Eingriffsrecht Bayern

Polizeiliche Befugnisse zur Datenverarbeitung

von

Jürgen Teubert

VERLAG DEUTSCHE POLIZEILITERATUR GMBH
Buchvertrieb

1 Einführung

1.1 Geschichtliche Entwicklung

Der Schutz personenbezogener Informationen ist keine Erfindung der Neuzeit, sondern wird seit vielen Jahrhunderten mit Selbstverständlichkeit praktiziert. Zwar verwendete man seinerzeit und auch teilweise heute hierbei nicht den Begriff Datenschutz, im Kern aber wird er getroffen: Zu erinnern sei hier an das „Beichtgeheimnis" oder an das sog. „Bankgeheimnis"[1], eine Erläuterung dieser Begriffe erscheint hier nicht erforderlich. Eine gesetzliche Regelung des Bankgeheimnisses in Deutschland gibt es nicht, jedoch wurde seit dem 1.4.2005 mit dem „Gesetz zur Förderung der Steuerehrlichkeit" das Bankgeheimnis in Deutschland faktisch abgeschafft. Mit dem Eid des Hippokrates[2] wurde unter anderem nicht nur die kurative Verpflichtung für Mediziner, sondern auch die „ärztliche Schweigepflicht" manifestiert. Diese entfaltet sogar – bis hin zum Verhältnis Polizei und Arzt – eine Fernwirkung, wenn es um die Frage geht, wann Ärzte berechtigt oder verpflichtet sind, die ärztliche Schweigepflicht zu brechen, um geplante oder bereits begangene Straftaten anzuzeigen. So ist der Arzt nicht berechtigt, die Polizei zu verständigen, wenn der Patient während der Behandlung ein schweres Verbrechen gesteht, denn § 138 StGB gilt nur für bevorstehende Straftaten.[3]

Erwähnenswert in diesem Zusammenhang ist auch das „Recht am eigenen Bild", das im KunstUrhG aus dem Jahre 1907 geschützt wird. Doch bereits im Jahre 1871 wurde mit Inkraftsetzung des StGB das Rechtsgut des Privat- oder Fremdgeheimnisses in den §§ 203 und 204 geschützt. Später wurden die § 201a (Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen) und § 353b (Verletzung des Dienstgeheimnisses) in das StGB aufgenommen. Bemerkenswert ist, dass diese Bereiche schon sehr früh als geheimhaltungsbedürftig und schützenswert angesehen wurden.

George Orwell hat in seinem 1949 in London erschienenen Roman „1984"[4] die negative Utopie eines totalitären Überwachungsstaates im Jahre 1984 dargestellt. „Big Brother is watching you" wurde Synonym für permanente, lückenlose und anlassunabhängige staatliche Überwachung. Die Existenz des „Großen Bruders" wurde im Buch weder als wahr noch als unwahr dargestellt, letztendlich ist „er" eine Fiktion geblieben. Dass es eine lückenlose und anlassunabhängige Überwachung durch den Staat nicht geben wird, darüber wacht das Bundesverfassungsgericht über die Legislative mit kritischem Blick auf die Vereinbarkeit von Gesetzen mit dem Grundgesetz der Bundesrepublik Deutschland.[5]

Die technische Entwicklung auf dem Gebiet der EDV hatte gesetzliche Regelungen zwangsläufig zur Folge, mit denen die personenbezogenen Daten der Bürger vor unnötigen Beeinträchtigungen geschützt werden sollten. Die erste gesetzliche Regelung in Bayern wurde im „Gesetz über die Organisation der elektronischen Datenverarbeitung im Freistaat Bayern"

1 Das Bank„geheimnis" besteht de facto nicht mehr, da Auskünfte öffentlich-rechtlicher Kreditinstitute nach § 161 Abs. 1 StPO an die Staatsanwaltschaft verpflichtend sind, nicht jedoch Privatbanken; siehe auch Meyer-Goßner 2010, § 161 Rn. 4; zur Auskunft gegenüber bzw. zum Kontenabrufverfahren der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) siehe BaFinJournal 04/09 (Ausgabe April 2009) S. 3 zum Thema „Aufsichtspraxis – Kontenabruf: 150 Millionen Euro sichergestellt" unter http://www.bafin.de vom 31.10.2010.

2 Griechischer Arzt (um 460 bis 370 v. Chr.); der Eid des Hippokrates gilt als erste grundlegende Formulierung einer ärztlichen Ethik, wobei Hippokrates jedoch wohl nicht der Urheber des Eides war.

3 Schönke/Schröder 2010, § 138 StGB Rn. 8.

4 George Orwell, NINETEEN EIGHTY-FOUR, Verlag Ullstein GmbH, Frankfurt/M – Berlin – Wien 1976, Ullstein Buch Nr. 3253.

5 Siehe z.B. BVerfG, Urteil vom 2.3.2010, Az. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, zur Vorratsdatenspeicherung gemäß §§ 113a, 113b TKG und § 100g StPO.

Teubert „Eingriffsrecht Bayern", 1. Auflage 2019
ISBN 978-3-8011-0857-1

(EDVG) aus dem Jahre 1970 verfasst, mittlerweile mit Ablauf des Jahres 2001 außer Kraft getreten. Die eigentlichen Datenschutzgesetze vom Bund und dem Freistaat Bayern wurden 1977 bzw. 1978 verabschiedet.

1.2 Verfassungsrecht

Im richtungweisenden „Volkszählungsurteil" hat das BVerfG[6] zum **Grundrecht der informationellen Selbstbestimmung (RiS)** entschieden, dass „unter den Bedingungen der modernen Datenverarbeitung der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten umfasst wird" und damit „die Befugnis des Einzelnen (gewährleistet), grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". Das BVerfG hat verschiedene Ausprägungen des **Allgemeinen Persönlichkeitsrechts** gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hervorgebracht, zuletzt in seiner Entscheidung vom 27.2.2008[7] zur Online-Durchsuchung:

- Recht auf informationelle Selbstbestimmung (RiS),[8]
- Recht am gesprochenen Wort,[9]
- Recht am eigenen Bild,[10]
- Recht auf Privatsphäre,[11]
- Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[12]

Zusammenfassung

Das RiS dient dem Schutz des Bürgers vor unbegrenzter Informationserhebung, -verarbeitung und -nutzung personengebundener Daten. Es gewährt damit dem Bürger die Befugnis, grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Schranken des Persönlichkeitsschutzes

Für das Allgemeine Persönlichkeitsrecht im Sinne des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG findet zwar die **Schrankentrias** der allgemeinen Handlungsfreiheit keine unmittelbare Anwendung (a.M. vertr.), allerdings ist das RiS als Teil des Allgemeinen Persönlichkeitsrechtes nicht schrankenlos gewährleistet. Die Schrankentrias bezeichnet 3 rechtliche Schranken, die das Grundgesetz setzt für das Recht auf freie Entfaltung der Persönlichkeit und somit sowohl für die allgemeine Handlungsfreiheit als auch für das allgemeine Persönlichkeitsrecht. Diese rechtlichen Schranken sind im Einzelnen die verfassungsmäßige Ordnung, die Rechte anderer sowie das Sittengesetz. Aufgrund der Unbestimmtheit (Sit-

6 BVerfG 1. Senat, Urteil vom 15.12.1983, Az: 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83.
7 BVerfG vom 27.2.2008, Az: 1 BvR 370/07; 1 BvR 595/07.
8 BVerfGE 65, 1 (42) = NJW 1984, S. 419.
9 BVerfGE 34, 238 (246f.) = NJW 1973, S. 891; BVerfGE 54, 148 (155) = NJW 1980, S. 2070; BVerfGE 106, 28 (41) = NJW 2002, S. 3619.
10 BVerfGE 101, 361 (381) = NJW 2000, S. 1021; BVerfG, NJW 2005, S. 3271 (3271); BVerfGE 120, 180 (198) = NJW 2008, S. 1793.
11 BVerfGE 80, 367 (373 f.) = NJW 1990, S. 563; BVerfGE 101, 361 (382 f.) = NJW 2000, S. 2021; BVerfGE 120, 180 (199) = NJW 2008, S. 1793.
12 BVerfG vom 27.2.2008, Az: 1 BvR 370/07; 1 BvR 595/07.

Teubert „Eingriffsrecht Bayern", 1. Auflage 2019
ISBN 978-3-8011-0857-1

tengesetz) bzw. Ableitung aus der verfassungsmäßigen Ordnung (Rechte anderer) erlangen diese beiden Schranken neben der verfassungsmäßigen Ordnung kaum Bedeutung. Vielmehr sind Einschränkungen der informationellen Selbstbestimmung auf gesetzlicher Grundlage möglich. Der Bürger hat keine uneingeschränkte Herrschaft über seine personenbezogenen Daten. Im überwiegenden Interesse der Allgemeinheit ist ein Zugriff auf persönliche Daten des Bürgers ohne, ja sogar gegen seinen Willen zulässig. Insofern steht das RiS unter dem Vorbehalt gesetzlicher Ermächtigungen. Erforderlich ist allerdings eine gesetzliche Grundlage, die den Anforderungen der Normenklarheit genügt und eine bereichsspezifische Regelung darstellt. Spezifisch für den Bereich der Gefahrenabwehr stellen die Art. 12 bis 14 sowie 30 ff. PAG verfassungskonforme Ermächtigungsgrundlagen dar. Nach h.M. bedarf es einer Zitierung des Art. 2 Abs. 1, Art. 1 Abs. 1 GG nicht; eine Zitierung im Sinne des Art. 19 Abs. 1 GG ist daher in Art. 74 PAG nicht erforderlich.

Der bayerische Gesetzgeber hat mit der 3. Änderung des PAG (MEPolG), die am 01.10.1990 in Kraft getreten ist, diese Forderung des BVerfG im Bereich der Gefahrenabwehr umgesetzt; der Bundesgesetzgeber erst viel später, zuletzt im StVÄG 1999.

Mit Aufnahme der Befugnis zur **Online-Durchsuchung** gemäß Art. 45 in das PAG hat das BVerfG[13] den Umfang des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) um das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** erweitert und zugleich Voraussetzungen und Schranken definiert. Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen. Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen.

Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff an Art. 10 Abs. 1 GG zu messen. Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG vor, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist. Nimmt der Staat im Internet öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein.[14]

Die 3 Grundwerte der IT-Sicherheit sind Vertraulichkeit, Verfügbarkeit und Integrität.

13 BVerfG vom 27.2.2008, Az: 1 BvR 370/07; 1 BvR 595/07, Leitsätze.
14 BVerfG vom 27.2.2008, Az: 1 BvR 370/07; 1 BvR 595/07, Leitsätze.

Teubert „Eingriffsrecht Bayern“, 1. Auflage 2019
ISBN 978-3-8011-0857-1

Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken. Als **Vertraulichkeit** hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert, dass vertrauliche Informationen vor unbefugter Preisgabe geschützt werden müssen. Mit **Verfügbarkeit** wird dem Benutzer garantiert, dass Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung stehen.[15] **Integrität** bedeutet, dass Daten vollständig und unverändert sind. Der Begriff „Information" wird in der Informationstechnik für „Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z.B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung manipuliert wurde.[16]

Thema dieses Buches sind ausschließlich Eingriffe in das Allgemeine Persönlichkeitsrecht im Sinne von Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG. Unberührt davon bleiben Rechtseingriffe in Art. 10 GG, für die die Art. 42 bis 44 PAG sowie die §§ 100a, 100g, 100i StPO eine Rechtsgrundlage darstellen.

1.3 Bundesdatenschutzgesetz (BDSG)

1.3.1 Anwendungs- und Schutzbereich

Zweck des BDSG ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Nach § 1 Abs. 1 BDSG gilt es für die Verarbeitung personenbezogener Daten durch

- **öffentliche Stellen des Bundes** (sowohl Behörden [z.B. BKA, BPol, BfV] als auch sonstige öffentliche Stellen [z.B. Beliehene]),
- **öffentliche Stellen der Länder**, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie Bundesrecht ausführen oder als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt (mittlerweile haben alle deutschen Bundesländer eigene Datenschutzgesetze, insofern gilt in Bayern grundsätzlich das Bayerische Datenschutzgesetz).
- Für **nichtöffentliche Stellen** gilt das BDSG für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

Soweit bei der Verarbeitung von personenbezogenen Daten eine Einwilligung des betroffenen Bürgers vorausgeht, ist eine Rechtsgrundlage dafür entbehrlich, z.B. Einwilligung in Datenspeicherung im Rahmen eines Handy-Vertrages, Antrag für eine Kreditkarte oder Einwilligung in die SCHUFA-Auskunft bei Kreditvergabe.

§ 1 Abs. 2 BDSG regelt die **Konkurrenzen** zu speziellen Datenschutzregelungen in Rechtsvorschriften des Bundes (z.B. StPO, AufenthG, StVG), die dem BDSG vorgehen. Jedoch in Bezug auf das VwVfG geht das BDSG vor, soweit bei der Ermittlung eines Sachverhaltes personenbezogene Daten verarbeitet werden (§ 1 Abs. 3 BDSG).

15 Leitfaden Informationssicherheit des BSI, S. 14.
16 Ebenda.

Teubert „Eingriffsrecht Bayern", 1. Auflage 2019
ISBN 978-3-8011-0857-1

1.3.2 Datenschutzrechtliche Begriffe

Die Definitionen datenschutzrechtlicher Begriffe der §§ 2, 46 BDSG decken sich mit denen in der Richtlinie (EU) 2016/680, so dass an dieser Stelle auf die Ausführungen in Ziffer 1.6 verwiesen wird. Die Legaldefinitionen aus §§ 2, 46 BDSG sind für eingriffsrechtliche Begründungen nach Bundesgesetzen, z.B. StPO, bindend.

1.3.3 Sanktionsnorm

In § 43 BDSG (Ordnungswidrigkeit) ist die vorsätzliche oder fahrlässige Nichtbeachtung der Vorschriften des BDSG mit einem Bußgeld bis zu 50 000 Euro bedroht. Wer bestimmte Handlungen vorsätzlich gegen Entgelt, in Bereicherungs- oder Schädigungsabsicht begeht, erfüllt den Tatbestand eines Vergehens gem. § 42 Abs. 1 oder 2 BDSG. Die Verfolgung tritt gemäß § 42 Abs. 3 BDSG nur auf Antrag des Betroffenen ein (Antragsdelikt).

Zusammenfassung

Das BDSG gilt nur für öffentliche Stellen des Bundes, soweit keine spezielle Regelung besteht. Es gilt weiter für Privatpersonen, die personenbezogene Daten verarbeiten, nutzen oder erheben. Der unbefugte Umgang mit personenbezogenen Daten kann eine Ordnungswidrigkeit nach § 43, unter besonderen Voraussetzungen ein Vergehen nach § 42 BDSG darstellen. Für die bayerische Polizei entwickelt es kaum Anwendungsfälle aufgrund der Subsidiaritätsklausel in § 1 Abs. 1 Satz 1 Nr. 2 BDSG

1.4 Bayerisches Datenschutzgesetz (BayDSG)

1.4.1 Anwendungs- und Schutzbereich

Der **Gesetzeszweck** und damit der **Schutzbereich** des BayDSG ist, dass der Einzelne in seinem Persönlichkeitsrecht vor unzulässigem Umgang mit personenbezogenen Daten durch öffentliche Stellen geschützt wird.

Der **Anwendungsbereich** des BayDSG ist in Art. 1 Abs. 1 geregelt. Danach gilt das BayDSG für Behörden und sonstige öffentliche Stellen des Freistaates Bayern, der Gemeinden, Gemeindeverbände und der sonstigen juristischen Personen des öffentlichen Rechts, soweit sie der Aufsicht des Freistaates Bayern unterstehen. Unter den Voraussetzungen des Art. 1 Abs. 2 BayDSG gilt dieses Gesetz auch für Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen.

1.4.2 Sanktionsnorm

Art. 23 Abs. 1 BayDSG zählt konkrete, nur vorsätzlich ahndbare Tathandlungen auf und stellt auf das Tatbestandsmerkmal „unbefugt“ ab. Unbefugt handelt, wer keine entsprechende gesetzliche Ermächtigung für seinen Umgang mit den personenbezogenen Daten hat. Weiter muss es sich um Daten handeln, die „nicht offenkundig“ sind. Dies sind z.B. alle Daten über eine Person, die in Dateien der Polizei gespeichert sind, z.B. IGVP, KAN, Fahndungsdatei usw. Zuständig für die Ahndung und Verfolgung der **Ordnungswidrigkeit** gemäß Art. 23 BayDSG – begangen durch Polizeibeamte – sind die dem Bayerischen Staatsministerium des Innern,

Teubert „Eingriffsrecht Bayern“, 1. Auflage 2019
ISBN 978-3-8011-0857-1

für Sport und Integration unmittelbar nachgeordneten Polizeidienstellen (Polizeipräsidien der Bayerischen Polizei) gemäß § 91 Abs. 3 ZustV.[17] Handelt der Täter in einer bestimmten Absicht im Sinne des Art. 23 Abs. 2 BayDSG (Entgelt, Bereicherung, Schädigung), liegt ein Vergehen vor, das eine Freiheitsstrafe bis zu 2 Jahren vorsieht. Dieses **Vergehen** wird nur auf Antrag des Betroffenen verfolgt. Unbefugt ist die Datennutzung, wenn sie nicht für die polizeiliche Aufgabenerfüllung im Sinne des Art. 2 PAG notwendig ist. So ist eine Abfrage personenbezogener Daten in der Personenvollauskunft des INPOL-Bayern (Recherche z.B. im Bayerischen L-KAN und B-KAN) unzulässig, wenn diese lediglich aus Neugierde, Langeweile oder als Gefälligkeit erfolgt.

Beispiele:

Der Freundschaftsdienst
Der Personalleiter einer ortsansässigen Firma bittet einen Polizeibeamten der örtlichen PI um einen Freundschaftsdienst. Dieser recherchiert die Daten einer Bewerberin der Firma im Bayerischen L-KAN und übermittelt das Trefferergebnis dem Personalleiter. Daraufhin wird die Bewerberin abgelehnt.

Die Abfrage sowie die Weitergabe der KAN-Daten sind rechtswidrig, ebenso unzulässig wären bereits auch eindeutige verbale oder gestikulierende Andeutungen gegenüber dem Personalleiter über polizeiliche Einträge.

Mitteilung eines Negativ-Ergebnisses
Im oben genannten Beispiel wäre selbst die Mitteilung eines Negativ-Ergebnisses (kein Eintrag der Bewerberin im L-/B-KAN) an den Personalleiter nicht zulässig. Die Verletzung des Dienstgeheimnisses gemäß § 353b StGB ist grundsätzlich zu prüfen![18]

Der Tatbestand des Ausspähens von Daten gemäß § 202a StGB wird in diesem Zusammenhang nach herrschender Meinung nicht berührt, da der Polizeibeamte auf die Daten berechtigt zugreift. Eine Manipulation an der Zugangsberechtigung wird nicht vorgenommen.

Bei Verstößen gegen datenschutzrechtliche Bestimmungen stehen folgende Sanktionsnormen zur Disposition:

- § 202a StGB – Ausspähen von Daten,
- § 202b StGB – Abfangen von Daten,
- § 202c StGB – Vorbereiten des Ausspähens und Abfangen von Daten,
- § 202d StGB – Datenhehlerei
- § 203 StGB – Verletzung von Privatgeheimnissen,
- § 353b Abs. 1 StGB – Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht,
- Art. 23 Abs. 1, 2 BayDSG.

Zusammenfassung

Das BayDSG gilt für alle Behörden und öffentliche Stellen des Freistaates Bayern sowie der Gemeinden, Gemeindeverbände und juristische Personen des öffentlichen Rechts, soweit sie der Aufsicht des Freistaates Bayern unterstehen. Soweit im PAG oder sonstigen Rechtsvorschriften spezielle Regelungen bestehen, ist das BayDSG subsidiär. Die Sanktionsnorm des Art. 23 BayDSG ist auch für den Bereich des PAG relevant.

17 Zuständigkeitsverordnung vom 16.6.2015, GVBl Nr. 7/2015, S. 184.
18 Siehe auch BGH v. 23.3.2001, 2 StR 488/00.

Teubert „Eingriffsrecht Bayern“, 1. Auflage 2019
ISBN 978-3-8011-0857-1

1.5 Konkurrenzen zum Bayerischen PAG

1.5.1 Verhältnis PAG – BayDSG

Art. 1 Abs. 5 und 6 BayDSG enthalten Vorrangregelungen. Die Regelungen der Art. 30 ff. PAG gehen den Bestimmungen des BayDSG vor! Das BayDSG ist gegenüber dieser bereichsspezifischen Regelung subsidiär.

Zusammenfassung

Enthält das PAG jedoch keine spezielle Regelung, dann kommt das BayDSG zur Anwendung. Die klare Konkurrenzabgrenzung des Art. 66 PAG erleichtert eine Beurteilung. Das bedeutet nun für die Praxis: Für das PAG gilt die Sanktionsnorm des Art. 23 BayDSG.

Beispiel:

Neuer Freund der Tochter

Die Tochter von PHK A hat einen neuen Freund. Um zu wissen, mit wem es seine Tochter zu tun hat, führt er ohne dienstlichen Anlass eine Abfrage im L- und B-KAN durch. Der neue Freund ist offensichtlich „in Ordnung". PHK A erzählt niemanden von diesem vorgenommenen Datenabgleich.

Lösungsanhalt

Die KAN-Abfrage ist nur unter den Voraussetzungen des Art. 61 Abs. 1 Satz 1 oder 2 PAG zur Gefahrenabwehr bzw. im Rahmen der Straf-/OWi-Verfolgung nach § 98c StPO zulässig. Die dort geforderten Voraussetzungen liegen nicht vor, eine Befugnis steht nun PHK A nicht zur Seite. Er handelt deshalb unbefugt. Der Datenabgleich ist rechtswidrig!

Hinweis

Das PAG enthält keine speziellen Regelungen bezüglich unberechtigter Abfragen. Es gelten dafür gemäß Art. 66 PAG die Bestimmungen des BayDSG. PHK A hat vom BayDSG geschützte, nicht offenkundige personenbezogene Daten entgegen Art. 61 Abs. 1 PAG im Sinne des Art. 23 Abs. 1 Nr. 1 Buchst. c BayDSG abgerufen und kann deswegen mit einer Geldbuße bis 30 000 Euro belegt werden. Zuständige Ahndungs- und Verfolgungsbehörde ist gemäß § 91 Abs. 3 ZustV das für PHK A zuständige bayerische Polizeipräsidium.

1.5.2 Verhältnis PAG – weitere spezielle Rechtsvorschriften

Neben den Regelungen des **BDSG** und denen des **BayDSG** gibt es in einer Vielzahl von Gesetzen **spezielle datenschutzrechtliche Regelungen**. Das BDSG findet praktisch für den bayerischen Polizeibereich keine Anwendung, da für bayerische Behörden das BayDSG Vorrang hat. Soweit jedoch im PAG oder in anderen Rechtsvorschriften spezielle Befugnisse vorhanden sind, gehen diese dem BayDSG vor. Spezialgesetzliche Regelungen außerhalb des PAG finden sich z.B. in

- StPO, OWiG,
- § 87 AufenthG (Datenübermittlung an die Ausländerbehörde),
- §§ 67 ff. SGB X (Schutz der Sozialdaten),
- §§ 35 ff. StVG (Auskunft aus dem Zentralen Fahrzeugregister),
- § 34 BMG (Datenübermittlung aus dem Melderegister),
- Art. 9 BayVersG (Bild- und Tonaufnahmen oder -aufzeichnungen durch die Polizei),
- Art. 24 BayVSG (Datenübermittlung an das Bayerische LfV),
- Art. 7 ff. UnterbrG (Verständigungspflichten),
- BKAG, SDÜ.

Teubert „Eingriffsrecht Bayern", 1. Auflage 2019
ISBN 978-3-8011-0857-1

Diese oben genannten Regelungen gehen wiederum den Bestimmungen des PAG vor! Nicht immer werden dabei typische Begriffe des Datenschutzes verwendet, so dass der Bezug zum Datenschutz nicht immer leicht hergestellt werden kann. Formulierungen wie „... sind zu informieren ...“ oder „... zu verständigen ...“ oder „... haben dem Jugendamt unverzüglich mitzuteilen ...“ deuten z.B. auf eine Datenübermittlung hin. Obwohl das PAG auch Befugnisse zur Datenübermittlung anbietet, gehen diese speziellen Regelungen dem PAG vor!

Beispiel:

Mitteilung an die Ausländerbehörde

Eine Polizeistreife stellt einen Ausländer fest, der sich schon längere Zeit ohne erforderliche Aufenthaltstitel in der Bundesrepublik aufhält. Dies stellt bei vorsätzlichem Handeln ein Vergehen nach §§ 4 Abs. 1 Satz 1, 95 Abs. 1 Nr. 2 AufenthG dar.

Gem. § 87 Abs. 2 Nr. 1 AufenthG haben öffentliche Stellen, somit auch die Polizei, unverzüglich die zuständige Ausländerbehörde über den illegalen Aufenthalt des Ausländers zu unterrichten. Die dabei zwangsläufig erforderliche Übermittlung personenbezogener Daten ist dabei beinhaltet. Es kommt somit für diese Datenübermittlung nicht Art. 56 Abs. 1 Nr. 2 PAG, sondern nur § 87 Abs. 2 Nr. 1 AufenthG als Rechtsgrundlage in Betracht.

§ 87 Abs. 2 AufenthG enthält eine Befugnis, aus der wiederum auf die spezielle Aufgabe i.S.d. Art. 2 Abs. 4 PAG i. V. m. § 87 Abs. 2 AufenthG geschlossen werden darf.

Zusammenfassung

Spezielle Regelungen des Datenschutzes in anderen Rechtsvorschriften gehen dem PAG vor. Gegenüber dem BayDSG hat das PAG Vorrang, soweit dort spezielle Regelungen enthalten sind.

1.6 Datenschutzrechtliche Begriffe

Datenschutzrechtliche Begriffsdefinitionen sind in der Richtlinie (EU) 2016/680 sowie im BDSG erläutert. Im BayDSG sowie im PAG finden sich deshalb keine Definitionen.

1.6.1 Datensicherheit, Datensicherung und Datenschutz

Mit **Datensicherheit** wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein anderer Begriff dafür ist „Informationssicherheit“.

Vertraulichkeit: Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.

Verfügbarkeit: Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.

Integrität: Die Daten sind vollständig und unverändert. Der Begriff „Information“ wird in der Informationstechnik für „Daten“ verwendet, denen je nach Zusammenhang bestimmte Attribute, wie z.B. Autor oder Zeitpunkt der Erstellung, zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung manipuliert wurde.

Teubert „Eingriffsrecht Bayern“, 1. Auflage 2019
ISBN 978-3-8011-0857-1

Bei einer **Datensicherung** (engl. Backup) werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt. Schutzobjekt ist die Hard- und Software. Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass eine EDV-technische Anlage und die dort vorhandenen personenbezogenen Daten vor unberechtigtem Zugriff gesichert werden. Dazu hat der bayerische Gesetzgeber in Art. 32 BayDSG (Anforderungen an die Sicherheit der Verarbeitung) Maßnahmen zur Datensicherung formuliert. So wird z.B. die geforderte Zugangskontrolle in Form von Benutzerkennung und Passwort umgesetzt. Mit der Zugriffskontrolle werden die Anwender nur für die Anwendungen berechtigt, die für die berufliche Aufgabenerfüllung erforderlich sind. Bei der Bayer. Polizei werden z.B. die Zugriffsrechte für INPOL-Bayern oder IGVP in der bayerischen Beschäftigtendatenbank (BDB) vergeben. Weitere Definitionen sind in den Regelungen zur Datenträger-, Speicher-, Benutzer-, Transport-, Übertragungs-, Eingabe- und Auftragskontrolle zu finden.

Unter **Datenschutz** versteht man den Schutz personenbezogener Daten vor dem Missbrauch durch Dritte (nicht zu verwechseln mit Datensicherheit).[19] Schutzobjekt ist der Mensch mit seinen personenbezogenen Daten. Die Wahrung des Rechts auf informationelle Selbstbestimmung (RiS) lebender Menschen kann nur gewährleistet werden, wenn entsprechende Maßnahmen zur Datensicherung und Datensicherheit getroffen wurden. Die Ausführungen zum RiS sind im Abschnitt 1.2 Verfassungsrecht zu finden.

Die folgenden Erläuterungen **datenschutzrechtlicher Begriffe** sind abschließend im Art. 3 Richtlinie (EU) 2016/680 definiert und sind auch für das PAG unmittelbar anwendbar! Da das PAG und auch die Vollzugsbekanntmachung zum PAG weitestgehend auf datenschutzrechtliche Begriffsdefinitionen verzichten, können diese Definitionen aus Art. 3 Richtlinie (EU) 2016/680 für eine eingriffsrechtliche Begründung nach dem PAG herangezogen werden.

1.6.2 Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.[20] Personenbezogene Daten sind somit Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen.

- Einzelangaben sind alle Informationen zu einer Person, die geeignet sind, Rückschlüsse auf diese zu ziehen, d. h. sie zu bestimmen oder bestimmbar zu machen, z.B. Name, Adresse, Telefon-, Ausweis-, Versicherungsnummer, Kfz-Kennzeichen.
- Persönliche Verhältnisse sind Angaben über den Betroffenen selbst, seine Identifizierung und Charakterisierung, z. B. Familienstand, Staatsangehörigkeit, Beruf, Konfession, Erscheinungsbild, besondere körperliche Merkmale, Werturteile, so auch Fotografien, Videoaufzeichnungen, Fingerabdrücke, Röntgenbilder, DNA-Status.

19 BSI (Hrsg.), Leitfaden Informationssicherheit, Stand: Februar 2012, S. 14.
20 Art. 3 Nr. 1 Richtlinie (EU) 2016/680.

Teubert „Eingriffsrecht Bayern“, 1. Auflage 2019
ISBN 978-3-8011-0857-1

- Sachliche Verhältnisse sind Angaben über einen auf den Betroffenen beziehbaren Sachverhalt, z.B. ein Pkw-Aufkleber mit Ausdruck einer politischen Meinung oder einer Einstellung zu einem Sachverhalt. Zwar handelt es sich im Kern um sachbezogene Daten, diese lassen aber Rückschlüsse auf eine Person zu.

Zusammenfassung

Alle Daten, die einer konkreten Person zugeordnet werden können und daher mit dieser Person im unmittelbaren Zusammenhang stehen, sind personenbezogene Daten.

Im Zweifelsfall ist zugunsten des Betroffenen vom Vorliegen einer Personenbezogenheit der Daten auszugehen, was auch unmittelbaren Einfluss auf die spätere (eingriffs-)rechtliche Beurteilung eines Sachverhaltes hat.

Daten **juristischer Personen** (z.B. Firma X) und nicht rechtsfähiger Personenvereinigungen sind vom Begriff der personenbezogenen Daten nicht umfasst, es sei denn, sie enthalten Angaben über natürliche Personen (z.B. Vorstandsvorsitzender der Firma X).

Die Daten **Verstorbener** fallen nicht unter den Schutzbereich des RiS. Der Umgang mit diesen Daten wird im § 189 StGB geschützt.

Für **behördeninterne personenbezogene Daten**, z.B. die Urlaubsplanung, Liste über zugeteilte Waffen, Personalakten usw. (sog. Verwaltungsdateien) gelten natürlich nicht die Bestimmungen des PAG, sondern die des BayDSG bzw. der beamtenrechtlichen Gesetze. Hiervon zu unterscheiden sind „Polizeidateien" (z.B. IGVP, KAN), die zur Wahrnehmung der Aufgaben nach Art. 2 PAG eingerichtet werden. Hierunter können auch die personenbezogenen Daten Verstorbener subsumiert werden.

1.6.3 Behörde, öffentliche Stelle und nichtöffentliche Stelle

Da in den Befugnisvorschriften des PAG zuweilen neben der öffentlichen Stelle auch die Behörde genannt wird, sind diese beiden Begriffe zunächst zu unterscheiden.

Behörde ist jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt (§ 1 Abs. 4 VwVfG, § 1 Abs. 2 SGB X), wobei hier der funktionale Behördenbegriff gemeint ist, da die Funktion der öffentlichen Aufgaben ausschlaggebend sein soll.

Öffentliche Stellen nehmen nun auch (tatsächlich) Aufgaben der öffentlichen Verwaltung wahr, ohne Behörde zu sein (z.B. gesetzliche Krankenversicherer, Bezirkskaminkehrer im Rahmen der Feuerstättenmessung nach 1. BImSchV, Werksfeuerwehr bei Brandeinsätzen). § 2 Abs. 2 BDSG definiert öffentliche Stellen der Länder als die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes oder sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

Nichtöffentliche Stellen sind gemäß § 2 Abs. 4 BDSG natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 des BDSG fallen. Nimmt eine nichtöffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes (siehe Erläuterungen hierzu unter öffentliche Stellen).

Teubert „Eingriffsrecht Bayern", 1. Auflage 2019
ISBN 978-3-8011-0857-1

1.6.4 Datei

Eine **automatisierte Datei** ist eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann. Kernelement automatisierter Dateien ist der Einsatz von EDV-Technik, d. h. personenbezogene Daten werden in elektronischer Form gespeichert und zur Verfügung gestellt. Das Dateiformat (Word, Excel, PDF, PowerPoint etc.) oder das Datenbanksystem (Access, Oracle, Informix etc.) spielt dabei keine Rolle.

Im Unterschied dazu können dieselben personenbezogenen Daten in **nicht automatisierten Dateien** angelegt werden, das ist jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann. Hier kommt dagegen keine EDV zum Einsatz, die Daten werden konventionell in manuell geführten Handkarteien, -registern oder Papierordnern zusammengeführt. Eingriffsrechtlich spielt diese Unterscheidung keine wesentliche Rolle, vielmehr jedoch im Rahmen der Prüfung der Genehmigungszuständigkeit zum Führen einer Datei.

Als **Dateisystem** bezeichnet § 46 Nr. 6 BDSG jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

Nicht unter den Begriff Datei gehören **Akten und Aktensammlungen**, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können. Akten sind alle sonstigen amtlichen oder dienstlichen Zwecken dienenden Unterlagen, dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

1.6.5 Datenverarbeitung

Nach Art. 3 Nr. 2 Richtlinie (EU) 2016/680 (§ 46 Nr. 2 BDSG) beinhaltet die Verarbeitung jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Das dabei angewandte Verfahren spielt keine Rolle. Wichtige Inhalte der Datenverarbeitung werden im Folgenden erläutert:

- **Erheben** ist das (aktive) Beschaffen von Daten über Betroffene. Diese Aktivität spiegelt sich in den damit verbundenen Tätigkeiten wider, z.B. gezieltes Beobachten, Nachfragen, Anrufen, Befragen, Foto- und Videografieren. Erhält die Polizei unaufgefordert personenbezogene Daten, ohne diese „anzunehmen", (also ohne Speicherung, Nutzung usw.), dann liegt kein Rechtseingriff in das RiS dieser Personen vor, die Polizei hat von sich aus nicht (aktiv) in das RiS des Betroffenen eingegriffen.
- **Speichern** ist das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung.
- **Verändern** ist das inhaltliche Umgestalten gespeicherter personenbezogener Daten.

ISBN 978-3-8011-0857-1

- **Übermitteln** ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an Dritte in der Weise, dass
  - die Daten durch die speichernde Stelle an Dritte weitergegeben werden oder
  - Dritte Daten einsehen oder abrufen, die von der speichernden Stelle zur Einsicht oder zum Abruf bereitgehalten werden.
- Den **Datenabgleich** als speziell geregelte Form der Datenübermittlung regeln Art. 46 und 61 PAG.
- **Sperren** ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.
- **Löschen** ist das Unkenntlichmachen gespeicherter personenbezogener Daten.
- **Datennutzung** jede Verwendung personenbezogener Daten. Darunter fällt insbesondere die Weitergabe von personenbezogenen Daten innerhalb derselben Polizeidienststelle (z. B. tägliche Lagebesprechung).

Beispiele:

Abgrenzung zur Datenerhebung
Ein Bürger kommt zur Polizeiinspektion und legt eine Liste mit 20 Kennzeichen von Fahrzeugen vor, die im Halteverbot stehen. Datenerhebung aus Sicht der Polizei ist nicht gegeben. Werden daraufhin jedoch Maßnahmen ergriffen (gebührenpflichtige Verwarnung, Speicherung im IGVP), dann sind für diese Nutzung bzw. Speicherung personenbezogener Daten (Kfz-Kennzeichen) Befugnisse zu prüfen.

„Schlicht-hoheitliches Handeln"
Eingriffsrechtlich ist der Begriff „Datenerhebung" auch nicht zu eng auszulegen. Wenn z.B. während einer Streifenfahrt kurzzeitig und ohne besonderen Aufwand eine Person beobachtet wird, um festzustellen, ob von ihr eine Gefahr ausgeht, dann ist das zwar noch von der allgemeinen Aufgabenwahrnehmung des Art. 2 Abs. 1 PAG gedeckt und bedarf aufgrund des „schlicht-hoheitlichen Handelns" der Polizei keiner gesetzlichen Rechtfertigung nach Art. 30 ff. PAG.

Zusammenfassung
Der Datenspeicherung geht immer eine Datenerhebung bzw. Datenübermittlung voraus. Diese Begriffe sind voneinander zu unterscheiden. Während die Datenerhebung in den Art. 31 bis 52 PAG geregelt ist, enthalten die Art. 53 und 54 PAG Regelungen über die Speicherung, Veränderung und Nutzung, die Art. 55 bis 61 PAG die Übermittlung inklusive Abgleich und Art. 62 PAG die Berichtigung, Löschung und Sperrung.

1.6.6 Weitere Begriffe zum Datenschutz[21]

- **Profiling** ist jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.
- **Pseudonymisierung** ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr

21 Vgl. Art. 3 Richtlinie (EU) 2016/680.

Teubert „Eingriffsrecht Bayern", 1. Auflage 2019
ISBN 978-3-8011-0857-1

einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

- **Anonymisieren** ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Dies spielt insbesondere bei der Verwendung personenbezogener Daten zu Schulungszwecken eine Rolle (siehe hierzu Art. 54 Abs. 4 PAG).
- **Genetische Daten** sind personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.
- **Biometrische Daten** mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.
- **Gesundheitsdaten** sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.
- **Besondere Kategorien personenbezogener Daten** sind
  - Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
  - genetische Daten,
  - biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
  - Gesundheitsdaten und
  - Daten zum Sexualleben oder zur sexuellen Orientierung.
- **Speichernde Stelle** ist jede öffentliche Stelle, die personenbezogene Daten für sich selbst speichert oder durch andere im Auftrag speichern lässt. Insbesondere Auskünfte aus Dateien dürfen grundsätzlich nur durch diese Stellen erteilt werden, so werden beispielsweise Auskünfte aus dem B-KAN durch das BKA erteilt, obwohl die angelieferten Daten auch aus den Bundesländern, z.B. Bayern stammen.
- **Dritte** sind alle Personen oder Stellen außerhalb der speichernden Stelle. Dritte sind nicht die Betroffenen sowie diejenigen Personen und Stellen, die im Inland oder innerhalb der Mitgliedstaaten der Europäischen Union personenbezogene Daten im Auftrag erheben, übermitteln oder sonst verarbeiten. Diese Personenart spielt insbesondere dann eine Rolle, wenn personenbezogene Daten insbesondere automatisiert bzw. technisch unterstützt erhoben werden, z.B. Telekommunikationsüberwachung, Foto- und Videografie, Lauschangriff. Der Gesetzgeber hat für diese Maßnahmen in den gesetzlichen Regelun-

Teubert „Eingriffsrecht Bayern“, 1. Auflage 2019
ISBN 978-3-8011-0857-1

gen jeweils den sog. unvermeidbaren bzw. unvermeidlichen Dritten mit aufgenommen. Gespräche, Lichtbilder etc. dieser Personen werden zwar zwangsläufig mit aufgezeichnet (erhoben), sind jedoch nicht Zieladressat der Maßnahme. Die Rechtmäßigkeit einer Maßnahme wird davon nicht berührt.

1.6.7 Relevanz bei Rechtsprüfungen

Im Rahmen materiell-rechtlicher Beurteilungen nach dem PAG können grundsätzlich immer die Definitionen aus Art. 3 Richtlinie (EU) 2016/680 herangezogen werden. Zwingend erforderlich sind sie jedoch dann, wenn Zweifel hinsichtlich des Vorliegens bestehen. Sie erfüllen jedoch nie den Status einer wesentlichen Formvorschrift für eine Befugnis, sondern dienen lediglich der Erläuterung! Für Rechtsprüfungen nach der StPO gelten analog die Definitionen aus § 46 BDSG.

Beispiele:

Funkfahndung
Im Rahmen einer Vermisstenfahndung führt der DGL eine Funkdurchsage mit der Bitte um Mitfahndung durch. Dazu werden die Personalien der vermissten Person sowie eine kurze Personenbeschreibung samt aktueller Bekleidung an die Streifenfahrzeuge im polizeilichen Funkverkehrskreis mitgeteilt.

Lösungsanhalt
Hier werden personenbezogene Daten der vermissten Person an andere Polizeidienststellen weitergegeben. Es handelt sich um eine Datenverarbeitung in Form der Datenübermittlung innerhalb des öffentlichen Bereichs. Diese ist gem. Art. 56 Abs. 1 Nr. 1 PAG zulässig, weil dies zur Erfüllung einer polizeilichen Aufgabe, nämlich dem raschen Auffinden der vermissten Person, erforderlich ist. Der DGL ist gem. Art. 55 Abs. 1 Satz 1 PAG für die Rechtmäßigkeit dieser Datenübermittlung verantwortlich.
Die Erläuterungen der Begriffe „personenbezogenen Daten“ und „Datenübermittlung“ können nun aus Art. 3 Nr. 1 und 2 Richtlinie (EU) 2016/680 herangezogen werden.

Teubert „Eingriffsrecht Bayern“, 1. Auflage 2019
ISBN 978-3-8011-0857-1