

Eingriffsrecht Bayern

**Polizeiliche Befugnisse
zur Datenverarbeitung**

von
**Stefan Heißenhuber,
Thomas Scheuring
und
Jürgen Teubert**



VERLAG DEUTSCHE POLIZEILITERATUR GMBH
Buchvertrieb

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

www.VDPolizei.de

2. Auflage 2026

© VERLAG DEUTSCHE POLIZEILITERATUR GMBH Buchvertrieb;

Forststr. 3a, 40721 Hilden, 2026

E-Mail: service@vdpolizei.de

Alle Rechte vorbehalten

Satz: VDP GMBH Buchvertrieb, Hilden

Druck und Bindung: C.H.Beck, Nördlingen

Printed in Germany

ISBN 978-3-8011-0947-9

© VERLAG DEUTSCHE POLIZEILITERATUR GMBH Buchvertrieb, Hilden
Heißenhuber • Scheuring • Teubert, „Eingriffsrecht Bayern“, 2. Auflage 2026
ISBN 978-3-8011-0947-9

Vorwort zur Neuauflage 2026

Jürgen Teubert hat dieses Buch mit großem Engagement entworfen. Diese gute Arbeit versuchen wir fortzuführen. Aktualisierungen und Ergänzungen wurden insbes. durch die PAG Novellen 2021 (insbes. Art. 11a Abs. 2, Art. 13 Abs. 1 Nr. 4, Art. 14 Abs. 3, 4, Art. 20 Abs. 2 S. 2, Art. 32a, 33 Abs. 4 S. 5, 60a, Art. 94 ff PAG) und 2024 (insbes. Art. 16, 29, 33 Abs. 10, 36 Abs. 4, 41, 44, 45, 49, 61a PAG) erforderlich.

Besonders bedanken möchten wir uns bei Herrn Ltd. Polizeidirektor Konrad Stangl für seinen Gastbeitrag zum Versammlungsrecht.

Für Anregungen und Verbesserungsvorschläge sind wir sehr dankbar:

thomas.scheuring@pol.hfoed.bayern.de

bzw.

stefan.heissenhuber@pol.hfoed.bayern.de

Stefan Heißenhuber und Thomas Scheuring

Hochschule für den öffentlichen Dienst in Bayern – Fachbereich Polizei

Kastl, Frühjahr 2026

Inhaltsverzeichnis

Vorwort zur Neuauflage 2026	5
Literaturverzeichnis	15
Abkürzungsverzeichnis	18
Symbolik	26
1 Einführung.....	29
1.1 Geschichtliche Entwicklung.....	29
1.2 Verfassungsrecht	30
1.3 Allgemeine Systematik des Datenschutzrechts	31
1.4 Bundesdatenschutzgesetz (BDSG).....	32
1.4.1 Anwendungs- und Schutzbereich	32
1.4.2 Datenschutzrechtliche Begriffe	33
1.4.3 Sanktionsnorm	33
1.5 Bayerisches Datenschutzgesetz (BayDSG).....	33
1.5.1 Anwendungs- und Schutzbereich	33
1.5.2 Datenschutzrechtliche Begriffe	34
1.5.3 Sanktionsnorm	34
1.6 Konkurrenzen zum Bayerischen PAG	35
1.6.1 Verhältnis PAG – BayDSG.....	35
1.6.2 Verhältnis PAG – weitere spezielle Rechtsvorschriften.....	36
1.7 Datenschutzrechtliche Begriffe	37
1.7.1 Datensicherheit, Datensicherung und Datenschutz	37
1.7.2 Personenbezogene Daten.....	38
1.7.3 Behörde, öffentliche Stelle und nichtöffentliche Stelle	39
1.7.4 Datei	39
1.7.5 Datenverarbeitung	39
1.7.6 Weitere Begriffe zum Datenschutz	41
1.7.7 Relevanz bei Rechtsprüfungen	42
2 Bayerisches Polizeiaufgabengesetz	43
2.1 III. Abschnitt Datenverarbeitung	45
2.1.1 Art. 30 PAG – Allgemeine Grundsätze	45
2.1.2 Art. 31–32a PAG Datenerhebung	47
2.1.2.1 Abgrenzung der Art. 12–14 bzw. Art. 33–52 PAG	47
2.1.2.2 Art. 31 PAG – Grundsätze der Datenerhebung.....	49
2.1.2.3 Art. 32 PAG – Generalklausel zur Datenerhebung.....	52
2.1.2.3.1 Definition Datenerhebung.....	52
2.1.2.3.2 Überblick zu Art. 32 PAG	53
2.1.2.3.3 Prüfungsschema bzw. Befugnisvoraussetzungen zu Art. 32 Abs. 1 PAG.....	54

2.1.2.3.4	Erörterungen zu Art. 32 Abs. 1 PAG.....	54
2.1.2.3.5	Formulierungsbeispiele zu Art. 32 Abs. 1 PAG.....	57
2.1.2.3.6	Art. 32 Abs. 2 PAG.....	59
2.1.2.4	Art. 32a PAG – Molekulargenetische Untersuchung bei Spurenmaterial unbekannter Herkunft	61
2.1.2.4.1	Allgemeine Ausführungen	61
2.1.2.4.2	Abgrenzungen:	62
2.1.2.4.3	Prüfungsschema und zu prüfende Maßnahmen	62
2.1.2.4.4	Beispiele	63
2.2	Besondere Befugnisse und Maßnahmen der Datenerhebung (Art. 33–52 PAG)	65
2.2.1	Art. 33 PAG – Offene Bild- und Tonaufnahmen	65
2.2.1.1	Öffentliche Veranstaltungen und Ansammlungen, Art. 33 Abs. 1 PAG.....	66
2.2.1.1.1	Absatz 1 Nr. 1 Bild- und Tonaufnahmen oder -aufzeichnungen bei öffentlichen Veranstaltungen und Ansammlungen von den Verantwortlichen einer Gefahr	66
2.2.1.1.2	Absatz 1 Nr. 2: Übersichtsaufnahmen bzw. -aufzeichnungen.....	70
2.2.1.2	Art. 33 Abs. 2 PAG – Konkrete Gefahren, drohende Gefahren für ein bedeutsames Rechtsgut und „gefährliche Orte“	72
2.2.1.3	Art. 33 Abs. 3 „Gefährdete Objekte“	73
2.2.1.4	Art. 33 Abs. 4 PAG „Bodycam, Dashcam“	74
2.2.1.5	Art. 33 Abs. 5 PAG – Intelligente Systeme	81
2.2.1.6	Art. 33 Abs. 6 – Hinweispflicht	82
2.2.1.7	Art. 33 Abs. 7 PAG – Dritte.....	82
2.2.1.8	Art. 33 Abs. 8 – Speicherdauer und Nutzungsrechte.....	82
2.2.1.9	Art. 33 Abs. 9 PAG – Abgrenzung zu Art. 9 BayVersG	83
2.2.1.10	Art. 33 Abs. 10 PAG – Zugriff auf außerpolizeiliche Videoüberwachung.....	83
2.2.1.11	Formulierungsbeispiele zu Art. 33 PAG	84
2.2.1.12	Exkurs: Art. 24 BayDSG (i.V.m. Art. 6 DSGVO).....	88
2.2.2	Elektronische Aufenthaltsüberwachung nach Art. 34 PAG.....	89
2.2.2.1	Allgemeine Erläuterungen und Abgrenzungen	89
2.2.2.2	Erläuterungen zum Tatbestand	90
2.2.2.3	Beispiel:	92
2.2.3	Postsicherstellung, Art. 35 PAG	93
2.2.3.1	Allgemeine Ausführungen und Abgrenzungen:.....	93
2.2.3.2	Erläuterungen zum Tatbestand und den Förmlichkeiten	94
2.2.3.3	Beispiel	96
2.2.4	Art. 36 PAG – Besondere Mittel der Datenerhebung	97
2.2.4.1	Überblick zu Art. 36 PAG incl. der Förmlichkeiten	97
2.2.4.2	Art. 36 Abs. 1 Nr. 1 – Längerfristige Observation	100
2.2.4.3	Art. 36 Abs. 1 Nr. 2a – Verdeckter Einsatz technischer Mittel zum Abhören oder zur Aufzeichnung des nichtöffentlich gesprochenen Wortes.....	104

2.2.4.4	Art. 36 Abs. 1 Nr. 2b/c – Verdeckter Einsatz techn. Mittel zur Feststellung des Standortes oder der Bewegung einer Person oder einer beweglichen Sache	106
2.2.4.5	Art. 36 Abs. 1 Nr. 2d/e – Verdeckter Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen oder -aufzeichnungen	108
2.2.5	Art. 37 PAG – Einsatz verdeckter Ermittler (VE).....	111
2.2.5.1	Einleitende Ausführungen zu verdeckten Ermittlern	111
2.2.5.2	Vom VE sind die „nicht offen ermittelnden Polizeibeamten“ (NoeP) zu unterscheiden	112
2.2.5.3	Internet-VE bzw. Internet-NoeP u.a.....	113
2.2.5.4	Überblick zum Tatbestand des Art. 37 PAG	115
2.2.5.5	Formvorschriften	118
2.2.5.6	Beispiele	119
2.2.6	Art. 38 PAG – Einsatz von Vertrauenspersonen.....	122
2.2.6.1	Überblick zum Tatbestand.....	122
2.2.6.2	Grundrechtssichernde Verfahrensregelungen	126
2.2.6.3	Beispiel zum Einsatz einer Vertrauensperson.....	127
2.2.6.4	Inanspruchnahme von Informanten (Definition und Rechtsgrundlage).....	128
2.2.7	Art. 39 PAG – Automatisierte Kennzeichenerkennungssysteme (AKE).....	128
2.2.7.1	Allgemeine Ausführungen zur AKE.....	128
2.2.7.2	Erläuterungen zum Tatbestand	129
2.2.7.3	Anwendungsfälle für Art. 13 Abs. 1 Nrn. 1 bis 5 PAG	131
2.2.7.4	Beispiel	131
2.2.8	Art. 40 PAG – Polizeiliche Beobachtung oder gezielte Kontrolle	132
2.2.8.1	Allgemeine Erläuterungen.....	132
2.2.8.2	Abgrenzung:	134
2.2.8.3	Erläuterungen zum Tatbestand des Art. 40 PAG.....	134
2.2.8.4	Beispiel	138
2.2.9	Art. 41 PAG – Einsatz technischer Mittel in Wohnungen.....	140
2.2.9.1	Art. 41 PAG – Erläuterungen zum Tatbestand	140
2.2.9.2	Zusammenfassende Darstellung	145
2.2.9.3	Förmlichkeiten und Verwendungsbeschränkungen	146
2.2.9.4	Personenschutzmaßnahme (PSM) – Personenschutzsender (PSS), Art. 41 Abs. 1 S. 1, Abs. 6 PAG	147
2.2.9.5	Beispiel: Personenschutzsender (PSS) bei Verdecktem Ermittler innerhalb Wohnung.....	149
2.2.9.6	Verwendung für andere Zwecke Art. 48 Abs. 4 S. 2 PAG	150
2.2.10	Art. 45 PAG – Verdeckter Zugriff auf informationstechnische Systeme.....	150
2.2.10.1	Allgemeine Erläuterungen.....	150
2.2.10.2	Verfassungsrechtliche Erläuterungen und Abgrenzungen.....	151
2.2.10.3	VIS-Eingriffe außerhalb einer Onlinedurchsuchung	153

2.2.10.4	Übersicht zum Tatbestand des Art. 45 PAG	154
2.2.10.5	Erläuterungen zum Tatbestand	155
2.2.10.6	Verwendungsbeschränkungen und Förmlichkeiten	157
2.2.11	Art. 46 PAG – Rasterfahndung	159
2.2.11.1	Historie	159
2.2.11.2	Allgemeine Erläuterungen	159
2.2.11.3	Abgrenzungen	160
2.2.11.4	Art. 46 PAG – Erläuterungen zum Tatbestand	161
2.2.12	Art. 47 PAG – Unbemannte Luftfahrtsysteme (Drohnen)	162
2.2.13	Art. 47a PAG – Überwindung besonderer Sicherungen	163
2.2.13.1	Allgemeine Ausführungen und Abgrenzungen	163
2.2.13.2	Erläuterungen zum Tatbestand	165
2.2.14	Art. 48 PAG – Weiterverarbeitung von Daten, Datenübermittlung, Kennzeichnung und Sicherung	166
2.2.14.1	Allgemeines zur Zweckänderung	166
2.2.14.2	Erläuterungen zum Tatbestand	166
2.2.14.3	Beispiele	171
2.2.15	Art. 49 PAG – Berufsgeheimnisträger und Kernbereichsdaten	171
2.2.15.1	Allgemeines zu Art. 49 PAG	171
2.2.15.2	Erläuterungen zu den einzelnen Bestimmungen	172
2.2.16	Art. 50 PAG – Benachrichtigungspflichten	176
2.2.17	Art. 51 PAG Protokollierung und Kontrolle durch den Bayerischen Landesbeauftragten für den Datenschutz	178
2.2.18	Art. 52 PAG – Parlamentarische Kontrolle und Unterrichtung der Öffentlichkeit	180
2.3	Datenspeicherung, -übermittlung und sonstige Datenverarbeitung	181
2.3.1	Art. 53 PAG	181
2.3.1.1	Erläuterungen zu den Begriffen	181
2.3.1.2	Überblick zu Art. 53 PAG	183
2.3.2	Art. 54 PAG – Speicherung, Veränderung und Nutzung von Daten	185
2.3.2.1	Überblick zu Art. 54 PAG	185
2.3.2.2	Erläuterungen zum Tatbestand	186
2.3.2.3	Beispiele	190
2.3.3	Art. 55 PAG Allgemeine Regelungen zur Datenübermittlung	191
2.3.3.1	Allgemeine Ausführungen zur Datenübermittlung (DÜ)	191
2.3.3.2	Abgrenzungen	192
2.3.3.3	Übersicht zu den Übermittlungsvorschriften	193
2.3.3.4	Erläuterungen zu Art. 55 PAG	193
2.3.4	Art. 56 PAG Übermittlung an öffentliche Stellen im Inland	195
2.3.4.1	Erläuterungen zum Tatbestand	195

2.3.4.2	Beispiele zu Art. 56 Abs. 1 Nr. 1 PAG	200
2.3.5	Art. 57 PAG Übermittlung an öffentliche Stellen innerhalb der Europäischen Union	203
2.3.5.1	Allgemeine Erläuterungen	203
2.3.5.2	Beispiele	205
2.3.6	Art. 58 PAG Übermittlung an öffentliche Stellen in Drittstaaten und an internationale Organisationen	206
2.3.7	Art. 59 PAG Datenübermittlung an nichtöffentliche Stellen	210
2.3.7.1	Allgemeines	210
2.3.7.2	Erläuterungen zum Tatbestand	211
2.3.7.3	Beispiele	213
2.3.8	Art. 60 PAG Datenempfang durch die Polizei	219
2.3.8.1	Allgemeines	219
2.3.8.2	Überblick zum Tatbestand	219
2.3.8.3	Beispiele	221
2.3.8.4	Spezialfälle der Datenübermittlung an die Polizei	222
2.3.9	Art. 60a PAG Zuverlässigkeitsüberprüfung	231
2.3.9.1	Abgrenzungen	231
2.3.9.2	Allgemeine Erläuterungen	232
2.3.9.3	Überblick zum Tatbestand	233
2.3.9.4	Beispiele für Zuverlässigkeitsüberprüfungen nach Art. 60a Abs. 1 S. 3	234
2.3.9.5	Erläuterungen zu Art. 60a Abs. 5 PAG	235
2.3.10	Datenabgleich	236
2.3.10.1	Erläuterungen zum Datenabgleich	236
2.3.10.2	Datenabgleich mit polizeieigenen Dateien gem. Abs. 1 ggf. i.V.m. Abs. 2	237
2.3.10.3	Exkurs: AFIS-Schnellabgleich (sog. Fast-ID)	241
2.3.10.4	Beispiele	241
2.3.10.5	Abgleich mit außerpol. Datenbeständen gem. Art. 61 Abs. 3 PAG	244
2.3.10.6	Folgen bei unrechtmäßigen Datenverarbeitungen z.B. Datenabgleich zu privaten Zwecken	250
2.3.11	Art. 61a PAG	251
2.3.11.1	Allgemeine Ausführungen zu VeRA	251
2.3.11.2	Erläuterungen zum Tatbestand des Art. 61a PAG	254
2.3.11.3	Anwendungsfälle für VeRA	258
2.3.12	Sonstige Regelungen zur Datenverarbeitung	259
2.3.12.1	Art. 62 PAG Berichtigung, Löschung und Verarbeitungseinschränkung von Daten	259
2.3.12.2	Art. 63 PAG Automatisierte Abrufverfahren	260
2.3.12.3	Art. 64 PAG Errichtungsanordnung, Datenschutz-Folgenabschätzung	262
2.3.12.4	Art. 65 PAG Auskunftsrecht	265
2.4	Anwendung des Bayerischen Datenschutzgesetzes	268

3	Strafprozessordnung.....	269
3.1	Einführung.....	269
3.2	Anwendbarkeit im Bußgeldverfahren	272
3.3	Grundlagen.....	272
3.3.1	Formelle Rechtmäßigkeit.....	272
3.3.2	Legalitätsprinzip („Erforschungs- bzw. Verfolgungspflicht“).....	273
3.3.2.1	Anfangsverdacht.....	273
3.3.2.2	Tatverdächtiger (TV)/Beschuldigter (BS)	274
3.3.2.3	Todesermittlungen	276
3.3.2.4	Verhältnis Prävention – Repression („legendierte Kontrollen“)	277
3.3.3	Subsidiaritätsgrundsatz	277
3.3.4	Katalogstraftaten	278
3.3.5	Grundrechtssichernde Verfahrensregelungen – § 101 StPO	278
3.4	Datenerhebung	279
3.4.1	Generalklauseln.....	279
3.4.2	§ 163f StPO – Längerfristige Observation (Obs.)	282
3.4.2.1	Überblick zum Tatbestand.....	282
3.4.2.2	Beispiel	283
3.4.2.3	Exkurs: Kurzfristige Observation bzw. Beobachtung.....	283
3.4.2.4	Exkurs: Grenzüberschreitende Observation	284
3.4.3	Weitere Maßnahmen außerhalb von Wohnraum (Foto, Video, Audio)	287
3.4.3.1	§ 100h Abs. 1 S. 1 Nr. 1 StPO – Bildaufnahmen	287
3.4.3.1.1.	Überblick zum Tatbestand.....	287
3.4.3.1.2.	Abgrenzungen zu § 100h Abs. 1 S. 1 Nr. 1 StPO.....	289
3.4.3.1.3.	Bewertung des Laserhandmessgeräts.....	289
3.4.3.1.4.	Beispiele	290
3.4.3.2	§ 100h Abs. 1 S. 1 Nr. 2 StPO – sonst. für Observationszwecke bestimmte techn. Mittel.....	293
3.4.3.2.1.	Überblick zum Tatbestand.....	293
3.4.4	§ 100f StPO – Abhören außerhalb von Wohnungen	296
3.4.4.1	Überblick zum Tatbestand.....	296
3.4.4.2	Bsp.: Wg. Verdacht eines Verbrechens nach dem BtMG ordnete das Gericht schriftlich begründet und zeitlich befristet die Audioüberwachung des Pkw eines Kuriers mit Aufzeichnung an.	298
3.4.4.3	Abgrenzungsbeispiele	298
3.4.4.4	Beweisbeschaffung durch Privatpersonen	300
3.4.5	Wohnraumüberwachung.....	301
3.4.6	Online-Durchsuchung.....	303
3.4.6.1	Allgemeines	303
3.4.6.2	Überblick zum Tatbestand.....	304
3.4.7	Verdeckter Ermittler (VE)	305

3.4.7.1	Allgemeine Ausführungen zu verdeckten Ermittlern (VE) und nicht offen ermittelnden Polizeibeamten (NoeP).....	305
3.4.7.2	Übersicht und Erläuterungen zum Tatbestand.....	306
3.4.7.3	Abgrenzung zu Vernehmungen	310
3.4.7.4	Internet-VE und Internet-NoeP	310
3.4.7.5	Undercover Agent und Agent Provocateur.....	310
3.4.7.6	Gemengelage und Zufallsfunde.....	311
3.4.7.7	Beispiele	311
3.4.7.8	Exkurs: Informant	313
3.4.8	Polizeiliche Beobachtung.....	314
3.4.8.1	Allgemeine Ausführungen zur polizeilichen Beobachtung (PB).....	314
3.4.8.2	Überblick zum Tatbestand.....	315
3.4.8.3	Beispiele	316
3.5	Datenabgleich, Fahndungsmaßnahmen.....	318
3.5.1	§ 98c StPO Maschineller Abgleich mit vorhandenen Daten.....	318
3.5.1.1	Allgemeine Erläuterungen zum Datenabgleich	318
3.5.1.2	Übersicht und Erläuterungen zum Tatbestand.....	319
3.5.1.3	Videoauswertung bzw. -überwachung mit biometrischer Gesichtserkennung.....	320
3.5.1.4	Beispiele	321
3.5.2	Rasterfahndung.....	323
3.5.2.1	Allgemeines und Abgrenzungen vgl. Ausführungen zu Art. 46 PAG, unter Ziff. 2.2.11	323
3.5.2.2	Ablauf der Rasterfahndung	323
3.5.2.3	Übersicht zum Tatbestand.....	324
3.5.2.4	Abgrenzungs-Bsp. zu §§ 98c und 163 Abs. 1 S. 2 StPO.....	324
3.5.3	Schleppnetzfahndung (Netzfahndung).....	325
3.5.3.1	Ablauf der sog. Netzfahndung.....	325
3.5.3.2	Allgemeines zur Netzfahndung.....	326
3.5.3.3	Überblick und Erläuterungen zum Tatbestand	327
3.5.3.4	Beispiel	328
3.5.4	§ 163g StPO Automatische Kennzeichenerfassung	329
3.5.4.1	Allgemeine Erläuterungen.....	329
3.5.4.2	Übersicht und Erläuterungen zum Tatbestand.....	330
3.5.5	Personenfahndung	331
3.5.5.1	Einführung und Abgrenzungen.....	331
3.5.5.2	§ 131 StPO Ausschreibung zur Festnahme bekannter Täter.....	334
3.5.5.3	§ 131a StPO Ausschreibung zur Aufenthaltsermittlung von Beschuldigten und Zeugen und Veröffentlichung von Abbildungen.....	336
3.5.5.4	§ 131b Veröffentlichung von Abbildungen des Beschuldigten o. Zeugen	337
3.5.5.5	§ 131c StPO Anordnung und Bestätigung von Fahndungsmaßnahmen.....	338

3.5.5.6	Beispiele für polizeiliche Publikationen	341
3.5.6	Recherche in sozialen Netzwerken	341
3.5.6.1	Verfassungsrecht	341
3.5.6.2	Eingriffsrecht	342
3.5.6.3	Beispiele	343
3.6	Repressive Datenverarbeitung (insbes. Dateispeicherung)	346
3.6.1	Allgemeine Erläuterungen	346
3.6.2	Beispiel	348
3.7	Nutzung, Auskunft, Akteneinsicht	349
3.7.1	Allgemeine Ausführungen	349
3.7.2	Beispiel	351
3.7.3	Auskünfte in speziellen Fällen	352
3.8	Hypothetische Datenneuerhebung („Datenschutzrechtl. Zufallsfunde“).....	354
3.8.1	Hypothetische Datenneuerhebung	354
3.8.1.1	Allgemeine Erläuterungen	354
3.8.1.2	Klausurprüfung (Varianten)	355
3.8.1.3	Folgewirkung, falls die Anforderungen der Zweckänderungsvorschrift im Falle der Weiterverarbeitung innerhalb der Bayer. Polizei (Ziff. 3.8.1.2., Ziff. A) nicht eingehalten werden	356
3.8.2	Zweckänderung Prävention → Repression	357
3.8.3	Zweckänderung Repression → Prävention	358
3.8.4	Zweckänderung Prävention → Prävention	360
3.8.5	Zweckänderung Repression → Repression.....	362
3.8.6	Beispiel	363
3.8.7	Allgemeine Erläuterungen zur Zweckänderung von Daten aus einem PSS-Einsatz.....	366
4	Gastbeitrag zum Versammlungsrecht (Lt. PDir. K. Stangl)	367
4.1	Vorwort	367
4.2	Verfassungsrechtliche Aspekte.....	368
4.2.1	Allgemeines Persönlichkeitsrecht.....	368
4.2.2	Versammlungsfreiheit	368
4.3	Einfachgesetzliche Regelungen.....	371
4.3.1	Verhältnis von Versammlungs- und Polizeirecht	371
4.3.2	Konkretisierung der Gesetzessystematik.....	371
4.3.3	Art. 9 BayVersG als zentrale datenschutzrechtl. Regelung im BayVersG	372
4.3.3.1	Historische Entwicklung des (Art. 9) BayVersG.....	372
4.3.3.2	Datenschutz und Versammlungsrecht	373
4.3.3.3	Wesentliche Gesetzesmerkmale des Art. 9 BayVersG	375
4.4	Kontrovers diskutierte Themen	376
4.5	Weitere Regelungen im BayVersG mit Datenschutzbezug.....	383
4.6	(Klausur-)Beispiele mit Lösungsanhalten.....	385

Symbolik

Zur besseren Orientierung und Übersichtlichkeit sind einzelnen Abschnitten Symbole zugeordnet, die nachfolgend erläutert werden:

B	Befugnis
F	Wesentliche Formvorschrift
Beispiel	
Zusammenfassung	

In den Beispielen und Erläuterungen wurde aus Gründen der besseren Lesbarkeit auf eine geschlechtsspezifische Differenzierung (m/w/d) verzichtet. Sämtliche Rollen- und Funktionsbezeichnungen gelten im Sinne der Gleichbehandlung immer für alle Geschlechter.

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 an das „**Beichtgeheimnis**“ oder an das sog. „**Bankgeheimnis**“.¹ Eine gesetzliche Regelung des Bankgeheimnisses in Deutschland gibt es jedoch nicht, überdies 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.³

Erwähnenswert in diesem Zusammenhang ist auch das „**Recht am eigenen Bild**“, das im KunstUrhG aus dem Jahre 1907 geschützt wird. Zudem wurde bereits im Jahre 1871 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. Das „**Recht am eigenen Wort**“ wird in § 201 StGB geschützt.

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 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 personenbezogene Daten (pbd) 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“ (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 Das „Bankgeheimnis“ besteht de facto nicht mehr, da Auskünfte öffentlich-rechtlicher Kreditinstitute nach § 161 Abs. 1 StPO an die Staatsanwaltschaft verpflichtend sind. Privatbanken können zu Auskünften zwar nicht gezwungen werden, sind aber ihren Kunden gegenüber berechtigt, die Auskunft zur Abwendung einer Beschlagnahme freiwillig zu erteilen, vgl. Schmitt/Köhler 2025, § 161 StPO, Rn. 4.

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 Zur Offenbarung durch einen Arzt vgl. die Ausführungen unter Art. 60 PAG, insbes. Ziff. 2.3.8.4 (D).

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.

1.2 Verfassungsrecht

Im richtungsweisenden „Volkszählungsurteil“ hat das BVerfG⁶ 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 (APR)** gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hervorgebracht, **zuletzt** in seiner Entscheidung vom 26.2.2020:⁷

- Recht auf selbstbestimmtes Sterben⁸
- Recht auf informationelle Selbstbestimmung (RiS),⁹
- Recht am gesprochenen Wort,¹⁰
- Recht am eigenen Bild,¹¹
- Recht auf Privatsphäre,¹²
- Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.¹³

Zusammenfassung

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

Schranken des Persönlichkeitsschutzes

Für das APR 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 APR nicht schrankenlos gewährleistet. Vielmehr sind Einschränkungen der informationellen Selbstbestimmung auf gesetzlicher Grundlage (= verfassungsmäßige Ordnung) möglich. Der Bürger hat keine uneingeschränkte Herrschaft über seine pbD. 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

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, Urteil vom 26.02.2020; 2 BvR 2347/15.

8 BVerfG 2. Senat, Urteil vom 26. Februar 2020, 2 BvR 2347/15. 2 BvR 651/16, 2 BvR 1261/16, 2 BvR 1593/16, 2 BvR 2354/16, 2 BvR 2527/16

9 BVerfGE 65, 1 (42) = NJW 1984, S. 419.

10 BVerfGE 34, 238 (246f.) = NJW 1973, S. 891; BVerfGE 54, 148 (155) = NJW 1980, S. 2070; BVerfGE 106, 28 (41) = NJW 2002, S. 3619.

11 BVerfGE 101, 361 (381) = NJW 2000, S. 1021; BVerfG, NJW 2005, S. 3271 (3271); BVerfGE 120, 180 (198) = NJW 2008, S. 1793.

12 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.

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

verfassungskonforme Ermächtigungsgrundlagen dar. Ein Zitiergebot i.S. Art. 19 Abs. 1 S. 2 GG besteht nicht.

Mit der **Online-Durchsuchung** (vgl. Art. 45 PAG bzw. § 100b StPO) hat das BVerfG¹⁴ 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 oder drohende Gefahr für ein überragend wichtiges Rechtsgut bestehen (der Gesetzestext des Art. 45 Abs. 1 PAG nimmt dem Wortlaut nach auf bedeutende Rechtsgüter Bezug, durch die Beschränkung auf Art. 11a Abs. 2 Nr. 1 und 2 PAG handelt es sich aber ausschließlich um überragend wichtige Rechtsgüter). Überragend wichtig sind der Bestand oder die Sicherheit des Bundes oder eines Landes, Leben, Gesundheit und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung 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 (vorrangig) an **Art. 10 Abs. 1 GG** zu messen.¹⁵

Thema dieses Buches sind primär Eingriffe in das APR 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 bzw. 100g StPO eine Rechtsgrundlage darstellen.

1.3 Allgemeine Systematik des Datenschutzrechts

Im Datenschutzrecht finden grds. die europarechtliche Datenschutzgrundverordnung (DS-GVO) und **ergänzend** die nationalen bundes- (insbes. Bundesdatenschutzgesetz, BDSG) und landesrechtlichen Vorschriften (insbes. Bayer. Datenschutzgesetz, BayDSG) Anwendung.

Die **DS-GVO** (Verordnung (EU) 2016/679) hat als europarechtliche Regelung Anwendungsvorrang vor dem nationalen Datenschutzrecht, vgl. § 1 Abs. 5 BDSG bzw. Art. 2 BayDSG. Als Verordnung gilt sie unmittelbar in allen Mitgliedstaaten, Art. 288 Abs. 2 AEUV. Nationale Datenschutzgesetze (insbes. BDSG und BayDSG) ergänzen die DS-GVO, soweit sog. Öffnungsklauseln Abweichungen erlauben bzw. soweit im Einzelfall eine Konkretisierung erforderlich ist (z.B. Art. 6 Abs. 2 und 3, Art. 23, Art. 85 DS-GVO). Dem nationalen Gesetzgeber ist es grds.

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

¹⁵ Zum Verhältnis von Art. 10 GG zum APR/VIS (insbes. bei der Quellen-TKÜ) wird auf die Entscheidungen des BVerfG vom 24.06.2025 verwiesen - 1 BvR 2466/19 „Trojaner I“ und 1 BvR 180/23 „Trojaner II“. vgl. dazu die Ausführungen unter Ziff. 2.2.11.

verwehrt, unmittelbar geltende Regelungen aus der DS-GVO in nationalem Recht zu wiederholen. Das BDSG bzw. das BayDSG enthalten daher im Anwendungsbereich der DS-GVO keine umfassenden Regelungen im Datenschutz, sondern nur noch punktuelle Ergänzungen. Bei datenschutzrechtlichen Sachverhalten ist also zunächst die DS-GVO und nur ergänzend das nationale Recht zu prüfen.

Keine Anwendung findet die DS-GVO, wenn Daten im Rahmen der **Gefahrenabwehr bzw. Strafverfolgung** verarbeitet werden (vgl. Art. 2 Abs. 2 d DS-GVO). Für diesen Bereich gilt die EU-Richtlinie für den Datenschutz im Polizei- und Strafjustizbereich (Datenschutzrichtlinie (EU) 2016/680 – **DSRL-JI**). Diese Doppelregelung wurde erforderlich, weil sich die Mitgliedsländer bei der Gefahrenabwehr bzw. Strafverfolgung nicht auf eine Harmonisierung des Datenschutzrechts verständigen konnten. Eine Richtlinie gilt (im Unterschied zu einer Verordnung – s.o.) nicht unmittelbar, sondern enthält einen **nationalen Umsetzungsauftrag**, vgl. Art. 288 Abs. 3 AEUV. Dem wurde im BayDSG (Art. 28 bis 37) bzw. im BDSG (§§ 45 bis 85) und bereichsspezifisch u.a. im PAG und der StPO nachgekommen. Bei präventiven und repressiven Sachverhalten ist also der Prüfungseinstieg unmittelbar im nationalen Recht, wobei zunächst **bereichsspezifische** (z.B. PAG/StPO) und nur ergänzend die **allgemeinen** Normen aus dem Datenschutz (BayDSG/BDSG) zu prüfen sind (vgl. § 1 Abs. 2 BDSG, Art. 1 Abs. 5 BayDSG bzw. Ziff. 1.4–1.6).

Der Vollständigkeit halber sei erwähnt, dass ein Streit besteht, ob unter den Begriff der „Abwehr von Gefahren“ in Art. 2 Abs. 2d DS-GVO nur die straftatenbezogene Gefahrenabwehr zu verstehen ist und somit die nicht-straftatenbezogene Gefahrenabwehr dem Anwendungsbereich der DS-GVO unterfällt (der Wortlaut widerspricht hier einem weiten Verständnis der RL). Dieser Streit muss aber nicht entschieden werden, weil nahezu immer die Möglichkeit besteht, dass die Gefahrenabwehr zu einer Straftat führen kann, etwas in Vermisstenfällen.¹⁶

1.4 Bundesdatenschutzgesetz (BDSG)

1.4.1 Anwendungs- und Schutzbereich

Zweck des BDSG ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten (**pbD**, zu Erläuterungen vgl. Ziff. 1.7.2) in seinem Persönlichkeitsrecht beeinträchtigt wird. Nach § 1 Abs. 1 BDSG gilt es für die Verarbeitung pbD durch

- **öffentliche Stellen des Bundes** (sowohl Behörden [z.B. BKA, BPol, BfV] als auch sonstige öffentliche Stellen [z.B. Beliehehe]),
- **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. Weil mittlerweile alle deutschen Bundesländer und somit auch Bayern eigene Datenschutzgesetze haben, gilt für die Verarbeitung pbD durch Bayer. Behörden (und somit auch durch die Polizei) grds. das **BayDSG** (vgl. Ziff. 1.5).

Soweit die Bayer. Polizei aber **Bundesrecht ausführt** (= repressive Maßnahmen nach der StPO) findet das BDSG (i.V.m. § 500 StPO ergänzende) Anwendung. Deshalb ist bspw. für

¹⁶ Gesetzesbegründung zum BayDSG, LTDRs 17/19628, S. 47 bzw. Wilde/Ehmann/Niese/Knoblach, Datenschutz in Bayern, Art. 28 BayDSG, Rn. 6 ff.

Begriffsdefinitionen in der StPO auf § 46 BDSG (i.V.m. § 500 StPO) abzustellen, auch wenn die Datenverarbeitung durch die Bayer. Polizei erfolgt.

- **nichtöffentliche Stellen**, soweit diese ganz oder teilweise automatisiert erfolgt, bzw. bei nicht automatisierter Verarbeitung (z.B. bei nicht automatisierter Datenerhebung, wie einer mündlichen Befragung), wenn die pbD in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung erfolgt durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

Soweit bei der Verarbeitung von pbD eine **Einwilligung** des betroffenen Bürgers vorausgeht, ist eine Rechtsgrundlage dafür entbehrlich (vgl. Art. 7 DS-GVO), z.B. Einwilligung in die SCHUFA-Auskunft bei Kreditvergabe. Zur Einwilligung¹⁷ in polizeiliche Maßnahmen vgl. die Erwägungsgründe 35 und 37 zur DSRL-JI, Art. 30 Abs. 2 S. 1 Nr. 3 PAG bzw. § 500 StPO i.V.m. § 51 BDSG.

§ 1 Abs. 2 BDSG regelt die **Konkurrenzen** zu **speziellen** Datenschutzregelungen in Rechtsvorschriften des Bundes (z.B. StPO, AufenthG, StVG), **die dem BDSG vorgehen**. D.h., die StPO ist vorrangig zu prüfen und das BDSG kommt hier nur ergänzend zur Anwendung.

1.4.2 Datenschutzrechtliche Begriffe

Wie schon unter Ziff. 1.4.1 ausgeführt, ist für Definitionen im Bereich der StPO auf § 46 BDSG (i.V.m. § 500 StPO) abzustellen. Weil diese identisch mit Art. 4 DS-GVO sind [vgl. Ziff. 1.5.2], erfolgen einheitliche Erläuterungen unter Ziffer 1.7.

1.4.3 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).

1.5 Bayerisches Datenschutzgesetz (BayDSG)

1.5.1 Anwendungs- und Schutzbereich

Der **Gesetzeszweck** und damit der Schutzbereich des BayDSG ist, dass der Einzelne in seinem Persönlichkeitsrecht vor unzulässigem Umgang mit pbD 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

17 Die Einwilligung bzw. der Grundrechtsverzicht ist ein Akt persönlicher Freiheit, der der zu beurteilenden Handlung die Qualität des Rechtseingriffes nimmt. Weil in diesem Fall kein Grundrechtseingriff vorliegt, bedarf es für das polizeiliche Tätigwerden dann auch keiner Befugnis.

Nach hM ist ein Verzicht restriktiv zu interpretieren. Er muss immer **freiwillig** (autonome Motive, also kein „polizeilicher Druck“) in **Kenntnis aller Umstände** erfolgen (**Belehrung** über die Freiwilligkeit und deren **Dokumentation**). Dabei muss der Grundrechtsträger **einwilligungsfähig** sein (insbes. keine Volltrunkenheit – ein Kind muss die nötige Verstandesreife haben, ansonsten entscheidet der gesetzliche Vertreter). Eine erteilte Einwilligung ist jederzeit **frei widerrufbar** (dann wird sofort eine Befugnis erforderlich).

sie der Aufsicht des Freistaates Bayern unterstehen (zur Ausnahme für die repressive Datenverarbeitung vgl. Ziff. 1.4.1). Unter den Voraussetzungen des Art. 1 Abs. 2 BayDSG gilt dieses Gesetz auch für Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen.

1.5.2 Datenschutzrechtliche Begriffe

Für Definitionen findet Art. 4 DS-GVO über die Verweisung der Art. 2 S. 1, 28 II S. 1 Nr. 1 BayDSG Anwendung.¹⁸ Ergänzend wird auf Ziff. 1.7 verwiesen.

1.5.3 Sanktionsnorm

Art. 23 Abs. 1 BayDSG¹⁹ 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 pbD hat. So ist eine Abfrage pbD in der Personenvollauskunft des INPOL-Bayern, vgl. Art. 61 PAG) unzulässig, wenn diese lediglich aus Neugierde, Langeweile oder als Gefälligkeit erfolgt (das gilt auch für Selbstauskünfte).

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, für Sport und Integration unmittelbar nachgeordneten Polizeidienststellen (insbes. Präsidien der Bayerischen Polizei) gemäß § 91 Abs. 3 ZustV.²⁰ 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.

Beispiel:

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 ist rechtswidrig, ebenso unzulässig wären bereits auch eindeutige verbale oder gestikulierende Andeutungen gegenüber dem Personalleiter über polizeiliche Einträge.²¹

¹⁸ Schmidbauer/Steiner, Art. 31 PAG, Rn. 16 bzw. 30. Tätigkeitsbericht des BayLfD, Ziff. 2.7.1.

¹⁹ Für die unbefugte Datenverarbeitung findet sich nach eA eine **Sanktionsbestimmung** in Art. 84 DS-GVO i.V.m. **Art. 23 BayDSG**, weil der Bayer. Gesetzgeber über Art. 84 DS-GVO Regelungslücken aus Art. 83 DS-GVO schließen kann, vgl. Datenschutz in Bayern, Wilde/Ehmann/Niese/Knoblach, Art. 83 DS-GVO, RN 14 ff, Art. 84 DS-GVO, RN 3 bzw. Dieterle ZD 2020, 135. Eine solche Lücke besteht hier, weil weisungsgebundene Personen keine Entscheidungsmacht über Zweck und Mittel der Datenverarbeitung haben und damit nicht als Verantwortliche gem. Art. 4 Nr. 7 Hs. 1 DS-GVO angesehen werden könnten. Eine als wohl hM zu bezeichnende Ansicht entnimmt den Bußgeldtatbestand hingegen unmittelbar aus Art. 83 I, II, V Buchst. DS-GVO, weil ein Beschäftigter beim sog. Mitarbeiterexzess sehr wohl als Verantwortlicher anzusehen ist, vgl. die Leitlinien des Europäischen Datenschutzausschuss, Rn. 88 bzw. Beitrag von Dr. Ehmann, Regierungspräsident von Unterfranken in der Zeitschrift Datenschutz – Praxis, 12/2019, S. 1 ff. und der Beschluss des OLG Stuttgart v. 25.2.2025 – 2 ORbs 16 Ss 336/24.

²⁰ Zuständigkeitsverordnung vom 16.6.2015, GVBl Nr. 7/2015, S. 184.

²¹ Eine polizeiliche Aufgabe kann hier aber im Rahmen der Zuverlässigkeitsüberprüfung vorliegen, Art. 60a, 61 I S. 2 PAG.

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 unzulässig (**Anm.:** Zulässige Übermittlungen sind in Art. 60a PAG geregelt). Die Verletzung des Dienstgeheimnisses gemäß § 353b StGB ist grundsätzlich zu prüfen!²²

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 – Ausspähens von Daten,
- § 202b StGB – Abfangen von Daten,
- § 202c StGB – Vorbereiten des Ausspähens und Abfangens 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.

1.6 Konkurrenzen zum Bayerischen PAG

1.6.1 Verhältnis PAG – BayDSG

Art. 1 Abs. 5 und 6 BayDSG enthalten Vorrangregelungen. D.h., die Regelungen der Art. 30 ff. PAG **gehen den Bestimmungen des BayDSG vor!** Das BayDSG ergänzt das PAG (zu Begriffsdefinitionen vgl. Art. 2 S. 1, 28 II S. 1 Nr. 1 BayDSG i.V.m. Art. 4 DS-GVO und zu Sanktionen vgl. Art. 23 BayDSG). Ergänzend wird hier auf **Art. 66 PAG** verwiesen.²³

²² Siehe auch BGH v. 23.3.2001, 2 StR 488/00.

²³ Art. 30 Abs. 2–4 PAG setzen lediglich die Grundsätze der **Art. 6, 7 und 10 DSRL-JI** um. Die allgemeinen Verarbeitungsgrundsätze des Art. 4 DSRL-JI werden hingegen in den allgemeinen Datenschutzbestimmungen der Art. 30 und Art. 31 nicht ausdrücklich aufgegriffen. Sie finden allerdings über Art. 66 S. 1 PAG i.V.m. Art. 28 Abs. 2 Nr. 2 BayDSG Anwendung (insbes. durch die Verweisung auf Art. 5 DS-GVO). Daher gelten auch die in Art. 5 DS-GVO verankerten Grundsätze der Rechtmäßigkeit, der fairen Verarbeitung, der Zweckbindung, der Datenminimierung, der Richtigkeit, der Speicherbegrenzung, der Integrität und Vertraulichkeit sowie der Rechenschaftspflicht und Transparenz. Der Grundsatz der Transparenz besagt, dass eine Verarbeitung für die betroffene Person nachvollziehbar sein muss. Mit ihm üblicherweise verbunden sind umfassende Informationspflichten der Verantwortlichen und weitgehende Auskunftsrechte der betroffenen Person. Angesichts der Befugnisse zu heimlichen Überwachungsmaßnahmen wird man den Verweis auf Art. 5 Abs. 1 lit. a DS-GVO allerdings wohl ähnlich wie nach S. 1 und S. 2 Erwägungsgrund 26 DSRL-JI verstehen müssen. Danach gilt das Gebot einer für die betroffene Person nachvollziehbaren Verarbeitung im Anwendungsbereich der DSRL-JI zwar auch, steht aber – entsprechende gesetzliche Befugnisse vorausgesetzt – verdeckten Ermittlungen nicht generell entgegen, vgl. Möstl/Schwabenbauer, Art. 30 PAG, Rn. 2.

1.6.2 Verhältnis PAG – weitere spezielle Rechtsvorschriften

Neben den Regelungen des **PAG** und des **BayDSG** gibt es eine Vielzahl von **speziellen datenschutzrechtlichen Regelungen**.²⁴ Diese gehen dem PAG bzw. dem BayDSG vor – z.B.:

- § 87 AufenthG (Datenübermittlung an die Ausländerbehörde),
- §§ 67 ff. SGB X (Schutz der Sozialdaten),
- §§ 35 ff. StVG (Auskunft aus dem Zentralen Fahrzeugregister),
- §§ 34 ff. 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. 14 BayPsychKHG (Verständigungspflichten),
- BKAG, SDÜ.

Nicht immer werden dabei typische Begriffe des Datenschutzes verwendet, so dass der Bezug zum Datenschutz oft nicht 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 § 477 StPO bzw. 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.

²⁴ Anwendbar über Art. 2 Abs. 4 PAG.

1.7 Datenschutzrechtliche Begriffe

Datenschutzrechtliche Begriffsdefinitionen sind in Art. 3 DSRL-JI, Art. 4 DS-GVO, sowie in § 46 BDSG erläutert.²⁵

1.7.1 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“, vgl. Art. 32 DS-GVO bzw. Art. 32 BayDSG und § 64 BDSG.

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.

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 pbD 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 pbD vor dem Missbrauch durch Dritte (nicht zu verwechseln mit Datensicherheit).²⁶ Schutzobjekt ist der Mensch mit seinen pbD. 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 **datenschutzrechtlichen Begriffe** werden in **Art. 4 DSGVO** (anwendbar bei präventiven Maßnahmen über die Verweisung in Art. 2 S. 1, 28 II S. 1 Nr. 1 BayDSG) bzw. **§ 46 BDSG** (anwendbar bei repressiven Maßnahmen über die Verweisung in § 500 StPO) definiert.

25 Das BayDSG verweist bzgl. Definitionen in Art. 2 Abs. 1 S. 1 i.V.m. 28 Abs. 1 S. 1 Nr. 1, Abs. 2 S. 1 Nr. 1 BayDSG auf Art. 4 DS-GVO. Auf diese Definitionsnorm ist bei polizeirechtlichen Maßnahmen abzustellen.

26 BSI (Hrsg.), Leitfaden zur Basis-Absicherung nach IT-Grundschutz, Oktober 2017, S. 84.

1.7.2 Personenbezogene Daten

Personenbezogene Daten (pbD) 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.²⁷

Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die Person zu identifizieren. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden, sollten alle objektiven Faktoren, wie Kosten und Zeitaufwand herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie (polizeiliche Abfrage- und Auswertemöglichkeiten) zu berücksichtigen ist.²⁸ Identifizierbar ist eine Person auch dann, wenn sie bei der Informationserhebung **anwesend** ist (z.B. Beobachtung einer bislang unbekannten Person), denn in diesem Fall ist die Person für die Dauer der Anwesenheit individualisiert und jede Information, die mit ihr in Zusammenhang steht, ist personenbezogen.²⁹

Information kann jede Feststellung sein, wie z.B. das Aussehen, eine Verhaltensweise, schriftliche oder mündliche Äußerungen, gemessene Geschwindigkeit oder das Fahrverhalten.

Zusammenfassung

Alle Daten (= Informationen), 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. GmbH X) und nicht rechtsfähiger Personenvereinigungen sind vom Begriff der pbD nicht umfasst, es sei denn, sie können auf „dahinterstehende“ natürliche Personen bezogen werden (z.B. Observation des Geschäftsführers).

Für **behördeninterne pbD**, z.B. die Urlaubsplanung, Liste über zugeteilte Waffen, Personalakten usw. (sog. Verwaltungsdateien) gelten 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.

²⁷ Art. 3 Nr. 1 Richtlinie (EU) 2016/680 bzw. Art. 4 Nr. 1 DS-GVO bzw. § 46 Nr. 1 BDSG.

²⁸ ErwG 26 S. 3 DSGVO.

²⁹ EUGH, Urt. v. 19.10.2016, C-582/14.

1.7.3 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 (vgl. § 2 Abs 2 BDSG) nehmen auch (tatsächlich) Aufgaben der öffentlichen Verwaltung wahr, ohne Behörde zu sein (z.B. gesetzliche Krankenversicherer, Bezirkskaminkehrer im Rahmen der Feuerstättenmessung nach 1. BImSchV, Feuerwehr, BRK, RKT, ...).

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).

1.7.4 Datei³⁰

Eine **automatisierte Datei** ist eine Sammlung pbD, die durch **automatisierte** Verfahren nach bestimmten Merkmalen ausgewertet werden kann. Kernelement automatisierter Dateien ist der **Einsatz von EDV-Technik**, d.h. pbD 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 (vgl. Art. 4 Nr. 6 DS-GVO bzw. VollzBek PAG zu Art. 47 a.F., Ziff. 47.1.).

Im Unterschied dazu können dieselben pbD in **nicht automatisierten Dateien** angelegt werden, das ist jede sonstige Sammlung pbD, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann. Hier kommt keine EDV zum Einsatz, die Daten werden konventionell in manuell geführten Handkarteien, -registern oder Papierordnern zusammengeführt. Eingriffsrechtlich spielt diese Unterscheidung keine wesentliche Rolle (vgl. Art. 54 PAG), vielmehr jedoch im Rahmen der Prüfung der Genehmigungszuständigkeit zum Führen einer Datei (vgl. Art. 64 PAG).

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 z.B. Einsatzbefehle und sonstigen Einsatzunterlagen. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

Bei der Speicherbefugnis im PAG wird nicht zwischen diesen Begriffen unterschieden, vgl. Art. 53, 54 PAG, anders hingegen in der StPO, vgl. §§ 483 ff., 496 ff. StPO.

1.7.5 Datenverarbeitung

Nach **Art. 4 Nr. 2 DS-GVO (§ 46 Nr. 2 BDSG)** beinhaltet die Verarbeitung jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit **pbD** wie das **Erheben**, das Erfassen, die **Organisation**, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das **Abfragen**, die Ver-

³⁰ vgl. die Ausführungen unter Ziff. 2.3.1.1.

wendung, 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**³¹ 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 pbD (z.B. Brief eines Mitteilers), 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.³² Die Erhebung beginnt aber spätestens mit gezielten Nachfragen.
- **Speichern**³³ ist das Erfassen, Aufnehmen oder Aufbewahren pbD auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung.
- **Verändern**³⁴ ist das inhaltliche Umgestalten gespeicherter pbD.
- **Übermitteln**³⁵ ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener pbD an Dritte (= Person außerhalb der erhebenden Stelle; vgl. Art. 4 Nr. 10 DS-GVO bzw. Ziff. 1.7.6) in der Weise, dass
 - die Daten durch die speichernde Stelle an Dritte weitergegeben werden (z.B. mündlich, per E-Mail, ...) oder
 - Dritte Daten einsehen oder abrufen, die von der speichernden Stelle zur Einsicht oder zum Abruf bereitgehalten werden (z.B. Fahndungsausschreibung in INPOL, Einstellen in die Morgenlage, Vermisstensuche im Intranet).
- Den **Datenabgleich**³⁶ als speziell geregelte Form der Datenübermittlung regeln Art. 46, 61 bzw. 61a im PAG und § 98a bzw. 98c in der StPO.
- **Sperrern**³⁷ ist das Kennzeichnen gespeicherter pbD, um ihre weitere Verarbeitung oder Nutzung einzuschränken.
- **Löschen**³⁸ ist das Unkenntlichmachen gespeicherter pbD.
- **Datennutzung**³⁹ (Auffangverwendung) ist jede sonstige Verwendung pbD. Darunter fällt insbesondere die Weitergabe von pbD innerhalb **derselben** Polizeidienststelle (z.B. tägliche Lagebesprechung oder telefonische Weitergabe von Informationen durch den DGL an seine Streifenbesatzung), vgl. Art. 53, 54 PAG, dort als „anderweitige Verarbeitung“ bezeichnet.).

31 vgl. die Ausführungen unter Ziff. 2.1.2 (insbes. Ziff. 2.1.2.3.1).

32 aA Schmidt, Rn. 130: Da dem Beschaffen der Daten der Zweck ihrer Verarbeitung immanent ist, liegt für den Fall, dass der Polizei unaufgefordert Daten zugehen, eine Datenerhebung dann vor, wenn die Polizei zur Kenntnisnahme verpflichtet ist, wenn die Daten also ein polizeiliches Tätigwerden erforderlich machen oder machen können.

33 vgl. die Ausführungen unter Ziff. 2.3.1.1.

34 vgl. die Ausführungen unter Ziff. 2.3.1.

35 vgl. die Ausführungen unter Ziff. 2.3.3.2.

36 vgl. die Ausführungen unter Ziff. 2.3.3.2.

37 vgl. die Ausführungen unter Ziff. 2.3.12.

38 vgl. die Ausführungen unter Ziff. 2.3.12.

39 vgl. die Ausführungen unter Ziff. 2.3.1.

Zusammenfassung

Der Datenspeicherung geht grds. 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.

1.7.6 Weitere Begriffe zum Datenschutz⁴⁰

- **Profiling** ist jede Art der automatisierten Verarbeitung pbD, die darin besteht, dass diese pbD 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 pbD in einer Weise, dass die pbD ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die pbD nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Hier finden die Datenschutzvorschriften Anwendung.
- **Anonymisieren** ist das Verändern pbD 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 bestimmbar natürlichen Person zugeordnet werden können. Dies spielt insbesondere bei der Verwendung pbD zu Schulungszwecken eine Rolle (siehe hierzu Art. 54 Abs. 4 PAG). Hier finden die Datenschutzvorschriften keine Anwendung.
- **Genetische Daten** sind pbD 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 (DNA) der betreffenden natürlichen Person gewonnen wurden.⁴¹
- **Biometrische Daten** mit speziellen technischen Verfahren gewonnene pbD 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.⁴²
- **Gesundheitsdaten** sind pbD, 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.⁴³

40 vgl. Art. 3 Richtlinie (EU) 2016/680, Art. 4 DS-GVO.

41 u.a. Art. 9 DS-GVO bzw. Art. 30 Abs. 2 PAG („besondere Kategorien von pbD“, vgl. die folgenden Erläuterungen).

42 u.a. Art. 9 DS-GVO bzw. Art. 30 Abs. 2 PAG („besondere Kategorien von pbD“, vgl. die folgenden Erläuterungen).

43 u.a. Art. 9 DS-GVO bzw. Art. 30 Abs. 2 PAG („besondere Kategorien von pbD“, vgl. die folgenden Erläuterungen).

- **Besondere Kategorien pbD** (vgl. u.a. **Art. 9 DS-GVO** bzw. **Art. 30 Abs. 2 PAG**) 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 **pbD** 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 pbD im Auftrag erheben, übermitteln oder sonst verarbeiten. Diese Personenart spielt insbesondere dann eine Rolle, wenn pbD automatisiert bzw. technisch unterstützt erhoben werden, z.B. Telekommunikationsüberwachung, Foto- und Videografie, Lauschangriff. Der Gesetzgeber hat für diese Maßnahmen in den gesetzlichen Regelungen 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.

1.7.7 Relevanz bei Rechtsprüfungen

Im Rahmen materiell-rechtlicher Beurteilungen nach dem PAG bzw. der StPO können grundsätzlich immer die Definitionen aus **Art. 4 DS-GVO** (PAG) bzw. **§ 46 BDSG** (StPO) 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!

Beispiel:

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

Bei den Personalien, der Personen- und Sachverhaltsbeschreibung handelt es sich um Informationen zu einer identifizierten Person und somit um pbD (**Art. 4 Nr. 1 DS-GVO**). Weil diese verarbeitet werden (hier: übermittelt, **Art. 4 Nr. 2 DS-GVO**), ist eine Befugnis erforderlich, **Art 53 Abs. 1 PAG**.

Diese ergibt sich aus Art. 56 Abs. 1 Nr. 1 PAG, weil die Übermittlung zur Erfüllung einer polizeilichen Aufgabe, nämlich dem raschen Auffinden der vermissten Person, erforderlich ist. Der DGL ist gem. Art. 55 Abs. 1 S. 1 PAG für die Rechtmäßigkeit dieser Datenübermittlung verantwortlich.