenschutzrechts gerecht zu werden. Automatisierte Trefferlisten dürfen nicht ohne nachgelagerte menschliche Prüfung zu Maßnahmen führen. Dies stärkt sowohl die Grundrechtskonformität als auch das Vertrauen in den Einsatz moderner Analysesysteme durch Sicherheitsbehörden.

Kostenfairness und Übergangsregelungen

Für Mitwirkungspflichten nach §§ 24, 25, 41 und 52 BPolG-E sollten verbindliche Kostenerstattungsregeln in Anlehnung an die Systematik des Justizvergütungs- und -entschädigungsgesetzes vorgesehen werden. Anders als bei § 96 (Unterstützungspflichten) BPolG-E, wo die Begründung eine Kostenerstattung zugunsten der betroffenen Unternehmen ausdrücklich annimmt, fehlt für Provider-Schnittstellen bislang eine entsprechende Absicherung. Dies betrifft nicht nur Telekommunikationsanbieter, sondern auch Betreiber von Verkehrs- und Infrastruktursystemen, die beispielsweise Fahr- oder Flugdaten bereitstellen oder räumliche und technische Einrichtungen zur Verfügung stellen. Übergangsfristen von mindestens zwölf bis achtzehn Monaten und verbindliche Ankündigungsfristen für Spezifikationsänderungen von mindestens sechs Monaten sind erforderlich, um eine realistische Planung und Investitionssicherheit zu gewährleisten. Unternehmen, die behördliche Spezifikationen ordnungsgemäß umsetzen, benötigen zudem einen »Haftungs-Safe-Harbor«, damit sie bei regelkonformer Integration behördlicher Schnittstellen nicht für behördlich verursachte Folgeeffekte haften.

Im Bereich der Unterstützungspflichten nach § 96 BPolG-E besteht darüber hinaus Präzisierungsbedarf. Insbesondere bei der Übermittlung von Fahrplandaten sollte klar

definiert werden, an welche Stellen diese Daten weitergegeben werden dürfen und zu welchen Zwecken sie genutzt werden können. Es bietet sich an, in der Gesetzesbegründung klarzustellen, dass sich die Pflicht auf nicht personenbezogene Daten beschränkt, die im Rahmen der eigenen Planung und Vorbereitung zur Gewährleistung eines störungsfreien Betriebs ohnehin verarbeitet werden. Auch die Verpflichtung zur Schaffung oder Bereitstellung von Einrichtungen bedarf einer Konkretisierung. Es sollte klargestellt werden, dass keine Pflicht zur Errichtung neuer Gewahrsamszellen oder vergleichbarer sicherheitsbehördlicher Infrastrukturen besteht. Schließlich sollte in Bezug auf weitere Leistungen deutlich werden, dass hieraus keine generelle Ermächtigung folgt, beliebige zusätzliche Flächen oder Leistungen von betroffenen Unternehmen zu verlangen, und dass bei der Selbstkostenerstattung praxistaugliche Instrumente wie Rahmenvereinbarungen anerkannt werden, ohne dass in jedem Einzelfall ein gesonderter Antrag gestellt werden muss.

Interoperabilität und Governance bei europäischen Informationssystemen

Im Bereich der Grenz- und Fluggastdatenverarbeitung nach § 52 BPolG-E sowie den §§ 54 (Übermittlung personenbezogener Daten an Mitgliedstaaten der Europäischen Union und Schengen-assoziierte Staaten) bis 56 (Übermittlung personenbezogener Daten im internationalen Bereich) BPolG-E sollten die bestehenden Schnittstellen zu europäischen Systemen wie EES, ETIAS, VIS und zukünftig Prüm II auf eine klare Zweckbindung und technische Interoperabilität ausgerichtet werden. Die Umsetzung sollte durch eine bundeseinheitliche Governance-Struktur koordiniert werden, die Zuständigkeiten, technische Standards und Prozesse für Änderungen verbindlich festlegt. Eine solche Struktur sollte insbesondere ein Register für Schnittstellen und Datenformate, ein standardisiertes Änderungsmanagement sowie dokumentations- und meldepflichtige Prozesse für Störungen, Fehler und Anpassungen enthalten.

Die Evaluierung nach § 106 (Berichtspflichten; Evaluierung) BPolG-E sollte anhand messbarer Qualitätsindikatoren erfolgen, etwa zur Systemverfügbarkeit, zu Fehlerquoten, zu Bearbeitungszeiten und zu dokumentierten Datenschutzvorfällen, und regelmäßig in einem Transparenzbericht veröffentlicht werden. Diese Maßnahmen gewährleisten Rechtssicherheit, stärken die Nachvollziehbarkeit von Datenflüssen und fördern das Vertrauen in eine moderne, europäisch vernetzte Sicherheitsarchitektur.

Rechtsgrundlage für automatisierte Datenanalyse

Über die punktuelle Nutzung digitaler Werkzeuge hinaus wird die künftige Leistungsfähigkeit der Bundespolizei maßgeblich davon abhängen, ob sie rechtssicher und grundrechtskonform automatisierte Datenanalysen einsetzen kann. Das Bundespolizeigesetz sollte daher ausdrücklich eine eigene Ermächtigungsgrundlage

für die automatisierte Datenanalyse enthalten. Die Ausgestaltung kann sich an bereits existierenden Normen in den Polizeigesetzen der Länder orientieren, etwa an den Vorschriften zur automatisierten Datenanalyse in Rheinland-Pfalz und Hessen, muss jedoch zwingend die Maßstäbe des Bundesverfassungsgerichts berücksichtigen. Das Urteil vom 16. Februar 2023 hat klargestellt, dass der Einsatz automatisierter Analysesysteme nur unter engen Voraussetzungen zulässig ist. Erforderlich sind insbesondere klar bestimmte Zwecke, streng definierte Gefahrenlagen, eine Differenzierung nach Datenarten und Sensitivität, transparente Prüf- und Filtermechanismen, ein wirksamer Kernbereichsschutz sowie dokumentierte Kontroll- und Löschprozesse.

Eine entsprechende Norm im Bundespolizeigesetz sollte deshalb präzise regeln, welche Datenkategorien in welchen Konstellationen analysiert werden dürfen, welche Schwellenwerte für den Einsatz automatisierter Analyseverfahren gelten, wie weit Querverknüpfungen zwischen verschiedenen Datenbeständen reichen dürfen und welche verfahrensrechtlichen Sicherungen – etwa richterliche Kontrolle, Berichtspflichten und dokumentationspflichtige Prüfentscheidungen – vorzusehen sind. Automatisierte Analysen dürfen nicht zu anlassloser Massendurchleuchtung führen, sondern müssen auf klar umschriebene, qualifizierte Gefahrenlagen begrenzt und streng verhältnismäßig ausgestaltet sein. Nur eine ausdrückliche, differenzierte Ermächtigungsgrundlage kann hier Rechtssicherheit schaffen, den verfassungsrechtlichen Anforderungen genügen und zugleich den gezielten Einsatz moderner Analysetechnologien ermöglichen.

Innovationslabor Bundespolizei

Um automatisierte Datenanalyse und weitere technische Entwicklung nicht nur normativ zu begleiten, sondern auch praktisch zu gestalten, sollte der Gesetzgeber zudem ein eigenes Innovationslabor für die Bundespolizei vorsehen: Viele Landespolizeien haben ein solches Innovationslabor bereits eingerichtet. Ein Innovationslabor der Bundespolizei könnte als organisatorisch klar abgegrenzte Einheit dienen, in der neue digitale Verfahren, automatisierte Analysesysteme und KI-gestützte Werkzeuge unter kontrollierten Bedingungen getestet, wissenschaftlich begleitet und datenschutzrechtlich bewertet werden, bevor sie in den Regelbetrieb überführt werden. In diesem Rahmen können Technikentwicklung, Datenschutz, IT-Sicherheit und praktische Einsatzanforderungen systematisch zusammengeführt werden. Das Innovationslabor sollte gesetzlich so verankert werden, dass eine enge Zusammenarbeit mit Wissenschaft und Wirtschaft möglich ist, ohne dass dies zu intransparenten Pilotanwendungen im Echtbetrieb führt. Es bedarf klarer Regeln für Testumgebungen, Testdatensätze, Evaluationskriterien und Ex-ante- sowie Ex-post-Kontrollen, damit Innovationen zielgerichtet gefördert und zugleich Grundrechte wirksam geschützt werden. Ein solches Labor würde nicht nur die technische und organisatorische Lernfähigkeit der Bundespolizei stärken, sondern auch dazu beitragen, dass neue Instrumente von Beginn an nach dem Prinzip »Security and Privacy by Design« konzipiert werden und sich an offenen Standards orientieren, die die Interoperabilität mit bestehenden Infrastrukturen der Digitalwirtschaft sicherstellen.

Telekommunikation und Providerpflichten

§ 24 BPolG-E zur Bestandsdatenauskunft regelt die Abfrage von Bestandsdaten bei Diensteanbietern. Die Abfrage von Bestandsdaten muss den Anforderungen des Teil 3 BDSG entsprechen, der die Richtlinie (EU) 2016/680 umsetzt. Die Datenschutz-Grundverordnung ist nur anwendbar, soweit keine Verarbeitung zu Zwecken der Strafverfolgung oder Gefahrenabwehr im Sinne des Teil 3 BDSG erfolgt. Entscheidend ist, dass die rechtlichen Grundlagen für die Bereitstellung personenbezogener Daten klar definiert sind, um Rechtsunsicherheiten zu vermeiden. Eine Überregulierung könnte die Zusammenarbeit zwischen Anbietern und Behörden behindern und das Vertrauen der Nutzerinnen und Nutzer in digitale Dienste beeinträchtigen.

§ 25 BPolG-E betrifft die Erhebung von Verkehrs- und Nutzungsdaten und damit präventive Auskünfte bei Verpflichteten nach § 3 Absatz 2 Satz 1 TDDDG[1]. Die Erhebung dieser Daten muss technisch umsetzbar und für die Anbieter zumutbar sein. Bezüglich der Kosten gelten die Anmerkungen wie im Abschnitt »Kostenfairness und Übergangsregelungen«.

§ 40 BPolG-E regelt die Überwachung der Telekommunikation, einschließlich der Quellen-TKÜ, als präventive Maßnahme. Die Überwachung muss im Einklang mit den Grundrechten der Bürgerinnen und Bürger stehen und darf die IT-Sicherheit der Anbieter nicht gefährden. Aus Sicht der Unternehmen ist sicherzustellen, dass technische Umsetzungen nicht zu neuen Sicherheitslücken führen. Forderungen, etwa Zugriff auf verteilte Netzkomponenten zu gewähren, um behördliche Spezialtechnik dort zu installieren, oder spezifische Software über Netze einzuspielen beziehungsweise angepasste Firmware auf Endgeräten auszurollen, würden die Funktionsfähigkeit und Sicherheit der Infrastrukturen beeinträchtigen. Bitkom empfiehlt daher, vor der verpflichtenden Implementierung technischer Überwachungsschnittstellen eine standardisierte Sicherheits- und Datenschutzbewertung vorzusehen. So kann sichergestellt werden, dass neue Integrationspflichten weder zu Sicherheitsrisiken noch zu unverhältnismäßigen Belastungen der betroffenen Anbieter führen. Ergänzend sollte ein klar geregeltes Verfahren für die Meldung und Behandlung technischer Schwachstellen geschaffen werden, um Transparenz und IT-Sicherheit zu erhöhen. Zugleich ist klarzustellen, dass Anbieter keine eigenständige Wartungs- oder Haftungsverantwortung für staatlich eingesetzte Überwachungssoftware tragen, sofern sie die behördlichen Vorgaben ordnungsgemäß umsetzen.

§ 41 BPolG-E betrifft die Identifizierung und Lokalisierung von Mobilfunkkarten und Endgeräten und umfasst unter anderem den Einsatz von stillen SMS und im Ergebnis auch IMSI-Catcher-nahe Maßnahmen. Solche Maßnahmen können datenschutzrechtliche Probleme aufwerfen. Es ist entscheidend, dass sie nur unter strengen rechtlichen Rahmenbedingungen eingesetzt werden dürfen, um den Datenschutz und die Privatsphäre der Bürgerinnen und Bürger zu gewährleisten. Lokalisierungs- und Identifizierungsmaßnahmen sollten nach dem Grundsatz der

[1] Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten | Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)

Verhältnismäßigkeit nur im Einzelfall, auf richterliche Anordnung und nur unter den Voraussetzungen der §§ 25 und 40 BPolG-E zulässig sein, sofern eine konkrete Gefahr vorliegt. Die technische Schnittstelle ist so auszugestalten, dass Daten nur auf Anfrage der zuständigen Behörde bereitgestellt werden. Eine permanente Datenabfrage oder automatisierte Überwachung würde dem Zweckbindungsprinzip des § 47 BPolG-E in Verbindung mit Teil 3 BDSG widersprechen. Aus Sicht der Anbieter ist hervorzuheben, dass die Nutzung vorhandener, standardisierter Auskunftsschnittstellen ausreichend ist und keine zusätzlichen, tief in die Infrastruktur eingreifenden Maßnahmen erfordert.

Sensorik, Video/Audio und automatisierte Systeme

§ 30 BPolG-E zur Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen bildet den Rahmen für polizeiliche Erhebungen vor Ort. Auch hier muss der Schutz der Privatsphäre gewahrt bleiben. Die rechtlichen Rahmenbedingungen sind so zu definieren, dass Transparenz, Verhältnismäßigkeit und Vertrauen der Bürgerinnen und Bürger in die Sicherheitsbehörden gewährleistet werden. Für verhältnismäßige, transparente und revisionssichere Datenerhebung mittels Video- und Audioaufzeichnungen sollten grundsätzlich die Maßnahmen und Prinzipien umgesetzt werde, wie sie im Abschnitt »Datenschutz und technische Verantwortung bei Sensorik, Drohnen und Biometrie« beschrieben wurden.

§ 31 BPolG-E zu selbsttätigen Bildaufnahme- und Aufzeichnungsgeräten enthält gegenüber der bisherigen Rechtslage nur redaktionelle Anpassungen und verweist im Wesentlichen auf bereits bestehende Befugnisse zum Einsatz fest installierter Kameras, etwa in Bahnhöfen oder Flughäfen. Aus Sicht der Digitalwirtschaft fehlen jedoch verbindliche technische und organisatorische Mindeststandards. Um Rechts- und Planungssicherheit zu gewährleisten, sollten in § 31 ausdrücklich bundeseinheitliche Löschfristen, die Pflicht zur Dokumentation von Zugriffen und Änderungen, die Kennzeichnung offener Aufzeichnungen und der Ausschluss von Tonaufnahmen bei stationären Systemen geregelt werden. Dies würde eine einheitliche Umsetzung im gesamten Bundesgebiet ermöglichen und unnötige Mehrfachintegrationen vermeiden.

§ 32 BPolG-E regelt mobile Bild- und Tonaufzeichnungsgeräte wie Bodycams und erweitert den zulässigen Einsatzbereich erheblich, insbesondere auf Situationen des Aufenthaltsvollzugs. Bitkom empfiehlt, § 32 um klare Aktivierungsschwellen, kurze Speicherfristen und transparente Dokumentationspflichten zu ergänzen. Audioaufzeichnungen sollten nur in begründeten Ausnahmefällen und mit gesonderter Freigabe zulässig sein. Darüber hinaus sollten für künftige unionsrechtliche Anforderungen an KI-Systeme in der Strafverfolgung angemessene Übergangsfristen vorgesehen werden, um eine geordnete technische Umsetzung zu ermöglichen.

§ 33 BPolG-E zur anlassbezogenen automatischen Kennzeichenerfassung begrenzt den Einsatz von Kennzeichenerfassungssystemen auf anlassbezogene, vorübergehende und nicht flächendeckende Maßnahmen. Nichttreffer sind unverzüglich zu löschen;

Treffer müssen überprüft und dokumentiert werden. Bitkom begrüßt diese grundrechtsschonende Ausgestaltung, regt jedoch an, ergänzend Qualitätsmaßstäbe und technische Standardisierungspflichten festzuschreiben. Insbesondere sollten Fehlalarm- und Erkennungsquoten regelmäßig evaluiert und Datenlisten sowie Schnittstellen bundeseinheitlich definiert werden, um eine effiziente Integration bei Betreiber- und Provider-Systemen zu gewährleisten. Ergänzend sollte hier sowie bei weiteren Datenverarbeitungsschritten eine klare gesetzliche Grundlage für automatisierte Analysen geschaffen werden, die sich am verfassungsrechtlichen Rahmen und an bestehenden landesrechtlichen Vorbildern orientiert.

§ 34 BPolG-E zur Gesprächsaufzeichnung regelt die Aufzeichnung von Gesprächen in Einsatz- und Führungsstellen auch bei Nutzung öffentlich bekannter Telefonnummern und sieht eine Löschung spätestens nach dreißig Tagen vor. Bitkom empfiehlt, ergänzend Integritäts- und Nachweisvorgaben aufzunehmen, etwa durch digitale Prüfsummen oder unveränderbare Sicherungsketten, um die Authentizität der Aufzeichnungen zu gewährleisten. Zudem sollten einheitliche Export- und Archivformate für forensische Zwecke festgelegt werden, um eine rechts- und beweissichere Weiterverarbeitung zu ermöglichen. Verdeckte Tonaufzeichnungen dürfen nur auf richterliche Anordnung und bei enger Zweckbindung erfolgen, um den verfassungsrechtlichen Anforderungen des Art. 10 GG und des Kernbereichsschutzes zu entsprechen. Diese Ergänzungen erhöhen die technische Nachvollziehbarkeit und Rechtssicherheit, ohne die Einsatzfähigkeit der Behörden zu beeinträchtigen.

§§ 35 und 36 BPolG-E zu besonderen Mitteln der Datenerhebung sowie zu Vertrauenspersonen und verdeckten Ermittlern übernehmen weitgehend die bisherige Systematik der verdeckten Datenerhebung, ohne verbindliche technische Mindeststandards oder Datenschutzmechanismen festzulegen. Bitkom empfiehlt, ergänzend Kernbereichsschutzmechanismen vorzusehen, etwa automatisierte Verfahren zur Filterung höchstpersönlicher Kommunikation sowie eine verpflichtende Protokollierung sämtlicher Datenverwendungen. Anfragen an Plattformen oder Telekommunikationsanbieter sollten über standardisierte Behörden-Schnittstellen erfolgen und mit zumutbaren Fristen beantwortet werden können. Um Rechtssicherheit und Verhältnismäßigkeit zu gewährleisten, sind Generalklauseln zu vermeiden und die einzelnen Befugnisse präzise zu definieren. Diese Ergänzungen schaffen klare Vollzugsgrundlagen, reduzieren technische und haftungsrechtliche Unsicherheiten und stärken zugleich das Vertrauen in datenschutzkonforme Ermittlungsverfahren.

Einsatz und Abwehr von Drohnen

Drohnen stellen sowohl Chancen als auch Risiken für die Sicherheitsbehörden dar. Es ist notwendig, klare Anforderungen an den Schutz vor unbemannten Luftfahrtsystemen zu prüfen, um Bedrohungen effektiv abwehren zu können. Die Zusammenarbeit zwischen Sicherheitsbehörden, Infrastrukturbetreibern und innovativen Akteuren der Digitalwirtschaft muss intensiviert werden, um neue Technologien effizient zu nutzen und gleichzeitig die notwendigen Sicherheitsmaßnahmen umzusetzen.

§ 38 BPolG-E zum Einsatz mobiler Sensorträger regelt behördliche Drohnen für Bild- und Tonaufnahmen sowie für Aufklärungs- und Inspektionszwecke. Die Vorschrift sollte dahingehend präzisiert werden, dass der Einsatz solcher Systeme nur unter klaren datenschutzrechtlichen und sicherheitstechnischen Rahmenbedingungen zulässig ist. Eine Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung vor Inbetriebnahme solcher Systeme sollte gesetzlich festgeschrieben werden. Darüber hinaus sollten die Systeme nach dem Grundsatz »Datenschutz durch Technikgestaltung« betrieben werden. Dazu gehört, dass Bild- und Tonaufzeichnungen auf das erforderliche Maß beschränkt, zeitnah ausgewertet und gelöscht werden sowie Missbrauch durch geeignete organisatorische und technische Maßnahmen ausgeschlossen wird. Die Zugriffsrechte der Bediensteten sind klar zu regeln, und jeder Abruf oder jede Nutzung der aufgezeichneten Daten ist nachvollziehbar zu dokumentieren. Es sollte zudem vorgesehen werden, dass nur Systeme eingesetzt werden, deren technische Sicherheit und Funkverträglichkeit nach anerkannten Standards geprüft wurde; eine Einbindung von Fachbehörden für Informationssicherheit kann hier zur Qualitätssicherung beitragen.

§ 39 BPolG-E regelt den Einsatz technischer Mittel zur Abwehr unbemannter Luftfahrtsysteme. Bitkom empfiehlt, die mit solchen Maßnahmen verbundenen Funk-, Sicherheits- und Haftungsrisiken ausdrücklich gesetzlich zu adressieren. Systeme, die zur Signalstörung oder -übernahme eingesetzt werden, sollten einer verbindlichen Sicherheits- und Funkzertifizierung unterliegen und nur verwendet werden dürfen, wenn ihre Kompatibilität mit den luftrechtlichen und funktechnischen Vorgaben nachgewiesen ist. Für Betreiber kritischer Infrastrukturen wie Flughäfen oder Bahnanlagen sind klare Verantwortungsabgrenzungen und Haftungsfreistellungen bei behördlich angeordneten Abwehrmaßnahmen vorzusehen, um Rechtssicherheit und Kooperationsbereitschaft zu gewährleisten.

Datenweiterverarbeitung und -übermittlung

Die §§ 42 bis 47 BPolG-E regeln die Weiterverarbeitung personenbezogener Daten, die Zweckbindung, die hypothetische Datenneuerhebung sowie Anforderungen an Dokumentation und Kennzeichnung. Bitkom empfiehlt, Zweckänderungen eng auszulegen und eine hypothetische Datenneuerhebung nur unter strengen, dokumentationspflichtigen Voraussetzungen zuzulassen. Für jede Weiterverarbeitung sollte eine nachvollziehbare Begründung mit Angabe des konkreten Zwecks und der rechtlichen Grundlage erfolgen, begleitet von einer lückenlosen Protokollierung und regelmäßiger Überprüfung der Erforderlichkeit.

Die §§ 49 bis 51 BPolG-E zu Ausschreibungen, Beobachtungs- und Kontrollmaßnahmen übernehmen die bisherige Struktur der Ausschreibungs- und Beobachtungsbefugnisse weitgehend, ohne verbindliche technische Standards oder Governance-Regeln festzulegen. Bitkom empfiehlt, einheitliche Schnittstellen- und Datenformate für Verbundsysteme festzulegen, Protokollierungs- und Auditpflichten für Weitergaben zwischen Bundes- und Länderbehörden sowie europäischen Partnern vorzusehen und im Rahmen von § 106 BPolG-E jährlich Qualitätskennzahlen, etwa zu Übermittlungsfehlern, Rückmeldelatenzen und Löschquoten, zu berichten.

§ 52 BPolG-E zur Erhebung von Fluggastdaten und deren Übermittlung an die Bundespolizei regelt Pflichten von Luftfahrtunternehmen. Automatisierte Datenabgleiche sollten stets ein »Human-in-the-Loop« -Verfahren vorsehen, um Fehlzuordnungen und unbeabsichtigte Diskriminierungen zu vermeiden. Das Gesetz sollte festlegen, dass automatisierte Treffer nur nach menschlicher Überprüfung zu Maßnahmen führen dürfen. Bestehende technische Schnittstellen der Luftfahrtunternehmen sind vorrangig weiterzuverwenden; neue Gateways sollten nur eingerichtet werden, wenn ein abgestimmter Migrations- und Kompatibilitätsplan vorliegt. Dies gewährleistet technische Interoperabilität, reduziert Integrationsaufwand und stärkt die Rechtssicherheit für Unternehmen.

§ 53 BPolG-E fasst die bestehenden Befugnisse zur innerstaatlichen Datenübermittlung zusammen, ohne technische oder organisatorische Mindeststandards verbindlich festzulegen. Bitkom empfiehlt, den Paragrafen um klare Vorgaben zu Schnittstellen, Protokollierung und Zweckbindung zu ergänzen, um eine rechts- und datenschutzkonforme Zusammenarbeit zwischen Behörden und privaten Stellen sicherzustellen. Übermittlungen an nichtöffentliche Stellen sollten nur bei gesetzlicher Aufgaben- oder Vertragsermächtigung und nachgewiesenen technischen und organisatorischen Schutzmaßnahmen erfolgen. Zudem sollte jede Übermittlung im Sinne der Transparenz und Verantwortlichkeit dokumentiert werden, einschließlich Zweck, Empfänger, Rechtsgrundlage und Löschfrist.

Fazit

Die Anpassung des Bundespolizeigesetzes ist ein wesentlicher Schritt zur Stärkung der Sicherheit in Deutschland. Datenschutz und IT-Sicherheit müssen dabei konsequent berücksichtigt werden.

Bitkom setzt sich für ein ausgewogenes Verhältnis zwischen Sicherheit, Datenschutz und der Wettbewerbsfähigkeit der Anbieter ein. Die hier genannten Forderungen sind notwendig, um die rechtlichen Rahmenbedingungen zukunftssicher zu gestalten und die digitale Transformation sicher, grundrechtskonform und vertrauenswürdig voranzutreiben.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Nemo Buschmann | Referent Verteidigung & Öffentliche Sicherheit
T +49 30 27576-101 | n.buschmann@bitkom.org

Verantwortliches Bitkom-Gremium
AK Öffentliche Sicherheit