

Datenschutzrecht und polizeiliche Datenverarbeitung

Kapitel 1: Einführung; das Volkszählungsurteil des Bundesverfassungsgerichts; historische Entwicklung und Zukunft des Datenschutzes

Einführung

A. Was ist Datenschutz?

- Schutz des Einzelnen davor, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (vgl. § 1 I BDSG)

bzw.

- Schutz des Rechts des Einzelnen, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen (vgl. Art. 33 S. 1 VvB; § 1 I Nr. 1 BlnDSG)

B. Gefahren für das Recht auf informationelle Selbstbestimmung

Allgemeine Gefahren polizeilicher Tätigkeit für das Recht auf informationelle Selbstbestimmung:

- Unfreiwilliges Bekanntwerden „sensibler“ Daten
- Unfreiwilliges Bekanntwerden privater Lebensumstände, auch wenn sie nicht „sensibel“ sind

Besondere Gefahren der automatisierten polizeilichen Datenverarbeitung für das Recht auf informationelle Selbstbestimmung:

- Weitergabe und Weiterverbreitung „sensibler“ und allgemein privater Daten
- Fehlerfortpflanzung: Große Auswirkungen einzelner fehlerhafter Daten, wenn diese für eine Vielzahl anderer Stellen bereitgestellt oder übermittelt und für einen langen Zeitraum gespeichert werden (Beispiel: Kreditinformationen)
- Verfälschung von Informationen durch Kontextverlust
- Informationsmacht durch Zusammenführen von Informationen (Beispiel: Bewegungsprofile)

Das Volkszählungsurteil des Bundesverfassungsgerichts

Urteil vom 15.12.1983; Fundstelle: BVerfGE 65, 1
(vgl. Link im Internet unter <http://tobias-herbst.de> - Rubrik „Materialien“ anklicken)

A. Der Sachverhalt

Nach dem Volkszählungsgesetz 1983 (VZG 1983) sollte im Jahre 1983 eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung durchgeführt werden. Hinsichtlich der zu erhebenden Daten enthielt das Gesetz folgende Regelungen:

„§ 2

Die Volkszählung und Berufszählung erfaßt:

- 1. Vornamen und Familiennamen, Anschrift, Telefonanschluß, Geschlecht, Geburtstag, Familienstand, rechtliche Zugehörigkeit oder Nichtzugehörigkeit zu einer Religionsgesellschaft, Staatsangehörigkeit;*
- 2. Nutzung der Wohnung als alleinige Wohnung, Hauptwohnung oder Nebenwohnung (§ 12 Abs. 2 des Melderechtsrahmengesetzes);*
- 3. Quelle des überwiegenden Lebensunterhaltes;*
- 4. Beteiligung am Erwerbsleben, Eigenschaft als Hausfrau, Schüler, Student;*
- 5. erlernten Beruf und Dauer der praktischen Berufsausbildung, höchsten Schulabschluß an allgemeinbildenden Schulen, höchsten Abschluß an einer berufsbildenden Schule oder Hochschule sowie Hauptfachrichtung des letzten Abschlusses;*
- 6. bei Erwerbstätigen sowie Schülern und Studenten Namen und Anschrift der Arbeitsstätte oder Ausbildungsstätte, hauptsächlich benutztes Verkehrsmittel und Zeitaufwand für den Weg zur Arbeitsstätte oder Ausbildungsstätte;*
- 7. bei Erwerbstätigen Geschäftszweig des Betriebes, Stellung im Beruf, ausgeübte Tätigkeit, Arbeitszeit, landwirtschaftliche und nichtlandwirtschaftliche Nebentätigkeit;*
- 8. im Anstaltsbereich die Eigenschaft als Insasse oder die Zugehörigkeit zum Personal oder zum Kreis der Angehörigen des Personals.*

§ 3

(1) Die gebäudestatistischen Fragen erfassen bei Gebäuden mit Wohnraum und bei ständig bewohnten Unterkünften Anschrift, Art und Baujahr sowie den Eigentümer oder an seiner Stelle den Nießbrauchberechtigten oder denjenigen, der Anspruch auf Übereignung oder auf Einräumung oder Übertragung eines Erbbaurechts oder Nießbrauchs hat.

(2) Die wohnungsstatistischen Fragen erfassen:

- 1. Art, Größe, Ausstattung und Verwendungszweck, Art der Beheizung und der Heizenergie sowie Bezugsjahr der Wohnung, Wohnverhältnis, Förderung der Wohnung mit Mitteln des sozialen Wohnungsbaus sowie Zahl und Nutzung der Räume;*
- 2. bei vermieteten Wohnungen außerdem die Höhe der monatlichen Miete;*
- 3. bei leerstehenden Wohnungen außerdem die Dauer des Leerstehens.*

§ 4

Die Arbeitsstättenzählung erfaßt:

1. bei allen nichtlandwirtschaftlichen Arbeitsstätten und Unternehmen

a) Namen, Bezeichnung, Anschrift, Telefonanschluß und Zahl der Sprechstellen, Art der Niederlassung, Art der ausgeübten Tätigkeit oder Art des Aufgabengebietes der Arbeitsstätte und des Unternehmens, Eröffnungsjahr, Angaben über Neuerrichtung oder Standortverlagerung, Träger der Arbeitsstätte bei Anstalten, Einrichtungen von Behörden oder der Sozialversicherung sowie von Kirchen, Verbänden oder sonstigen Organisationen,

b) Zahl der tätigen Personen nach Geschlecht, Stellung im Betrieb, Zahl der Teilzeitbeschäftigten sowie Zahl der ausländischen Arbeitnehmer nach Geschlecht,

c) Summe der Bruttolöhne und Bruttogehälter des vorhergehenden Kalenderjahres;

2. bei Hauptniederlassungen und einzigen Niederlassungen außerdem

a) Eintragung des Unternehmens in die Handwerksrolle,

b) Rechtsform des Unternehmens;

3. bei Hauptniederlassungen zusätzlich zu den Angaben nach den Nummern 1 und 2 für jede Zweigniederlassung

a) Namen, Bezeichnung, Anschrift, Art der ausgeübten Tätigkeit oder des Aufgabengebietes,

b) Zahl der tätigen Personen,

c) Summe der Bruttolöhne und Bruttogehälter des vorhergehenden Kalenderjahres.“

Die Volkszählung erfasste alle volljährigen Personen, in bestimmten Fällen auch Minderjährige. Es bestand eine bußgeldbewehrte Verpflichtung zur Beantwortung der im Rahmen der Volkszählung gestellten Fragen.

Nach § 9 VZG 1983 durften die erhobenen Daten mit den Melderegistern abgeglichen und als Einzelangaben ohne Namen im Wesentlichen an die Fachbehörden des Bundes und der Länder zur Erfüllung ihrer Aufgaben und für Planungszwecke auch an die jeweiligen Gemeinden übermittelt werden. Auch eine Auswertung der Daten für wissenschaftliche Zwecke war vorgesehen.

Das VZG 1983 wurde von Bundestag und Bundesrat einstimmig verabschiedet.

Auf zahlreiche Verfassungsbeschwerden einzelner Bürger hin wurde die Durchführung der Volkszählung vom BVerfG zunächst ausgesetzt; später erging das Volkszählungsurteil. In diesem Urteil erklärte das BVerfG einzelne Bestimmungen des VZG 1983 für verfassungswidrig und formulierte wesentliche Grundsätze des Datenschutzrechts.

B. Der Inhalt des Volkszählungsurteils

Nachdem das BVerfG die Verletzung anderer Grundrechte durch das VZG verneint hat, setzt es sich mit dem „**Recht auf informationelle Selbstbestimmung**“ auseinander. Dieses Recht ist ein Teil des in Art. 2 I i.V.m. Art. 1 I GG verankerten „allgemeinen Persönlichkeitsrechts“. Obwohl das Grundgesetz keine ausdrücklichen Regelungen zum Recht auf informationelle Selbstbestimmung enthält, wird dieses Recht vom BVerfG wie ein eigenständiges Grundrecht entfaltet. So wird es heute auch angewandt; man prüft also z.B. einen Eingriff in den Schutzbereich des Rechts auf informationelle Selbstbestimmung, Art. 2 I i.V.m. Art. 1 I GG, sowie die Schranken und Schranken-Schranken dieses Grundrechts.

Wörtlich führt das BVerfG zur Begründung und Herleitung des Rechts auf informationelle Selbstbestimmung aus (BVerfGE 65, 1, 41 ff.):

„Prüfungsmaßstab ist in erster Linie das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützte allgemeine Persönlichkeitsrecht.

1. a) Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Ihrem Schutz dient - neben speziellen Freiheitsverbürgungen - das in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht, das gerade auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen der menschlichen Persönlichkeit Bedeutung gewinnen kann. ... Es umfaßt ... auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden ...

Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes. Sie ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muß, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten [vgl. § 2 Abs. 1 BDSG]) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus - vor allem beim Aufbau integrierter Informationssysteme - mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekanntem Weise die Möglichkeiten einer Einsichtnahme und Einflußnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen.

Individuelle Selbstbestimmung setzt aber - auch unter den Bedingungen moderner Informationsverarbeitungstechnologien - voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.

Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von

dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

Das BVerfG führt weiter aus, dass Beschränkungen des Rechts auf informationelle Selbstbestimmung unter bestimmten Voraussetzungen möglich sind; solche Beschränkungen bedürfen in jedem Fall einer ausreichend klaren und bestimmten **gesetzlichen Grundlage** und müssen dem Grundsatz der **Verhältnismäßigkeit** entsprechen.

Die Zulässigkeit von Beschränkungen des Rechts auf informationelle Selbstbestimmung hängt dabei nicht alleine von der Art der jeweiligen Daten ab. Geschützt sind also nicht nur etwa Daten über intime Vorgänge, sondern grundsätzlich alle Daten, die sich auf eine bestimmte Person beziehen. Wörtlich heißt es dazu im Volkszählungsurteil (BVerfGE 65, 1, 45 f.):

„Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein "belangloses" Datum mehr.

Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs: Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungsmöglichkeiten und Verwendungsmöglichkeiten bestehen, läßt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten. ...

Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbareren Zwecken nicht zu vereinbaren. Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen.

Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein - amtshilfefester - Schutz gegen Zweckentfremdung durch Weitergabeverbote und Verwertungsverbote erforderlich. Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungspflichten, Auskunftspflichten und Löschungspflichten wesentlich.

Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung.“

Hinsichtlich der Erhebung und Verarbeitung von Daten für **statistische Zwecke** gelten nach den Ausführungen des BVerfG im Volkszählungsurteil einige Besonderheiten (BVerfGE 65, 1, 47 ff.). Die Erhebung von Daten für statistische Zwecke ist in der Regel nur dann sinnvoll, wenn diese Daten an unterschiedliche Stellen mit unterschiedlichen Aufgaben übermittelt werden können; dabei sollen die Daten auch für zukünftige Aufgaben aufbewahrt werden können, also „auf Vorrat“ gespeichert werden. Die mit diesen weitgehenden Verwendungsmöglichkeiten verbundenen Gefahren für das Recht auf informationelle Selbstbestimmung

müssen ausgeglichen werden durch besondere Vorkehrungen. So ist zu unterscheiden zwischen den Hilfsangaben in Gestalt von Identifikationsmerkmalen (Name, Anschrift, Kennnummer etc.), die für die Durchführung der Datenerhebung erforderlich sind, und den eigentlich zu erhebenden Daten. Die Hilfsangaben müssen möglichst frühzeitig gelöscht werden (**Anonymisierung** der Daten), und vor dieser Anonymisierung müssen besondere Vorkehrungen zur Geheimhaltung und Abschottung nach außen getroffen werden. Die Daten dürfen erst nach der Anonymisierung von den Statistischen Ämtern anderen staatlichen Organen oder sonstigen Stellen zur Verfügung gestellt werden.

Es ist also zu unterscheiden zwischen der Datenerhebung für statistische Zwecke und der Datenerhebung für Zwecke des Verwaltungsvollzugs. Die Datenerhebung für **statistische Zwecke** erfordert einerseits die möglichst frühzeitige Anonymisierung und die Abschottung und Geheimhaltung der Identifikationsmerkmale; andererseits ist die Weiterleitung (anonymisierter) statistischer Daten auch an einen nicht feststehenden Adressatenkreis zu nicht feststehenden Zwecken zulässig. Die Datenerhebung für **Zwecke des Verwaltungsvollzugs** dagegen verlangt keine Anonymisierung der Daten; die Zuordnung zu bestimmten Personen ist hier ja in den meisten Fällen gerade die Voraussetzung der sinnvollen Verwendung dieser Daten. Dafür besteht aber für diese Daten eine strikte Zweckbindung, die nur durch Einschränkungen bei der Verwendung und Übermittlung der Daten erreicht werden kann.

Eine Datenerhebung, die **beiden Zwecken** (Statistik und Verwaltungsvollzug) **gleichzeitig** dienen soll, ist in der Regel unverhältnismäßig und daher unzulässig (BVerfGE 65, 1, 61 ff.). Für den betroffenen Bürger wäre bei einer solchen Vermengung der Zwecke nicht klar genug erkennbar, zu welchen Zwecken seine Daten erhoben werden und wie sie verwendet werden sollen. Daher erklärte das BVerfG die Regelungen des § 9 VZG 1983, soweit sie den Melderegisterabgleich sowie die Übermittlung der Daten an die Fachbehörden des Bundes und der Länder und an die Gemeinden zulassen, für verfassungswidrig (BVerfGE 65, 1, 63 ff.). Dabei betont das BVerfG, dass die Daten allein durch Weglassen des Namens der jeweiligen Person und deren Religionszugehörigkeit (das ist teilweise Voraussetzung der Übermittlung nach § 9 VZG 1983) noch nicht faktisch anonymisiert seien, weil sie dem jeweils Betroffenen noch ohne Schwierigkeiten zuzuordnen seien (BVerfGE 65, 1, 65).

Historische Entwicklung und Zukunft des Datenschutzes

1970: Hessisches Datenschutzgesetz als weltweit erstes Datenschutzgesetz; danach Schweden (**1973**), USA (**1974**).

1977: Bundesdatenschutzgesetz

1983: Volkszählungsurteil des BVerfG. Wichtiger Impuls für die Gesetzgebung: Nach dem Urteil genügen die allgemeinen Regelungen im BDSG und den Landesdatenschutzgesetzen nicht mehr; vielmehr fordert das BVerfG bereichsspezifische Regelungen

In der Folgezeit werden eine Reihe bereichsspezifischer Datenschutzregelungen vor allem von den Landesgesetzgebern geschaffen, u.a. in den jeweiligen Polizeigesetzen. Das BDSG wird **1990** geändert, das BKAG erhält erst **1997** bereichsspezifische Datenschutzregelungen.

1992: Das Berliner ASOG wird neu gefasst und erhält bereichsspezifische Datenschutzregelungen

1995: EG-Datenschutzrichtlinie

2001: Novellierung des BDSG zur Anpassung an die EG-Richtlinie

Ziele der zukünftigen Datenschutzgesetzgebung („Modernisierung des Datenschutzes“): V.a. Konzentration der gesetzlichen Regelungen in möglichst wenigen Gesetzen; die wichtigsten Grundsätze des Datenschutzes sollen in den Datenschutzgesetzen des Bundes und der Länder geregelt werden. In Spezialgesetzen (z.B. dem ASOG) sollen nur noch bereichsspezifische Ausnahmeregelungen von diesen allgemeinen Grundsätzen enthalten sein.

Kapitel 2: Überblick über wichtige gesetzliche Regelungen zum Datenschutz

A. Bundesdatenschutzgesetz (BDSG)

Anwendungsbereich: § 1 II BDSG:

„Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,

2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie

a) Bundesrecht ausführen oder

b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,

3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.“

B. Berliner Datenschutzgesetz (BlnDSG)

Anwendungsbereich: § 2 I BlnDSG:

„Zum Schutz personenbezogener Daten nach Maßgabe dieses Gesetzes sind alle Behörden und sonstigen öffentlichen Stellen (insbesondere nichtrechtsfähige Anstalten, Krankenhausbetriebe, Eigenbetriebe und Gerichte) des Landes Berlin und der landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (§ 28 des Allgemeinen Zuständigkeitsgesetzes) verpflichtet. Dies gilt auch für natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen.“

vgl. ferner § 2 V BlnDSG:

„Dieses Gesetz regelt den Schutz personenbezogener Daten für die Behörden und sonstigen öffentlichen Stellen umfassend. Andere Landesgesetze können für bestimmte Behörden und sonstige öffentliche Stellen einzelne notwendige Abweichungen von diesem Gesetz vorschreiben; im übrigen richtet sich der Datenschutz auch in diesen Fällen nach den Vorschriften dieses Gesetzes.“

C. ASOG

Anwendungsbereich: Tätigkeit der Polizei und der Ordnungsbehörden im Rahmen der Aufgaben nach § 1 ASOG, also v.a. bei der Gefahrenabwehr und vorbeugenden Straftatenbekämpfung.

Wichtige Vorschriften: §§ 28, 42-50 ASOG (allgemeine Vorschriften zum Datenschutz). Darüber hinaus stellen fast alle Standardmaßnahmen Datenerhebungen dar (Ausnahmen: Platzverweisung und verwandte Maßnahmen, Gewahrsam, Sicherstellung), so dass die entsprechenden Befugnisnormen auch als Datenschutzregelungen angesehen werden können.

D. StPO

Anwendungsbereich: Strafverfolgung

Wichtige Vorschriften: z.B. §§ 81e ff. (DNA-Untersuchung), 98a ff. (Rasterfahndung und Datenabgleich), 100a ff. (Überwachung der Telekommunikation, Einsatz technischer Mittel, Großer Lauschangriff), 110a ff. (Verdeckte Ermittler), 163d ff. (Schleppnetzfahndung, polizeiliche Beobachtung, längerfristige Observation)

E. Andere bereichsspezifische Regelungen, z.B.:

- §§ 67 ff. SGB X, insb. §§ 68, 73 SGB X (Übermittlung von Sozialdaten an die Polizei, Nutzung von Sozialdaten für ein Strafverfahren)
- §§ 28 ff. StVG, insb. § 30 I Nr. 1 StVG (Übermittlung aus dem Verkehrszentralregister zum Zwecke der Strafverfolgung) und § 35 I Nr. 2-4 (Übermittlung aus den Fahrzeugregistern für Zwecke der Verfolgung von Straftaten und Ordnungswidrigkeiten und zur Gefahrenabwehr)
- § 18 MRRG (Melderechtsrahmengesetz): Übermittlung von Daten aus dem Melderegister zur Erfüllung von Aufgaben des Empfängers
- § 2b PersAuswG, § 22 PaßG: Übermittlung von Daten (einschließlich Lichtbildern und Unterschriften) aus dem Personalausweis- bzw. Paßregister, wenn die ersuchende Behörde berechtigt ist, die Daten zu erhalten und ohne die Daten ihre Aufgaben nicht erfüllen könnte.
- § 78 III AuslG (Übermittlung erkennungsdienstlicher Unterlagen durch das BKA an Polizeibehörden), § 8 III AsylVfG (Übermittlung von Daten zum Zwecke der Strafverfolgung), §§ 10 ff. AZRG (Übermittlung von Daten aus dem Ausländerzentralregister)
- § 10 GwG (Geldwäschegesetz): Verwendung von Aufzeichnungen über die Identität von Bankkunden und über bestimmte Kontobewegungen zum Zwecke der Strafverfolgung
- § 21 I Nr. 2 SÜG (Sicherheitsüberprüfungsgesetz): Übermittlung von Daten aus der Sicherheitsüberprüfung zum Zwecke der Strafverfolgung
- § 7 IV G10: Übermittlung von Daten aus der Telekommunikationsüberwachung durch den BND zur Verhinderung von Straftaten
- § 180 StVollzG: Verwendung von Daten der Vollzugsbehörden zur Gefahrenabwehr und zur Strafverfolgung

Kapitel 3: Anwendung des BlnDSG im Bereich der polizeilichen Gefahrenabwehr; wichtige Begriffe und Grundsätze des Datenschutzrechts

A. Grundsätzliches

Das BlnDSG gilt nach § 2 I BlnDSG u.a. für alle Behörden des Landes Berlin, also auch für die Berliner Polizei, insbesondere im Bereich der Gefahrenabwehr. Bereichsspezifische Sonderregelungen in spezielleren Gesetzen, zu denen auch das ASOG zählt, gehen allerdings den allgemeineren Vorschriften des BlnDSG vor. Das folgt schon aus dem Spezialitätsgrundsatz und ist darüber hinaus in § 2 V BlnDSG ausdrücklich geregelt.

B. Anwendbare Vorschriften des BlnASOG

Im Bereich des ASOG anwendbar sind daher v.a. die Begriffsbestimmungen (§ 4 BlnDSG – die hier definierten Begriffe werden teilweise auch im ASOG verwendet) und die Vorschriften über den Berliner Datenschutzbeauftragten (§§ 21 ff. BlnDSG)

I. Begriffsbestimmungen

§ 4 BlnDSG enthält eine Reihe von Definitionen datenschutzrechtlicher Begriffe (der Gesetztext ist im Folgenden kursiv wiedergegeben, Erläuterungen in normaler Schrift):

*(1) Im Sinne dieses Gesetzes sind **personenbezogene Daten** Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (**Betroffener**). Entsprechendes gilt für Daten über Verstorbene, es sei denn, daß schutzwürdige Belange des Betroffenen nicht mehr beeinträchtigt werden können.*

Einzelangaben: Angaben, die sich auf einzelne Personen beziehen. Keine Einzelangaben sind z.B. zusammenfassende Angaben über Personengruppen, aus denen sich keine Informationen über einzelne Personen schließen lassen. Beispiel: Durchschnittsgehalt mehrerer Mitarbeiter einer Firma.

Persönliche oder sachliche Verhältnisse: Alle Informationen, die eine Person betreffen, einschließlich Informationen über ihre Beziehungen zur (z.B. sozialen oder wirtschaftlichen) Umwelt und einschließlich von Werturteilen über die Person.

bestimmt: Aus den Angaben selbst ergibt sich, dass sich die Informationen auf diese und nur diese Person beziehen.

bestimmbar: Die Identität der Person, auf die sich die Informationen beziehen, kann unter Verwendung von Zusatzwissen und notfalls mit Hilfe statistischer Methoden und dem Einsatz von Computern festgestellt werden.

§ 4 I BlnDSG enthält eine Legaldefinition des Begriffs „Betroffener“. Gemeint ist immer diejenige Person, über die die jeweiligen Daten etwas aussagen.

Daten über Verstorbene sind nur nach dem BlnDSG, nicht nach dem BDSG geschützt.

Firmen- und Geschäftsdaten und Daten über juristische Personen und sonstige Personenvereinigungen sind nur dann personenbezogen, wenn sich aus ihnen Einzelangaben über bestimmte oder bestimmbare natürliche Personen schließen lassen. Reine Geschäftsdaten sind also keine personenbezogenen Daten und daher nicht durch das BlnDSG geschützt.

*(2) **Datenverarbeitung** ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten. Im Sinne der nachfolgenden Vorschriften ist*

*1. **Erheben** das Beschaffen von Daten über den Betroffenen,*

Erheben ist nur das aktive, von einem entsprechenden Willen getragene Beschaffen von Daten. Die Kenntnisnahme genügt; die Daten müssen nicht aufgezeichnet werden. Es muss sich um personenbezogene Daten handeln („über den Betroffenen“). Die Erhebung muss nicht systematisch erfolgen.

Beispiele:

- Befragen einer Person; Beobachten einer Person
- Das Erben eines Datenträgers ist keine Datenerhebung

2. **Speichern** das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger,

Erfassen: nicht nur die Eingabe in einen Computer, sondern jede Art der Aufzeichnung und körperlichen Fixierung, z.B. Schreiben per Hand oder mit der Schreibmaschine.

Aufnehmen: Aufzeichnen mit Hilfe einer apparativen Vorrichtung, z.B. die Tonaufnahme auf Tonband.

Aufbewahren: Das Entgegennehmen bereits aufgezeichneter Daten in der bestehenden Verkörperung und Bereithalten zur eigenen Verwendung. Beispiel: Annahme einer Diskette mit einer Adressdatei.

Datenträger: Jedes Medium, auf dem Daten lesbar festgehalten werden; dabei kommt es nicht darauf an, ob zum Lesen der Daten technische Hilfsmittel erforderlich sind oder nicht. Beispiele: Diskette, Festplatte, Notizblock.

Das technisch bedingte reine Kopieren von Daten (z.B. auf eine Sicherungsdiskette) ist kein Speichern, wenn dadurch kein neuer Verwendungszusammenhang hergestellt wird und sich die Verfügbarkeit der Daten nicht ändert.

3. **Verändern** das inhaltliche Umgestalten gespeicherter Daten, ungeachtet der dabei angewendeten Verfahren,

Inhaltliches Umgestalten: Jede Maßnahme, durch die der Informationsgehalt geändert wird. In vielen (nicht in allen) Fällen stellt die Veränderung gleichzeitig eine Löschung (der „alten“) und eine Speicherung (der „neuen“) Daten dar. Die gesetzlichen Regelungen zur Löschung und zur Speicherung sind gegenüber den Regelungen zur Veränderung die spezielleren. Dann müssen i.d.R. die gesetzlichen Voraussetzungen der Löschung und der Speicherung vorliegen, nicht die der Veränderung. Im Ergebnis ist das aber praktisch ohne Auswirkungen, weil die gesetzlichen Voraussetzungen der Veränderung identisch mit denen der Speicherung und Löschung sind.

4. **Übermitteln** das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, daß die Daten durch die datenverarbeitende Stelle an den Dritten weitergegeben werden oder daß der Dritte zum Abruf bereitgehaltene Daten abrufen,

Bekanntgeben: Vergrößerung des Personenkreises, dem die Daten zugänglich sind.

Weitergeben: Jede aktive Handlung, durch die die Information in den Bereich des Adressaten gelangt. Gemeint ist nicht nur eine technische Übermittlung z.B. mittels Computernetzwerken oder durch die Weitergabe von Computerdatenträgern, sondern auch z.B. die mündliche Mitteilung, das Lesenlassen, ein Kopfnicken oder ein „vielsagender Blick“.

Abrufen: Die Aktivität geht hier vom Empfänger aus. Er verschafft sich die Verfügung über die Daten, ohne dass eine weitere menschliche Entscheidung seitens der übermittelnden Stelle über die zu übermittelnden Daten erforderlich ist. Die Übermittlung findet erst zum Zeitpunkt des tatsächlichen Abrufs statt, nicht schon durch das Bereithalten.

Gespeicherte Daten: In irgendeiner Form verkörperte Daten, z.B. auf Diskette, Festplatte, Papier. Zum Übermitteln muss allerdings nicht diese Verkörperung weitergegeben werden. So werden z.B. schriftliche Notizen auch dadurch übermittelt, dass man die Einsicht in diese Notizen gewährt.

Durch Datenverarbeitung gewonnene Daten: Solche Daten, die aus gespeicherten Daten durch Datenverarbeitungsvorgänge, also z.B. durch Filterung oder logische Verknüpfung erst gewonnen werden.

5. Sperren das Verhindern weiterer Verarbeitung gespeicherter Daten,

Das Sperren von Daten wird gesetzlich oft dann angeordnet, wenn die Daten eigentlich gelöscht werden müssten, die Löschung aber zu aufwändig oder unmöglich ist (vgl. § 48 II 2 ASOG). Die Sperrung kann (im Gegensatz zum Löschen) i.d.R. rückgängig gemacht werden.

Das Gesetz macht keine Vorgaben zur Art und Weise der Sperrung. Möglich ist z.B. die entsprechende Markierung von Computerdaten (einzelner Datenfelder oder Datensätze) in Verbindung mit der Beschränkung des Zugriffs auf diese Daten durch die verwendete Software. Andere Möglichkeit (vgl. § 48 III ASOG): Sperren von Daten in Akten durch Anbringen eines entsprechenden Vermerks.

6. Löschen das Beseitigen gespeicherter Daten,

Beseitigen: Die Verwendung der Daten muss für die Zukunft endgültig unmöglich gemacht werden. Können die Daten rekonstruiert werden, liegt kein Löschen vor. Daher müssen alle Kopien (auch automatisch erstellte Sicherungskopien) gelöscht werden.

Beispiele:

- Schwärzung in schriftlichen Akten
- Physische Vernichtung von schriftlichen Akten oder Computerdatenträgern (Schredder)
- Überschreiben von Computerdatenträgern mit anderen Daten. Der bloße Löschbefehl in Computersoftware genügt hier oft nicht, weil dadurch nur der Platz, auf dem die „gelöschten“ Daten gespeichert sind, als frei für neue Speicherungen markiert wird; die „gelöschten“ Daten werden dadurch noch nicht mit anderen Daten überschrieben und können noch rekonstruiert werden. Empfehlenswert ist daher die Verwendung spezieller Software zum sicheren Löschen.

7. Nutzen jede sonstige Verwendung personenbezogener Daten.

Sonstige Verwendung: Verwendung, die kein Erheben, Speichern, Verändern, Übermitteln, Sperren oder Löschen darstellt.

Es muss sich um personenbezogene Daten handeln.

Beispiele:

- Auswerten von Daten durch die verarbeitende Stelle mit personenbezogenem Ergebnis (z.B. Erstellen von Listen von Personen mit bestimmten Merkmalen)
- Verwendung von Daten zur Korrespondenz mit dem Betroffenen (Adresse)
- Erstellen einer Sicherungskopie ohne Änderung der Verfügbarkeit der Daten (dann liegt keine Speicherung vor)

(3) Im Sinne dieses Gesetzes ist

1. datenverarbeitende Stelle jede Behörde oder sonstige öffentliche Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt; nimmt diese unterschiedliche gesetzli

che Aufgaben wahr, gilt diejenige Organisationseinheit als datenverarbeitende Stelle, der die Aufgabe zugewiesen ist,

Im ASOG ist nur von „Stelle“ die Rede; die Definition der datenverarbeitenden Stelle ist jedoch anzuwenden. Wichtig ist der Begriff für die Datenübermittlung: Die Übermittlungsvoraussetzungen müssen immer dann vorliegen, wenn Daten zwischen verschiedenen „Stellen“ übertragen werden.

„Daten verarbeiten lässt“: Auftragsdatenverarbeitung z.B. durch ein Service-Rechenzentrum. Entscheidend für die Definition der Stelle ist die gesetzliche Aufgabenzuordnung. Dadurch soll die Zweckbindung der Daten gesichert werden: Die Übertragung zu einer anderen Stelle mit anderen Aufgaben ist nur unter den besonderen Voraussetzungen der Datenübermittlung zulässig.

Beispiele:

- Universität
- Staatsanwaltschaft in einem bestimmten Amtsgerichtsbezirk
- Verschiedene Ämter desselben Bezirks in Berlin (z.B. Bauamt, Wirtschaftsamt)
- Die Straßenverkehrsbehörde und die Versammlungsbehörde sind als verschiedene Organisationseinheiten des Polizeipräsidenten von Berlin mit unterschiedlichen Aufgaben jeweils eigenständige datenverarbeitende Stellen.

2. Empfänger *jede Person oder Stelle, die Daten erhält,*

Es gilt die Definition der Stelle aus Nr. 1.

3. Dritter *jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene oder diejenigen Personen und Stellen, die in den Fällen der Nummer 1 im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union Daten im Auftrag verarbeitet,*

Auch der Begriff „Dritter“ hat eine besondere Bedeutung für die Datenübermittlung. Die Voraussetzungen der Datenübermittlung müssen nur dann erfüllt sein, wenn die Daten an einen „Dritten“ übertragen werden.

Der Betroffene und die Stellen, die Auftragsdatenverarbeitung betreiben, sind keine „Dritten“; die Übertragung von Daten an sie oder von ihnen ist daher meist zulässig, ohne dass die Voraussetzungen der besonderen Übermittlungsvorschriften erfüllt sein müssten.

Stellen, die Auftragsdatenverarbeitung außerhalb der Europäischen Union betreiben, sind „Dritte“.

4. automatisierte Datenverarbeitung *jede durch Einsatz eines gesteuerten technischen Verfahrens selbständig ablaufende Datenverarbeitung,*

Diese Definition weicht von der Definition des BDSG (dort in § 3 II 1) ab; das BDSG verlangt den Einsatz von „Datenverarbeitungsanlagen“. In der Sache ist aber das Gleiche gemeint. Entscheidend ist der Einsatz von Datenverarbeitungstechnik (Computern).

5. eine Datei *eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei), oder eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht automatisierte Datei),*

Der Begriff Datei hat im Datenschutzrecht eine eigene, von der technischen und umgangssprachlichen Verwendung abweichende Bedeutung. Entscheidend ist nicht das Medium (z.B.

Diskette, Festplatte, CD-ROM, Papier, Film, Videoband), sondern die Möglichkeiten, den Inhalt des Mediums auszuwerten.

automatisierte Datei: Datensammlung, die direkt (ohne manuelle Bearbeitung jedes einzelnen Datensatzes) mit Hilfe automatisierter Datenverarbeitung ausgewertet werden kann; die Auswertung muss sich dabei auf personenbezogene Merkmale beziehen. Diese Definition hängt von den technischen Möglichkeiten ab. Die automatisierte Datei muss keine Computerdatei im technischen Sinne sein.

Beispiele:

- Ein Stapel maschinenlesbarer Schecks ist eine automatisierte Datei
- eine Sammlung von reinen Bilddateien (im technischen Sinne) ist dann eine automatisierte Datei (im datenschutzrechtlichen Sinne), wenn es technische Möglichkeiten gibt, den Bildinhalt automatisch auszuwerten. Das ist heute der Fall (nicht aber noch vor wenigen Jahren).
- Textdateien (im technischen Sinne) sind i.d.R. automatisierte Dateien.

nicht automatisierte Datei: eine gleichartig aufgebaute Datensammlung, die zwar nicht mit automatisierten Verfahren ausgewertet werden kann, aber so beschaffen ist, dass eine (manuelle) Ordnung oder Auswertung der Daten nach personenbezogenen Merkmalen möglich ist. Gleichartiger Aufbau bedeutet dabei Aufbau nach einem bestimmten Ordnungsschema, z.B. die einheitliche räumliche Anordnung bestimmter Informationen auf einem Formular; eine Sortierung nach einer bestimmten Reihenfolge ist dabei nicht vorausgesetzt. In der Regel handelt es sich bei nicht automatisierten Dateien nicht um Computerdateien im technischen Sinne.

Beispiele:

- Personalkartei, Kundenkartei
- Sammlung ausgefüllter Formulare, z.B. Anträge oder Erfassungsbögen

*6. eine **Akte** jede sonstigen amtlichen oder dienstlichen Zwecken dienende Unterlage, soweit sie nicht Datei im Sinne von Nummer 5 ist; dazu zählen auch Bild- und Tonträger, nicht jedoch Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen,*

Auch der Begriff „Akte“ entspricht nicht dem umgangssprachlichen Begriff. Die Akte ist v.a. von den Dateien (Nr. 5) abzugrenzen. Akten sind also Unterlagen, die nicht gleichartig aufgebaut sind oder zumindest nicht nach personenbezogenen Merkmalen geordnet oder ausgewertet werden können. Auch Computermedien können Akten im Sinne des Datenschutzrechts sein.

Beispiele:

- Schriftliche Aufzeichnungen, es sei denn, sie erfassen mehrere gleichartige Sachverhalte nach einem bestimmten Schema mit personenbezogenen Merkmalen (dann handelt es sich um nicht automatisierte Dateien)
- CD-ROMs mit Bilddateien, die weder automatisch noch manuell nach personenbezogenen Merkmalen ausgewertet werden können (z.B. technische Bilder als Bestandteil von Sachverständigengutachten).

*7. **Anonymisieren** 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,*

Nicht notwendig ist, dass die Daten nach dem Anonymisieren überhaupt nicht mehr „personenbezogen“ sind. Die Zuordnung zu einer Person muss nicht ganz unmöglich sein, sondern nur einen unverhältnismäßigen Aufwand erfordern.

Beispiele:

- Löschung der Identifikationsmerkmale. Das reicht aber nur dann aus, wenn sich nicht aus den übrigen Daten der Personenbezug mit verhältnismäßigem Aufwand rekonstruieren lässt. Gegebenenfalls müssen weitere Merkmale gelöscht werden.
- Merkmalsaggregation: Für einzelne Merkmale werden größere Kategorien gebildet, die mehr Datensätze umfassen. So ist es möglich, anhand des Merkmals „Alter“ den einzigen Einwohner einer Gemeinde zu identifizieren, der 102 Jahre alt ist; wird das Alter allerdings nur in einer Spannweite angegeben („älter als 80 Jahre“), dann ist die Identifizierung nicht mehr ohne weiteres möglich.

8. Pseudonymisieren das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren,

Die Zuordnung des Kennzeichens (Pseudonym) zu der jeweiligen Person erfolgt durch eine Zuordnungsregel. Entscheidend ist, wer diese Zuordnungsregel kennt.

Beispiele:

- Der Betroffene selbst kennt als einziger die Zuordnungsregel
- Ein vertrauenswürdiger Dritter kennt die Zuordnungsregel
- Die datenverarbeitende Stelle selbst kennt die Zuordnungsregel. Das kann dann sinnvoll sein, wenn die Daten in pseudonymisierter Form an eine andere Stelle übermittelt werden sollen, um dem Empfänger die Identität des Betroffenen nicht zu offenbaren.

9. mobiles personenbezogenes Speicher- und Verarbeitungsmedium ein Datenträger,

a) der an den Betroffenen ausgegeben wird,

b) auf dem personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und

c) bei dem der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

Vorausgesetzt wird die Möglichkeit der Datenverarbeitung auf dem Datenträger selbst. Ein bloßes Speichermedium (z.B. Diskette) genügt daher nicht.

Gebrauch des Mediums: andere Verwendung als die bewusste Steuerung von Verarbeitungsprozessen mittels Tastatur, Sprache o.ä. Gemeint ist v.a. das Einführen in ein Lese-/Schreibgerät oder das Vorbeiführen an einem Funkempfänger.

Beispiel: Smart Card oder Chipkarte, z.B. der Krankenversicherung

II. Vorschriften über den Berliner Datenschutzbeauftragten

Wichtige Vorschriften:

§ 23

Verschwiegenheitspflicht

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. ...

§ 24

Aufgaben und Befugnisse

(1) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den Behörden und sonstigen öffentlichen Stellen. ...

(3) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit beobachtet die Auswirkungen der automatischen Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der Behörden und sonstigen öffentlichen Stellen dahingehend, ob sie zu einer Beschränkung der Kontrollmöglichkeiten durch das Abgeordnetenhaus oder die Bezirksverordnetenversammlungen führen. Er kann Maßnahmen zum Schutz gegen derartige Auswirkungen anregen. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist über die Einführung neuer Automationsvorhaben und wesentliche Änderungen automatisierter Datenverarbeitungen im Bereich der Behörden und sonstigen öffentlichen Stellen zu informieren. ...

§ 26

Beanstandungen

(1) Stellt der Berliner Beauftragte für Datenschutz und Informationsfreiheit Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzvorschriften oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

- 1. bei Behörden und sonstigen öffentlichen Stellen der Hauptverwaltung gegenüber dem zuständigen Mitglied des Senats, im übrigen gegenüber dem Präsidenten des Abgeordnetenhauses oder dem Präsidenten des Rechnungshofs,*

2. ...

3. ...

... und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. ...

§ 27

Anrufung

Jedermann kann sich an den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden, wenn er der Ansicht ist, daß bei der Verarbeitung personenbezogener Daten durch Behörden oder sonstige öffentliche Stellen gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzvorschriften verstoßen worden ist oder ein solcher Verstoß bevorsteht. Dies gilt auch für Dienstkräfte der Behörden und sonstigen öffentlichen Stellen, ohne daß der Dienstweg einzuhalten ist.

§ 28

Unterstützung

(1) Die Behörden und sonstigen öffentlichen Stellen sind verpflichtet, den Berliner Beauftragten für Datenschutz und Informationsfreiheit und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen sind dabei insbesondere

- 1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungsprogramme,*
- 2. die in Nummer 1 genannten Unterlagen und Akten herauszugeben und Kopien von Unterlagen, von automatisierten Dateien, von deren Verfahren und von organisatorischen Regelungen zur Mitnahme zur Verfügung zu stellen,*
- 3. jederzeit Zutritt in alle Diensträume und Zugriff auf elektronische Einrichtungen zu gewähren.*

Satz 2 gilt für die in § 19 a Abs. 1 Satz 7 genannten Aufgaben (Aufgaben des Verfassungsschutzes, der Gefahrenabwehr, der Strafverfolgung und der Steuerverwaltung) nicht, soweit das jeweils zuständige Mitglied des Senats im Einzelfall feststellt, daß die Einsicht in die Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet. Auf Antrag des Berliner Beauftragten für Datenschutz und Informationsfreiheit hat die Senatsverwaltung dies im zuständigen Ausschuß des Abgeordnetenhauses in geheimer Sitzung zu begründen. Die Entscheidung des Ausschusses kann veröffentlicht werden.

(2) Berufs- und Amtsgeheimnisse entbinden nicht von der Unterstützungspflicht.

§ 29

Berichte und Gutachten

...

(2) Außerdem hat er dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen. ...

III. Andere für die polizeiliche Datenverarbeitung wichtige Vorschriften des BDSG

§ 3a

Wartung

(1) Datenverarbeitungssysteme sind so zu gestalten, dass bei ihrer Wartung möglichst nicht auf personenbezogene Daten zugegriffen werden kann. Sofern dies nicht sichergestellt ist, hat die datenverarbeitende Stelle durch technische und organisatorische Maßnahmen sicherzustellen, dass nur auf die für die Wartung unbedingt erforderlichen personenbezogenen Daten zugegriffen werden kann. Dabei sind insbesondere folgende Anforderungen zu erfüllen: Es ist

- 1. sicherzustellen, dass nur dafür autorisiertes Personal die Wartung vornimmt,*
- 2. sicherzustellen, dass jeder Wartungsvorgang nur mit Wissen und Willen der speichernden Stelle erfolgen kann,*
- 3. zu verhindern, dass personenbezogene Daten im Rahmen der Wartung unbefugt entfernt oder übertragen werden,*
- 4. sicherzustellen, dass alle Wartungsvorgänge während der Durchführung kontrolliert werden können,*
- 5. sicherzustellen, dass alle Wartungsvorgänge nach der Durchführung nachvollzogen werden können,*
- 6. zu verhindern, dass bei der Wartung Programme unbefugt aufgerufen werden können, die für die Wartung nicht benötigt werden,*
- 7. zu verhindern, dass bei der Wartung Datenverarbeitungsprogramme unbefugt verändert werden können, und*

8. die Wartung so zu organisieren und zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Eine Wartung durch andere Stellen darf über die Anforderungen nach Absatz 1 hinaus nur auf Grund schriftlicher Vereinbarungen erfolgen. Darin sind folgende Regelungen zu treffen:

1. Art und Umfang der Wartung,

2. Abgrenzung der Rechte und Pflichten zwischen Auftraggeber und Auftragnehmer,

3. eine Protokollierungspflicht beim Auftraggeber und die Verpflichtung des Auftragnehmers, Weisungen des Auftraggebers zum Umgang mit den Daten auszuführen und sich an dessen Weisungen zu halten,

4. die Daten dürfen ausschließlich für den Zweck der Wartung verwendet werden,

5. Sicherstellung, dass keine Datenübermittlung an andere Stellen durch den Auftragnehmer erfolgt,

6. Löschung der Daten nach Abschluss der Wartungsarbeiten,

7. die technische Verbindung muss vom Auftraggeber hergestellt werden, sofern dies nicht möglich ist, ist ein Rückrufverfahren verbindlich festzulegen,

8. Anwesenheit des Systemverwalters ist möglichst sicherzustellen,

9. Verschlüsselung von personenbezogenen Daten auf dem Übertragungsweg nach dem jeweiligen Stand der Technik und

10. für den Fall, dass ein Auftragnehmer außerhalb der Mitgliedstaaten der Europäischen Union tätig wird, sind stets die jeweiligen Regelungen des § 14 über die Übermittlung personenbezogener Daten an ausländische und internationale Stellen anzuwenden. Die mit Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses zu verpflichten.

(3) Ist bei Wartungsarbeiten nur ein Zugriff auf Daten in verschlüsselter, pseudonymisierter oder anonymisierter Form gegeben, so dass die mit der Wartung betraute Stelle Betroffene nicht reidentifizieren kann, so sind nur Maßnahmen nach Absatz 2 Satz 1 und 3 erforderlich. Ein Zugriff darf nur zweckgebunden erfolgen.

(4) Im Sinne dieses Gesetzes ist

1. Wartung die Summe der Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Hard- und Software von Datenverarbeitungsanlagen; dazu gehören die Installation, Pflege, Überprüfung und Korrektur der Software sowie die Überprüfung und Reparatur oder der Austausch von Hardware,

2. Fernwartung die Wartung der Hard- und Software von Datenverarbeitungsanlagen, die von einem Ort außerhalb der Stelle, bei der die Verarbeitung personenbezogener Daten erfolgt, mittels Einrichtung zur Datenübertragung vorgenommen wird, und

3. Verschlüsselung das Ersetzen von Klartextbegriffen oder Zeichen durch andere in der Weise, dass der Klartext nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wieder lesbar gemacht werden kann.

§ 5a

Datenvermeidung

Die Planung, Gestaltung und Auswahl informationstechnischer Produkte und Verfahren haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Der Grundsatz der Datenvermeidung konkretisiert den allgemeinen Verhältnismäßigkeitsgrundsatz.

§ 6

Zulässigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn

1. dieses Gesetz oder
2. eine besondere Rechtsvorschrift sie erlaubt oder
3. der Betroffene eingewilligt hat.

...

(3) Wird die Datenverarbeitung auf die Einwilligung des Betroffenen gestützt, so ist dieser in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, aufzuklären. Die Aufklärungspflicht umfaßt bei beabsichtigten Übermittlungen auch den Empfänger der Daten sowie den Zweck der Übermittlung. Der Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern kann.

(4) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, so ist der Betroffene darauf schriftlich besonders hinzuweisen.

(5) Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf seiner freien Entscheidung beruht. Sie ist insbesondere unwirksam, wenn sie durch Androhung ungesetzlicher Nachteile oder durch fehlende Aufklärung bewirkt wurde. ...

§ 8

Datengeheimnis

(1) Dienstkräften von Behörden und sonstigen öffentlichen Stellen, die Daten für sich oder im Auftrag verarbeiten, ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Diese Verpflichtung ist für Personen, die bei nicht öffentlichen Auftragnehmern öffentlicher Stellen dienstlichen Zugang zu personenbezogenen Daten haben, vertraglich sicherzustellen.

(2) Die Dienstkräfte sind bei der Aufnahme ihrer Tätigkeit nach Maßgabe des Absatzes 1 zu verpflichten. Ihre Pflichten bestehen auch nach Beendigung ihrer Tätigkeit fort.

§ 9

Erforderlichkeit

(1) Nach Maßgabe der nachfolgenden Vorschriften ist die Verarbeitung personenbezogener Daten nur zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Gesetz der datenverarbeitenden Stelle zugewiesenen Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist.

§ 31b

Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit der Einsatz der Videoüberwachung zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die datenverarbeitende Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung, die Identität der verarbeitenden Stelle sowie über die

Zweckbestimmung der Verarbeitung zu benachrichtigen. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen. Eine Pflicht zur Benachrichtigung besteht nicht, wenn

- 1. eine Abwägung ergibt, dass das Benachrichtigungsrecht des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung aus zwingenden Gründen zurücktreten muss,*
- 2. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,*
- 3. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder*
- 4. die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist.*

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 3 oder 4 abgesehen wird.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

§ 31b BlnDSG betrifft nur die Videoüberwachung von Räumen, nicht von Straßen und Plätzen.

C. Nicht anwendbare Vorschriften des BlnDSG

Bezüglich des Verhältnisses zwischen BlnDSG und ASOG enthält § 51 ASOG eine ausdrückliche Normierung des Spezialitätsgrundsatzes. Demnach finden die Vorschriften der §§ 6a, 9 II und der §§ 10 bis 17 BlnDSG im Anwendungsbereich des ASOG keine Anwendung.

§ 6a BlnDSG lautet:

(1) Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen oder die die Gesundheit oder das Sexualleben betreffen, dürfen nur verarbeitet werden, wenn angemessene Garantien zum Schutz des Rechts auf informationelle Selbstbestimmung bestehen und eine besondere Rechtsvorschrift, die den Zweck der Verarbeitung bestimmt, dies erlaubt.

...

Die genannten Daten dürfen also im Anwendungsbereich des ASOG verarbeitet werden.

§ 9 II BlnDSG lautet:

Sind personenbezogene Daten in Akten derart verbunden, daß ihre Trennung nach erforderlichen und nicht erforderlichen Daten auch durch Vervielfältigung und Unkenntlichmachung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, so sind die Kenntnisnahme, die Weitergabe innerhalb der datenverarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgabe erforderlich sind, ... zulässig. Diese Daten unterliegen insoweit einem Verwertungsverbot.

„Überflüssige“ personenbezogene Daten in Akten dürfen daher im Anwendungsbereich des ASOG selbst dann nicht zur Kenntnis genommen, weitergegeben oder übermittelt werden, wenn sie mit den erforderlichen Daten in der genannten Weise verbunden sind.

§§ 10 bis 17 BlnDSG regeln die Datenerhebung, Zweckbindung, Datenübermittlungen, Abrufverfahren, Auskunft, Benachrichtigung und Einsichtnahme sowie Berichtigung, Sperrung

und Löschung von Daten und das Widerspruchsrecht. Für diese Gegenstände enthält das ASOG eigene Spezialregelungen v.a. in den §§ 42 ff., aber auch bei einzelnen Standardmaßnahmen (z.B. hinsichtlich der Zweckbindung in § 18 VII: „zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität“).

§ 15a BlnDSG lautet:

Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Eine Entscheidung nach Satz 1 kann durch Gesetz zugelassen werden, wenn es die Wahrung der berechtigten Interessen des Betroffenen sicherstellt.

Weil gem. § 51 ASOG auch diese Vorschrift im Bereich des ASOG nicht anwendbar ist, sind hier solche „automatisierten Einzelentscheidungen“ zulässig.

Kapitel 4: Ermittlungen, Befragungen, Datenerhebungen (§ 18 I-VI ASOG)

- Verhältnis Ermittlung/Befragung: Befragungen sind ein Unterfall von Ermittlungen
- Verhältnis Ermittlung/Datenerhebung: Der Begriff der Datenerhebung bestimmt sich nach § 4 II Nr. 1 BlnDSG und ist auf personenbezogene Daten beschränkt. Datenerhebung ist daher nicht lediglich ein Unterfall der Ermittlung. So können Ermittlungen auch zur Erlangung nicht personenbezogener Daten dienen; dann sind sie keine Datenerhebung.
- Verhältnis Befragung/Datenerhebung: Der Zweck der Befragung kann, muss aber nicht die Erhebung personenbezogener Daten sein. Grundsätzlich sind von den beiden Maßnahmen verschiedene Grundrechtspositionen betroffen: bei der Befragung die allgemeine Handlungsfreiheit (Art. 2 I GG), bei der Erhebung personenbezogener Daten die informationelle Selbstbestimmung (Art. 2 I i.V.m. 1 I GG). Im Falle der Datenerhebung durch Befragung eines Dritten können auch verschiedene Grundrechtsträger betroffen sein.

A. Rechtsfolge

I. Befragung

1. Eingriffscharakter der Befragung

Abgrenzung: Polizeiliche (eingriffsrelevante) Befragung oder informatorische Befragung

Verbindlichkeit als Eingriffskriterium: Die Befragung ist dann ein Eingriff, wenn sie aus der Sicht des Bürgers verbindlich ist, weil entweder eine gesetzliche Duldungspflicht besteht oder der befragende Polizeibeamte den Eindruck der Verbindlichkeit erweckt.

Ein Eingriff liegt vor z.B. bei „*aufgezügelter Zwangskommunikation*“, z.B. Anhalten, Beamte folgen der Person, entfernen sich nicht aus Wohnung etc.

Kein Eingriff liegt dagegen vor, wenn dem Betroffenen bewusst ist, dass er sich entziehen kann, weil keine Duldungspflicht besteht, z.B. bei erkennbar unverbindlichem Befragen (Fragen nach dem Weg, Fragen in die Menge) oder bei aufgedrängter Information.

2. Befugnisse:

- Befragung (Duldungspflicht des Befragten)
- Möglichkeit, den Befragten für die Dauer der Befragung anzuhalten
- Pflicht des Befragten zur Auskunft über Personalien
- unter bestimmten Voraussetzungen Pflicht des Befragten zu weiteren Auskünften.

3. Auskunftsverweigerungsrechte (§ 18 VI i.V.m. §§ 52-55 StPO)

Fraglich ist, ob sich hieraus nur ein Verweigerungsrecht bezüglich möglicher Straftaten oder Ordnungswidrigkeiten ergibt oder auch ein gefahrenabwehrbezogenes; erstere Interpretation ist vorzugswürdig.

II. Ermittlung

Ermittlungen sind alle nach außen zielenden Verwaltungshandlungen, die darauf abzielen, einen Sachverhalt aufzuklären. Ermitteln ist das Verschaffen von Informationen als Entscheidungsgrundlage für behördliches Handeln.

§ 18 I ASOG ist die präventiv-polizeiliche Ermittlungsgeneralklausel. Da viele Ermittlungstätigkeiten speziell geregelt sind, findet die Generalklausel nur in wenigen Fällen Anwendung.

Offene und verdeckte Ermittlung:

§ 18 II ASOG gilt für alle Ermittlungen, nicht nur für die nach der Generalklausel des § 18 I ASOG. Die Vorschrift unterscheidet zwischen offener und verdeckter Ermittlung. Die offene Ermittlung ist nach § 18 II ASOG der Regelfall, die verdeckte nur als Ausnahme unter besonderen Voraussetzungen zulässig. Problematisch ist die Abgrenzung:

1. Ansicht: Eine Ermittlung ist nur dann verdeckt, wenn heimliche oder getarnte Maßnahmen vorgenommen werden, insbesondere die Zugehörigkeit zur Polizei bewusst verschleiert wird. Beispiel: verdeckter Ermittler.

2. Ansicht: Eine Ermittlung ist schon dann verdeckt, wenn sie für die betroffene Person überhaupt nicht oder jedenfalls nicht als polizeilich wahrnehmbar ist. Offen ist dann nur die Ermittlung, bei der die betroffene Person weiß, dass jemand in seiner Eigenschaft als Polizeibeamter ihm gegenüber eine Ermittlungsmaßnahme vornimmt. Beispiel: offene Befragung.

Die 2. Ansicht ist vorzugswürdig, weil nur sie den Anforderungen des BVerfG im Volkszählungsurteil gerecht wird. Wesentlich für das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 I i.V.m. 1 I GG ist nämlich, dass der Betroffene erkennen können muss, welche Informationen über ihn bekannt werden.

III. Erhebung personenbezogener Daten

Datenerhebung ist nach § 4 II Nr. 1 BlnDSG das Beschaffen von Informationen über die betroffene Person.

Viele spezielle Mittel und Methoden der Datenerhebung sind in Spezialnormen geregelt (v.a. in den Standardbefugnissen nach §§ 19 ff. ASOG, z.B. Durchsuchung, Identitätsfeststellung). Ist dies der Fall, so sind nur die Spezialnormen anzuwenden, ein Rückgriff auf § 18 I ASOG kann nicht stattfinden.

Für den Anwendungsbereich des § 18 I ASOG bleiben daher nur wenige nicht spezialgesetzlich geregelte Mittel und Methoden der Datenerhebung übrig.

Beispiele: offenes oder verdecktes Belauschen ohne technische Mittel (kein Fall des § 25 ASOG) und kurzfristiges Observieren (auch kein Fall des § 25 ASOG). Dagegen kann die Videoüberwachung öffentlicher Straßen und Plätze nicht auf § 18 I ASOG gestützt werden, weil diese Maßnahme so eingriffsintensiv ist, dass sie der Ermächtigung durch eine besondere Befugnisnorm bedarf (vgl. auch den neu eingefügten § 24a ASOG für die Videoüberwachung an gefährdeten Objekten).

B. Tatbestand

I. Befragung (Abs. 3, 4)

1. Befugnis zur Befragung und zum Anhalten

Befragung muss zu Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich sein. Aufgaben ergeben sich aus § 1 ASOG. Strafverfolgung ist hier nicht gemeint (arg. § 17 II ASOG).

Erforderlich ist die Annahme, dass die befragte Person sachdienliche Angaben machen kann; diese Annahme muss an nachvollziehbare Tatsachen anknüpfen, bloße Vermutungen reichen nicht aus.

2. Auskunftspflicht zu Personalien

Gleiche Voraussetzungen wie Befragung.

3. weitere Auskunftspflicht

§ 18 begründet selbst keine Auskunftspflicht, sondern setzt diese voraus.

Umstritten ist, ob sich die Pflicht auch aus dem ASOG ergeben kann. Vertretbar ist die Ansicht, dass sich im Falle des Vorliegens einer konkreten Gefahr die Auskunftspflicht aus §§ 13, 14, 16 ASOG ergibt; die Befragung kann dabei auch den Zweck haben, den Störer zu ermitteln.

Auskunftspflichten können sich z.B. aus § 22 GastStG, § 52 BImSchG, § 10 BSeuchG ergeben.

Umstritten ist, ob sich Auskunftspflichten aus §§ 138, 323c StGB ergeben können. Das wird jedenfalls in den Fällen abzulehnen sein, in denen sich der Befragte durch entsprechende Auskünfte selbst belasten würde.

4. Besondere Voraussetzungen für die Befragung Dritter (§ 18 Abs. 4)

3 Alternativen:

- zu befragende Person ist nicht oder nicht rechtzeitig erreichbar; betrifft auch z.B. nicht ansprechbare Verletzte
- unverhältnismäßig hoher Aufwand einer direkten Befragung, z.B. wenn ein Dolmetscher herbeigezogen werden müsste. Dabei dürfen schutzwürdige Belange des Betroffenen nicht entgegenstehen; daher ist eine Abwägung mit der Sensibilität der erfragten Daten erforderlich
- Gefährdung der Aufgabenerfüllung, z.B. wenn die Gefahr der Tatsachenverschleierung besteht.

II. Ermittlung

Zweck der offenen und der verdeckten Ermittlung muss die Klärung des Sachverhalts in einer bestimmten polizeilichen Angelegenheit sein.

Verdeckte Ermittlungen sind nur zulässig, wenn

- das ASOG die verdeckte Maßnahme ausdrücklich zulässt, z.B. bei Observation und Einsatz technischer Mittel nach § 25 ASOG, Einsatz von V-Leuten und verdeckten Ermittlern nach § 26 ASOG und der polizeilichen Beobachtung nach § 27 ASOG

oder

- bei Gefährdung der Aufgabenerfüllung

oder

- wenn die verdeckte Maßnahme dem überwiegenden Interesse des Betroffenen entspricht (Anwendungsfälle für diese Alternative unklar).

Verdeckte Ermittlungen sind in jedem Fall *unzulässig*, wenn das Gesetz verdeckte Ermittlungen ausdrücklich verbietet, z.B.

- § 19 S. 2: Verbot bei Datenerhebung zur Vorbereitung für Hilfeleistung bei Gefahrenfällen,
- 24 I S. 3 ASOG: Verbot verdeckter Ton- und Bildaufzeichnungen bei Veranstaltungen und Ansammlungen.

III. Datenerhebung

Bei allen Fällen der Datenerhebung müssen die Voraussetzungen der Ermittlung erfüllt sein („im Zusammenhang“); auch die Datenerhebung muss also zur Klärung des Sachverhalts in einer bestimmten polizeilichen Angelegenheit erfolgen. Zusätzlich müssen die Voraussetzungen eines speziellen Tatbestandes erfüllt sein:

1. Datenerhebung zur Gefahrenabwehr

Voraussetzung ist eine konkrete Gefahr i.S.v. § 17 ASOG.

2. Datenerhebung zur Erfüllung übertragener Aufgaben

Erfüllung übertragener Aufgaben: § 1 II ASOG.

Diese Befugnis greift nur, wenn in den entsprechenden Rechtsvorschriften keine abschließende Regelung getroffen wurde (vgl. § 17 II ASOG). Die Befugnis gilt insbesondere nicht für die Verfolgung von Straftaten und Ordnungswidrigkeiten, auch nicht im Bereich des Versammlungsrechts. Es fragt sich daher, welcher Anwendungsbereich noch übrig bleibt, da weitestgehende Regelungen der Datenerhebung in speziellen Gesetzen vorliegen (z.B. StVG, GewO).

3. Datenerhebung zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung

Datenerhebung muss „erforderlich“ sein: Verhältnismäßigkeitsgrundsatz.

Zum Begriff der vorbeugenden Straftatenbekämpfung vgl. § 1 III ASOG: Verhütung von Straftaten und Vorsorge für zukünftige Strafverfolgung.

Zum Begriff der Straftaten von erheblicher Bedeutung vgl. § 17 III, IV ASOG: Verbrechen, bestimmte Vergehen und auch bestimmte Ordnungswidrigkeiten. V.a. bei Ordnungswidrigkeiten kann der Verhältnismäßigkeitsgrundsatz einer Datenerhebung zur vorbeugenden Straftatenbekämpfung entgegenstehen.

4. Datenerhebung zum Schutz privater Rechte

Es gelten die Einschränkungen des § 1 IV ASOG; die Datenerhebung muss darüber hinaus zum Schutz privater Rechte „erforderlich“ sein (Verhältnismäßigkeitsgrundsatz).

Beispiel: Erhebung der Daten eines Kfz-Halters, der sein Fahrzeug besitzstörend abgestellt hat.

5. Datenerhebung zur Leistung von Vollzugshilfe

Zur Vollzugshilfe vgl. §§ 1 V, 52 ff ASOG. Die Datenerhebung muss zur Leistung von Vollzugshilfe „erforderlich“ sein (Verhältnismäßigkeitsgrundsatz).

C. Adressat

- § 18 I 1 knüpft nicht an eine Gefahr an; daher hier kein Rückgriff auf §§ 13, 14, 16. Adressat ist die Person, die zur Klärung des Sachverhalts beitragen kann.
- § 18 I 2 enthält eine Adressatenregelung (Verweisung auf §§ 13, 14 16 ASOG und Nennung „anderer“ Personen). Der Hinweis auf „andere“ Personen bezieht sich nur auf die übertragenen Aufgaben, nicht auf die Gefahrenabwehr. Also gelten für Nichtstörer im Bereich der Gefahrenabwehr insbesondere die Einschränkungen des § 16 ASOG.
- § 18 I 3 enthält keine Adressatenregelung. Es gelten die allgemeinen Regeln. Für Datenerhebung zur vorbeugenden Straftatenbekämpfung gilt § 16 III ASOG. Die Formulierung „grundsätzlich nur“ in § 16 III ASOG wird teilweise so ausgelegt, dass Ausnahmen möglich sein sollen (z.B. Kontakt- und Begleitpersonen potenzieller Straftäter, so die Regelung in einigen anderen Polizeigesetzen).

D. Zuständigkeit

Ermittlungen, Befragungen und Datenerhebungen nach § 18 I 1, 2, also zur Gefahrenabwehr und zur Erfüllung übertragener Aufgaben: Ordnungsbehörden und Polizei.

Datenerhebungen nach § 18 I 3: nur Polizei.

E. Verfahrensvorschriften

Befragung: Hinweispflichten (§ 18 V ASOG).

F. Bezüge zu anderen Vorschriften

§ 21: Auskunftspflicht zu Personalien. Der Unterschied besteht darin, dass in § 18 kein Mittel zur Durchsetzung dieser Pflicht geregelt ist (bei § 21 gibt § 23 I Nr. 1 ASOG die Möglichkeit, die Identität mittels erkennungsdienstlicher Maßnahmen festzustellen; im Rahmen von § 18 gibt es diese Möglichkeit nicht).

G. Probleme

Datenerhebung zur vorbeugenden Straftatenbekämpfung: problematisch u.a. wegen weiter Tatbestandsfassung, Gesetzgebungskompetenz.

Kapitel 5: Kontrollen zur vorbeugenden Bekämpfung grenzüberschreitender Kriminalität (§ 18 VII ASOG)

Diese Maßnahme (andere Bezeichnung: Schleierfahndung) wurde durch Gesetz v. 11.5.1999 in das ASOG eingefügt.

Zweck: Ausgleich der Kontrollmöglichkeiten nach Wegfall der EU-Binnengrenzen.

A. Rechtsfolge

4 Maßnahmen:

- kurzzeitiges Anhalten
Zweck: Ermöglichung der Befragung, der Kontrolle der Ausweispapiere, der Augenscheinnahme mitgeführter Sachen
- Befragen
Anders als beim Befragen nach § 18 III ASOG besteht bei § 18 VII ASOG keine Auskunftspflicht z.B. bezüglich der Personalien. Auskunftspflichten können sich allenfalls aus anderen Gesetzen ergeben.
- Aushändigenlassen mitgeführter Ausweispapiere

Schwierigkeiten bei der Durchsetzung dieser Befugnis: § 18 VII sieht eine Durchsuchung der Person nicht vor; bezüglich der mitgeführten Sachen ist nur eine „Inaugenscheinnahme“ erlaubt (s.u.). Falls der Adressat behauptet, keine Papiere mitzuführen, gibt es daher keine brauchbare Befugnis zum Auffinden eventuell mitgeführter Papiere. Auch eine Identitätsfeststellung nach anderen Vorschriften dürfte dann kaum zulässig sein: § 21 I ASOG greift nicht, weil die Weigerung, die Papiere auszuhändigen, noch keine Gefahr für die öffentliche Sicherheit begründet, und eine Identitätsfeststellung als repressive Maßnahme (§§ 46, 53 OWiG i.V.m. § 163b StPO) wegen Verstoßes gegen § 111 I OWiG (falsche Namensangabe gegenüber zuständigem Amtsträger) ist auch nicht möglich, weil der Adressat nach § 18 VII ASOG nicht zur Angabe der entsprechenden Personaldaten verpflichtet ist.

Prüfung der Ausweispapiere: z.B. Prüfung auf Fälschung, nicht aber Erhebung der Personaldaten. § 18 VII gibt auch keine Befugnis für eine Datenabfrage oder einen Datenabgleich. Entsprechende Befugnisse müssen aus den jeweiligen Spezialvorschriften abgeleitet werden, z.B. §§ 18, 28 ASOG.

- Inaugenscheinnahme mitgeführter Sachen

Inaugenscheinnahme ist weniger als Durchsuchung. Andererseits ist nach allerdings umstrittener Auffassung nicht nur das bloße äußere Betrachten (z.B. eines Kfz) gemeint, sondern auch das Öffnen mitgeführter Behältnisse sowie eines Kofferraums oder der Ladefläche eines Kfz. Auch das Anheben einer Abdeckung ist demnach von der Befugnis erfasst. Eine weitergehende Durchsuchung wäre aber jedenfalls nur unter den Voraussetzungen etwa von § 21 III 4 ASOG oder § 35 ASOG zulässig. Denkbar ist z.B., dass die Inaugenscheinnahme zur Entdeckung von Tatsachen führt, die die Annahme rechtfertigen, dass sich in der Sache eine andere Sache befindet, die sichergestellt werden darf; dann wäre eine Durchsuchung nach § 35 I Nr. 3 ASOG zulässig.

Trotz der Bezeichnung beschränkt sich die Inaugenscheinnahme nicht auf die optische Wahrnehmung. Vielmehr ist jede sinnliche Wahrnehmung erfasst, also auch z.B. Hören, Riechen,

Schmecken oder Fühlen. Auch der Einsatz von Diensthunden zum Aufspüren von Betäubungsmitteln oder Sprengstoff soll demnach zulässig sein (str.).

B. Tatbestand

Folgende Merkmale müssen kumulativ vorliegen:

- Zweck: vorbeugende Bekämpfung der grenzüberschreitenden Kriminalität.
Der Begriff „grenzüberschreitende Kriminalität“ ist im ASOG nicht näher definiert; sein Sinn erschließt sich auch nicht aus den Gesetzesmaterialien. Unter Zuhilfenahme anderer Landespolizeigesetze ergibt sich aber folgende Möglichkeit der Auslegung:
Es handelt sich um Straftaten, bei denen sich die Täter den Grenzkontrollabbau innerhalb der EU sowie die Öffnung der Grenzen zu den Staaten des ehemaligen Ostblocks nutzbar machen, z.B. indem Tatbeiträge in mehreren Staaten geleistet werden, der Täter sich oder eine Sache ins Ausland in Sicherheit bringen oder eine deliktisch erlangte oder zu verwendende Sache einführen will oder bei Einschleusung oder illegaler Einreise ins Bundesgebiet.
Beispiele: Kraftfahrzeug- oder Abfallverschiebung, Ein- oder Ausfuhr von Waffen, Sprengstoff, Rauschgift, Nuklearmaterial oder Falschgeld, grenzüberschreitender Menschenhandel.

vorbeugende Kriminalitätsbekämpfung: zum Begriff vgl. § 1 III ASOG, d.h. Verhütung von Straftaten und Vorsorge für die Verfolgung künftiger Straftaten. Im Rahmen von § 18 VII ASOG liegt der Schwerpunkt bei der Verhütung von Straftaten; der Gesetzgeber hatte v.a. die abschreckende Wirkung der verdachtsunabhängigen Kontrollen vor Augen.
- Antreffen einer Person im öffentlichen Verkehrsraum.
Öffentlicher Verkehrsraum: Begriff stellt nicht auf Eigentumsverhältnisse ab, sondern auf allgemeine Zugänglichkeit. Keine Beschränkung auf Straßenverkehr. Also z.B. auch Gelände einer Tankstelle, Parkplatz einer Gaststätte oder eines Supermarkts, Binnengewässer, denkbar sogar der Luftraum. Person kann z.B. Fahrzeugführer, Fahrzeuginsasse oder bloßer Fußgänger sein.
- Aufgrund von Lagekenntnissen ist anzunehmen, dass Straftaten von erheblicher Bedeutung begangen werden sollen.
Straftaten von erheblicher Bedeutung: Definition in § 17 III, IV ASOG. Es muss sich um Straftaten der grenzüberschreitenden Kriminalität handeln.
Lagekenntnisse: Es muss Anhaltspunkte dafür geben, dass solche Straftaten begangen werden sollen, und dass die Täter an dem Ort der Kontrolle möglicherweise anzutreffen sind. Ausreichend sind z.B. Erkenntnisse über Örtlichkeiten und Wege, die die grenzüberschreitende Kriminalität benutzt. „Tatsachen“, die sich auf einen konkreten Einzelfall beziehen (vgl. z.B. die entsprechende Formulierung in § 18 III 1 ASOG), brauchen nicht vorzuliegen (daher sind die Kontrollen nach § 18 VII ASOG „verdachtsunabhängig“).

C. Adressat

Der Adressat ergibt sich aus § 18 VII ASOG selbst; Adressat ist demnach die Person, die den Voraussetzungen des § 18 VII ASOG entsprechend im öffentlichen Verkehrsraum angetroffen wird. Die allgemeinen Vorschriften der §§ 13, 14, 16 ASOG sind nicht anwendbar, weil die Befugnis des § 18 VII ASOG keine konkrete Gefahr voraussetzt.

D. Zuständigkeit

Zuständig für die Maßnahme ist gem. § 18 VII 1 ASOG die Polizei.

E. Verfahrensvorschriften

- Gem. § 18 VII 3 ASOG müssen Ort, Zeit und Umfang der Maßnahmen durch den Polizeipräsidenten oder seinen Vertreter angeordnet werden. Außerdem ist gem. § 18 VII 4 ASOG nach 14 Tagen zu prüfen, ob die Voraussetzungen der Maßnahmen weiterhin vorliegen.
- Beim Befragen gibt es – anders als bei der Befragung nach § 18 III ASOG – keine Belehrungspflicht.

F. Bezüge zu anderen Vorschriften

Sobald die Inaugenscheinnahme mitgeführter Sachen oder die Prüfung der Ausweispapiere Tatsachen offenlegt, aus denen sich das Vorliegen einer konkreten Gefahr ergibt, können weitere Maßnahmen aufgrund anderer Befugnisnormen (bei Vorliegen von deren Voraussetzungen) ergriffen werden.

G. Probleme

Wegen mangelnder Befugnisregelungen zur Durchsuchung, zur Befragung und zur Identitätsfeststellung in § 18 VII ASOG ist die Wirksamkeit der Maßnahme insgesamt zweifelhaft.

Kapitel 6: Erhebung von Daten zur Vorbereitung für die Hilfeleistung in Gefahrenfällen (§ 19 ASOG)

Zweck: Vorbereitung auf künftige Gefahrenlagen durch Informationsbeschaffung über bestimmte Personen. Die Maßnahme ist der eigentlichen Gefahrenabwehr vorgelagert.

A. Rechtsfolge

Erhebung bestimmter personenbezogener Daten: Namen, Vornamen, akademische Grade, Anschriften, Telefonnummern und andere Daten über die Erreichbarkeit (z.B. Telefonnummern, Melderufempfänger) sowie „nähere Angaben“ über die Zugehörigkeit zu einer der in der Vorschrift genannten Personengruppen.

„Nähere Angaben“: z.B. zur Zuverlässigkeit eines Anlagenbetreibers, zur mehrsprachigen Einsatzmöglichkeit eines Dolmetschers.

Freiwillige Angaben fallen nicht unter § 19 (kein Eingriff).

B. Tatbestand

- Betroffene Personen:
 1. Personen, deren Kenntnisse oder Fähigkeiten zur Gefahrenabwehr benötigt werden; z.B. Hausmeister, Dolmetscher, Abschlepp- und Bestattungsunternehmer, Ärzte (sog. Polizeihelfer)
 2. Verantwortliche für gefährliche Anlagen oder Einrichtungen; z.B. Inhaber von Tanklagern, Atomkraftwerken, chemischen Betrieben etc.
 3. Verantwortliche für gefährdete Anlagen oder Einrichtungen; z.B. Gebäude, die Ziel von Anschlägen sein können.
 4. Verantwortliche für öffentliche Veranstaltungen, die nicht dem Versammlungsrecht unterliegen; nicht nur Veranstalter, sondern z.B. auch Pächter oder Eigentümer des Grundstücks. Veranstaltung ist ein geplantes, aus dem Alltag herausgehobenes, zeitlich eingrenzbares Ereignis. Die Veranstaltung muss öffentlich zugänglich sein (nicht wenn Eintritt verlangt wird).
- Erforderlichkeit der Datenerhebung für die Vorbereitung der Hilfeleistung und das Handeln in Gefahrenfällen (auch hinsichtlich des Umfangs der Daten). Ohne die beabsichtigte Datenerhebung müssen das Handeln oder die Hilfeleistung in Gefahrenfällen nicht oder nur mit unverhältnismäßigem Aufwand möglich sein.

C. Adressat

Direkt aus § 19. Die allgemeinen Regeln (§§ 13, 14, 16 ASOG) sind nicht anwendbar, weil § 19 keine Gefahr voraussetzt.

D. Zuständigkeit

Ordnungsbehörden und Polizei nach § 19.

E. Verfahrensvorschriften

- Keine verdeckte Datenerhebung, § 19 S. 2
- Aber Datenerhebung ohne Kenntnis des Betroffenen („nicht bei der betroffenen Person“) zulässig. Dann nachträgliche Mitteilung an Betroffenen über Datenerhebung und deren Zweck, § 19 S. 3
- Widerspruch zulässig, § 19 S. 4. Hat nur deklaratorische Bedeutung.

F. Bezüge zu anderen Vorschriften

Im Umweltrecht, z.B. Atomrecht, Immissionsschutzrecht etc. gibt es spezielle Auskunfts- und Anzeigepflichten. Diese gehen dem § 19 vor.

Kapitel 7: Überblick über die automatisierte Datenverarbeitung bei Ordnungsbehörden und Polizei in Berlin

Wichtige Begriffe:

- Verbunddatei: Daten können von den Ländern online direkt in den Zentralrechner beim BKA eingegeben und von dort abgerufen werden
- Zentraldatei: konventionelle Übersendung der Daten an das BKA, das sie in die Datei eingibt; die Daten können dann an die Länder übermittelt oder zum Abruf bereitgestellt werden

Von der Polizei geführte Dateien:

ISVB

Informationssystem Verbrechensbekämpfung
Integrierter Bestandteil des bundesweit geführten INPOL (Informationssystem Polizei, s.u.)
Das ISVB als Großnetzverbund des Landes Berlin wird durch die Berliner Polizei betrieben und besteht seit dem 1.1.1983. Informationen über Beschuldigte oder auch Zeugen/Anzeigende, die im Zusammenhang mit strafprozessualen Ermittlungsverfahren stehen, werden allen Abfrageberechtigten (Identifikation über einen Kartenleser mit einem speziell codierten Anwenderausweis) zur Verfügung gestellt. Keine Informationen im Rahmen der Gefahrenabwehr oder mit Bezug auf Verkehrsstraftaten. Auswertung und Recherche für einen konkreten Anlass oder zur Erstellung der polizeilichen Kriminalstatistik (PKS). Sämtliche Zugriffe werden gespeichert, so dass später ermittelt werden kann, wer wann auf welche Daten zugegriffen hat.
Bestandteile u.a.: Straftaten- und Straftäterdatei, Namensindexdatei, Fahndungsdatei INPOL, Statistikdatei, Berechtigendatei, Ordnungsbuch- und Tagebuchdatei.

POLIKS

Nachfolgesystem für das ISVB (moderner und einfacher).

SIS

Schengener Informationssystem
Personen- und Sachfahndungssystem im Rahmen des Schengener Übereinkommens. Bundes- oder EU-weite Personenfahndungsersuchen werden in Berlin über das ISVB als Verbundnachricht an den Verbund-INPOL-Rechner überführt und für internationale Fahndungen über das BKA an die übrigen EU-Staaten in das SIS geleitet; keine automatische Weiterleitung auf das EU-Gebiet. Sachfahndungen werden dagegen direkt mit der Eingabe in das ISVB automatisch in den Datenbestand des SIS übernommen.
Das Schengener Durchführungsübereinkommen enthält in Art. 102-118 Datenschutzbestimmungen für das SIS.
Im Zuge der Erweiterung der EU wird das SIS gegenwärtig überarbeitet. Ziel ist ein neues System (SIS II), an dem auch die neuen Mitgliedstaaten beteiligt sind.

INPOL	Informationssystem der Polizei. Das INPOL-Bund-System enthält Datensammlungen, die entweder als Verbunddateien oder Zentraldateien allen Ländern zur Verfügung stehen.
Personenfahndungsdatei	Bundesweite Verbunddatei, geführt vom BKA (vgl. § 9 I BKAG). Bestandteil von INPOL. Enthält Daten über Personen, die zur Fahndung ausgeschrieben sind mit dem Ziel der Festnahme (aufgrund eines Haftbefehls), der Ingewahrsamnahme, der Aufenthaltsermittlung oder (bei Ausländern) der Ausweisung, Abschiebung oder Zurückweisung. Enthält außerdem Daten von Personen, die zur polizeilichen Beobachtung ausgeschrieben sind. Außer Personalien werden auch personengebundene Hinweise gespeichert wie z.B. „bewaffnet“, „gewalttätig“, „Prostitution“, „BTM-Konsument“, „geisteskrank“.
Sachfahndungsdatei	Bundesweite Verbunddatei mit Daten zu Gegenständen, die zum Zwecke der Beweissicherung, Einziehung, Eigentumssicherung zur Fahndung ausgeschrieben sind. Auch Daten zu Kfz, deren Kennzeichen zu entstempeln ist bzw. die zur polizeilichen Beobachtung ausgeschrieben sind, sowie abhanden gekommenen Ausweisen. Bestandteil von INPOL.
Haftdatei	Bundesweite Verbunddatei, geführt vom BKA (vgl. § 9 II BKAG), Bestandteil von INPOL. Enthält die Daten aller Personen, die sich aufgrund richterlich angeordneter Freiheitsentziehung in Justizverwahrung befinden. Löschung der Daten 2 Jahre nach Haftentlassung. Zweck: Die Fahndung nach in Haft befindlichen Personen soll vermieden werden, außerdem Alibiüberprüfung, Überwachung bevorstehender Haftentlassungen. Gespeichert werden Personalien (auch Aliasnamen) und Haftdaten.
Erkennungsdienstdatei	Bundesweite Verbunddatei, geführt vom BKA (vgl. § 8 VI BKAG), Bestandteil von INPOL. Enthält Daten über alle Personen, die erkennungsdienstlich behandelt wurden und deren erkennungsdienstliche Unterlagen aufbewahrt werden, insgesamt ca. 3.800.000 Datensätze. Gespeichert sind Personalien, Angaben zur Personenfeststellung, Angaben zur erkennungsdienstlichen Behandlung und die Aktenzeichen beim BKA bzw. der Dienststelle, die die erkennungsdienstliche Behandlung durchgeführt hat.
Datei Daktyloskopie	Bundesweite Verbunddatei, geführt vom BKA (vgl. § 8 VI BKAG), Bestandteil von INPOL. Enthält verformelte Fingerabdrücke; Zugriff auch über die Fingerabdruckformel.
AFIS	Automatisches Fingerabdruck-Informationssystem Bundesweite Zentraldatei, geführt vom BKA (vgl. § 8 VI BKAG), Bestandteil von INPOL. Fingerabdruckblätter werden automatisch eingelesen, digitalisiert und verformelt und mit dem vorhandenen Datenbestand abgeglichen. Erfassungszeit von wenigen Minuten, bei einer Treffsicherheit von 99 %.
VERMIUTOT	Bundesweite Zentraldatei, geführt vom BKA (vgl. § 9 III BKAG), Bestandteil von INPOL. Enthält Daten vermisster sowie unbekannter hilfloser Personen und Toter. Erfasst werden Daten zur Personenbeschreibung und auch ggf. über Gründe des Verschwindens („Un

glück“, „Familienzwistigkeiten“, „Trunksucht“, „Abenteurer“, „Streuner“, „Furcht vor Strafe“).

SPUDOK

Spurendokumentationssystem für die vorübergehende Unterstützung umfangreicher Ermittlungstätigkeiten, Bestandteil von INPOL. Das Spuren- und Hinweisaufkommen eines Falles wird vollständig gespeichert, einschließlich der Daten zu Anzeigeerstattem, Zeugen und Hinweisgebern. Formatfreie Texteingabe, daher auswertbar nach beliebigen Stichwörtern oder Namen. Zugriff hat in der Regel nur die die Ermittlungen führende Stelle; allerdings ist auch die Einrichtung eines länderübergreifenden oder bundesweiten Zugriffs möglich. Die Dateien werden nach Abschluss der Ermittlungen gelöscht bzw. archiviert. Die Löschung kann rechtlich problematisch sein, weil u.U. die Verteidigung oder die Staatsanwaltschaft auch nach Abschluss der polizeilichen Ermittlungen Zugriff auf die Daten haben möchte.

PIOS

Personen, Institutionen, Objekte und Sachen

Datei zur Sammlung und Auswertung des Inhalts von Ermittlungsakten zu Straftaten der Schwerekriminalität (Terrorismus, BTM, Landesverrat usw.); Bestandteil von INPOL; eingeführt 1975 im Zusammenhang mit der Terrorismusbekämpfung. Inzwischen ergänzt u.a. um Informationen zu Sachverhalten. PIOS ist geeignet zum Auffinden von Beziehungen zwischen Personen, Institutionen, Objekten und Sachen. Sein Zweck beschränkt sich nicht auf die Aufklärung einzelner Straftaten, sondern umfasst die Beobachtung eines ganzen Kriminalitätsbereichs, auch zur Gefahrenabwehr. Diese unklare Begrenzung des Zwecks der Datei ist datenschutzrechtlich problematisch. Problematisch ist auch die bei PIOS vorgesehene Erfassung „anderer Personen“, die selbst zwar nicht beschuldigt oder verdächtig sind, aber in (nicht näher definierter) Verbindung mit Beschuldigten, Verdächtigen oder entsprechenden Organisationen stehen.

APIS

Arbeitsdatei PIOS Innere Sicherheit

Erweiterung von PIOS um allgemeine Staatsschutzdelikte.

APIS beinhaltet für verschiedene Anlässe Unterdateien, auf die die Fachdienststellen des LKA je nach Art (Verbund- oder Zentraldatei) direkt oder nach Übermittlung zugreifen können.

Beispiele:

- APLF (Landfriedensbruch)
- APW (Waffen/Sprengstoff)
- APR (Rauschgift)
- APOK (Organisierte Kriminalität)
- APLV (Landesverrat)
- APOE (Osteuropäische Straftäter)
- APGENO (Völkermord)
- APAG (Personenschutz vor terroristischen Anschlägen)

FDR

Falldatei Rauschgift

Verbunddatei; Bestandteil von INPOL. Eingabe und Abruf von Daten durch BKA und LKA. Dient zur Aufklärung von BTM-Straftaten durch Speicherung und Vergleich des modus operandi. Gespeichert werden Daten des Täters einschließlich Personenbeschreibung sowie

die näheren Umstände der Tat (Tatzeit, Tatmittel, Begehungsweise, Rauschgiftmenge usw.).

(Sonstige) Falldateien Außer für Rauschgift gibt es Falldateien auch für die Bereiche Falschgeld, Geiselnahme, Waffen, Scheck, Tötungs- und Sexualdelikte, illegale Schleusertätigkeiten, Sprengstoff und Wirtschaft.

KAN Kriminalaktennachweis
Bundesweiter Fundstellennachweis (Verbunddatei) über kriminalpolizeiliche Personenakten zu schweren und überregional bedeutsamen Delikten.

Überregional bedeutsam:

- gewohnheits-, gewerbs- oder bandenmäßige Begehungsweise
- Triebtäterschaft
- planmäßige überörtliche Begehung
- Verfolgung extremistischer Ziele
- Begehung unter Mitführung von Schusswaffen
- internationale Betätigung
- erneute Straffälligkeit außerhalb des Wohn- oder Aufenthaltsortes

KAN ist Bestandteil von INPOL. Eine Abfrage kann in Berlin über das ISVB erfolgen, und zwar durch Polizeivollzugsbeamte mit ISVB-Berechtigung, d.h. alle in der strafprozessualen Sachbearbeitung tätigen Mitarbeiter. Die Speicherung von Daten in KAN erfolgt zentral durch das LKA.

KAN ist eine sehr umfangreiche Datensammlung (ca. 1.500.000 Personen). Sie enthält auch personengebundene Hinweise („gewalttätig“ etc.), die eine Einschätzung der gespeicherten Person ermöglichen. Datenschutzrechtlich problematisch, weil bei einer Abfrage häufig nur die in KAN gespeicherten Informationen, nicht aber die eigentliche Akte herangezogen wird (Gefahr der Verfälschung von Informationen durch Verkürzung).

Von anderen Stellen geführte Dateien:

EWV	<p>Verfahren „Einwohnerwesen“ des Landeseinwohneramtes Die Berliner Polizei kann über ihre ISVB-Terminals auch online über das Verfahren Einwohnerwesen (EWV) auf Daten des Landeseinwohneramtes zugreifen (reines Abrufsystem). Freigegeben für die Auskunft sind nicht die vollständigen Datensätze, sondern lediglich ausgewählte, notwendige Daten, die für eine Identifizierung oder zur Ladung notwendig sind (Namen, Geburtsdaten, Staatsangehörigkeit, gegenwärtige und frühere Meldeanschriften sowie Personalausweisdaten).</p>
KVA-System	<p>örtliches Fahrzeugregister beim Kraftfahrzeugverkehrsamt (KVA) im Landeseinwohneramt In Berlin Abfrage durch ISVB-Berechtigte aufgrund von § 36 Abs. 2 StVG z.B. bzgl. Daten über konkrete Fahrzeuge oder Halter zur Kontrolle von Fahrzeugen und Papieren, zur Verfolgung von Straftaten oder Ordnungswidrigkeiten bzw. zur Gefahrenabwehr.</p>
ZEVIS	<p>Zentrales Verkehrsinformationssystem beim Kraftfahrtbundesamt ZEVIS enthält das <i>Verkehrszentralregister</i> (Verurteilungen wegen Verkehrsstraftaten, Entzug der Fahrerlaubnis, Fahrverbote, Versagungen und Verzichte auf Fahr- und Fahrlehrerlaubnis, Geldbußen für Verkehrsordnungswidrigkeiten). ZEVIS enthält auch das <i>zentrale Fahrzeugregister</i> (Halter- und Fahrzeugdaten). Polizei hat Online-Zugriff u.a. auf die Halterdaten zum Zwecke der Strafverfolgung und der Gefahrenabwehr (vgl. § 35 I Nr. 1-4 i.V.m. § 36 II Nr. 1 StVG). Zugriff über Fahrzeugkennzeichen oder über Personalien. Verkehrsrechtlicher Zusammenhang des Abrufs nicht erforderlich. Der verkehrsrechtliche Zweck der Dateien tritt damit in den Hintergrund; das ist datenschutzrechtlich problematisch. Gewisser Ausgleich durch Protokollierung der Online-Anfragen; diese zeichnet aber nur die abfragende Stelle, nicht den Abfragegrund auf.</p>
AZR	<p>Ausländer-Zentralregister beim Bundesverwaltungsamt Enthält personenbezogene Daten über die in der Bundesrepublik Deutschland registrierten Ausländer. In Berlin Zugriff durch Polizei über die ISVB-Endgeräte; Abfrage z.B. von Meldestatus und rechtlicher Stellung, Asylverfahren, Abschiebung, Duldung sowie von Ausschreibungen zur Zurückweisung, Auslieferung, Aufenthaltsermittlung oder Festnahme (vgl. z.B. § 16 AZRG).</p>

§ 49 Errichtungsanordnung

- (1) Für jede automatisierte Datei über personenbezogene Daten und solche nicht automatisierte Dateien über personenbezogene Daten, aus denen personenbezogene Daten an andere Stellen übermittelt werden, ist jeweils eine Errichtungsanordnung zu erlassen. Ihr Inhalt bestimmt sich nach § 19 Abs. 2 Nr. 1 bis 4 sowie Nr. 6 und 7 des Berliner Datenschutzgesetzes. Sie hat außerdem Prüffristen nach § 48 Abs. 2 Satz 1 Nr. 2 zu enthalten. Die Errichtungsanordnung tritt an die Stelle der Dateibeschreibung nach § 19 Abs. 2 des Berliner Datenschutzgesetzes.
- (2) Die Senatsverwaltung für Inneres regelt das Nähere durch Verwaltungsvorschrift. Sie übersendet die Errichtungsanordnung dem Berliner Datenschutzbeauftragten.
- (3) Die Speicherung personenbezogener Daten in Dateien ist auf das erforderliche Maß zu beschränken. Die Notwendigkeit der Weiterführung oder Änderung der Dateien ist in angemessenen Abständen zu überprüfen.

§ 4 III Nr. 5 BlnDSG:

„eine Datei (ist) eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (**automatisierte Datei**), oder eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (**nicht automatisierte Datei**) ...“

§ 19 II BlnDSG:

„Für automatisierte Verarbeitungen hat die datenverarbeitende Stelle schriftlich festzulegen:

1. Name und Anschrift der datenverarbeitenden Stelle,
2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung,
3. Beschreibung der betroffenen Personengruppe und der diesbezüglichen Daten oder Datenkategorien,
4. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden,
- ...
6. zugriffsberechtigte Personen oder Personengruppen,
7. Fristen für die Sperrung und Löschung der Daten ...“

§ 49 ASOG ist lex specialis zu § 19 II BlnDSG (vgl. § 49 I 4 ASOG).

Zwecke des § 49 ASOG:

- Begrenzung der Anzahl der Dateien
- Erschwerung der Erweiterung der Merkmalsfelder einer bereits bestehenden Datei
- Selbstkontrolle der speichernden Stelle
- Erleichterung der Tätigkeit der Aufsichtsbehörden einschließlich des Datenschutzbeauftragten.

Verwaltungsvorschrift gem. § 49 II ASOG: „**Dateienrichtlinie**“ vom 4.12.1992.

- Zuständig für die Errichtungsanordnung ist nach der Richtlinie für alle kriminalpolizeilichen Bereiche der Landeskriminalpolizeidirektor, in den übrigen Fällen der Landeschutzpolizeidirektor.
- Errichtungsanordnungen sind der Senatsverwaltung für Inneres zur Zustimmung vorzulegen. Nach Prüfung und Zustimmung übersendet der Polizeipräsident die Errichtungsanordnungen auf dem Dienstweg dem Berliner Datenschutzbeauftragten (§ 49 II 2 ASOG).
- Der Betrieb einer Datei darf erst aufgenommen werden, wenn die Zustimmung der Senatsverwaltung für Inneres vorliegt. Bei Gefahr im Verzug darf der Betrieb ohne Zustimmung aufgenommen werden. Diese ist unverzüglich einzuholen.

Die Dateienrichtlinie schreibt für die Errichtungsanordnung u.a. folgenden Inhalt vor:

- konkrete Organisationseinheit, bei der die Datei geführt wird (dateiführende Stelle)
- Dateibezeichnung
- Zweckbestimmung der Datei
- Art und Umfang der zu speichernden Daten (z.B. Namen, Geburtsdatum, Staatsangehörigkeit, Adresse usw.)
- Rechtsgrundlagen für die Datenverarbeitung (evtl. mehrere, je nach Art der Daten)
- betroffener Personenkreis
- Art und Empfänger regelmäßig zu übermittelnder Daten
- Art und Herkunft regelmäßig empfangener Daten
- Art der Verarbeitung
- Fristen für die Überprüfung der Daten nach der PrüffristenVO gem. § 48 IV ASOG
- Zugriffsberechtigungen
- technische und organisatorische Maßnahmen zur allgemeinen Datensicherung (Zugriffssicherung) gem. § 5 BlnDSG.
- Art der Datenverarbeitung bei automatisierten Dateien
- Art der Übermittlung (automatisierter Rechnerverbund bzw. automatisiertes Abrufverfahren oder Austausch von Datenträgern, Listen u.ä.)
- Verfahren zur Einhaltung der Prüffristen

Der nach der Dateienrichtlinie erforderliche Inhalt der Errichtungsanordnung geht damit über den Mindestinhalt gem. § 49 I 2 ASOG i.V.m. § 19 II Nrn. 1-4, 6, 7 BlnDSG hinaus.

Da die Dateienrichtlinie allein für die Polizei gilt, müssen entsprechende Dateien der Ordnungsbehörden lediglich die Mindestanforderungen gem. § 19 II BlnDSG erfüllen.

§ 49 III: lex specialis zu § 11 ASOG; Konkretisierung des Verhältnismäßigkeitsgrundsatzes. Zu prüfen ist zunächst, ob die Datenverarbeitung in Dateien eine wesentliche Effizienzsteigerung erwarten lässt. Außerdem konkretisiert § 49 III 2 das zeitliche Übermaßverbot (§ 11 III ASOG).

Kapitel 9: Allgemeine Regeln über die Datenspeicherung, -veränderung und -nutzung (§ 42 ASOG)

§ 42 Allgemeine Regeln über die Datenspeicherung, -veränderung und -nutzung

- (1) Die Ordnungsbehörden und die Polizei können rechtmäßig erhobene personenbezogene Daten in Akten oder Dateien speichern, verändern und nutzen, soweit das zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist. Dies gilt auch für personenbezogene Daten, die die Ordnungsbehörden und die Polizei unaufgefordert durch Dritte erlangt haben.
- (2) Die Ordnungsbehörden und die Polizei dürfen personenbezogene Daten nur zu dem Zweck speichern, verändern und nutzen, zu dem sie die Daten erlangt haben. Die Nutzung sowie die weitere Speicherung und Veränderung zu einem anderen ordnungsbehördlichen oder polizeilichen Zweck ist zulässig, soweit die Ordnungsbehörden und die Polizei die Daten auch zu diesem Zweck hätten erheben und nutzen dürfen. Eine Verarbeitung zu anderen Zwecken liegt nicht vor, wenn sie die Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient. Der Zugriff auf personenbezogene Daten ist insoweit nur zulässig, als er für die Ausübung dieser Befugnisse unverzichtbar ist.
- (3) Die Polizei kann, soweit Bestimmungen der Strafprozeßordnung oder andere gesetzliche Regelungen nicht entgegenstehen, personenbezogene Daten, die sie im Rahmen von strafrechtlichen Ermittlungen gewonnen hat, speichern, verändern und nutzen, soweit das zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten (§ 1 Abs. 3) erforderlich ist.
- (4) Die Ordnungsbehörden und die Polizei können personenbezogene Daten über die zulässige Speicherdauer hinaus zu Aus- oder Fortbildung oder zu statistischen Zwecken in anonymisierter Form nutzen.
- (5) Werden personenbezogene Daten von Kindern, die ohne Kenntnis der Sorgeberechtigten erhoben worden sind, gespeichert, sind die Sorgeberechtigten zu unterrichten, soweit die Aufgabenerfüllung dadurch nicht mehr gefährdet wird. Von der Unterrichtung kann abgesehen werden, solange zu besorgen ist, daß die Unterrichtung zu erheblichen Nachteilen für das Kind führt.

A. Rechtsfolge

Speicherung, Veränderung und Nutzung personenbezogener Daten in Akten oder Dateien

- *Personenbezogene Daten*: vgl. § 4 I BlnDSG: Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person. Auch Daten über Verstorbene, es sei denn, dass schutzwürdige Belange des Betroffenen nicht mehr beeinträchtigt werden können.
- *Speicherung*: vgl. § 4 II Nr. 2 BlnDSG: das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger.
- *Veränderung*: vgl. § 4 II Nr. 3 BlnDSG: das inhaltliche Umgestalten gespeicherter Daten, ungeachtet der dabei angewendeten Verfahren.

- *Nutzung*: vgl. § 4 II Nr. 7 BlnDSG: jede sonstige Verwendung personenbezogener Daten, d.h. jede Verwendung, die kein Erheben, Speichern, Verändern, Übermitteln, Sperren oder Löschen darstellt.
- *Akte*: vgl. § 4 III Nr. 6 BlnDSG: jede sonstigen amtlichen oder dienstlichen Zwecken dienende Unterlage, soweit sie nicht Datei ist; dazu zählen auch Bild- und Tonträger, nicht jedoch Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.
- *Datei*: vgl. § 4 III Nr. 5 BlnDSG: Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei), oder eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht automatisierte Datei).

B. Tatbestand

Die Daten müssen zuvor rechtmäßig erhoben oder unaufgefordert von Dritten erlangt worden sein; der Zweck des Speicherns, Veränderns oder Nutzens muss die Erfüllung der polizeilichen Aufgaben, die zeitlich befristete Dokumentation oder die Vorgangsverwaltung sein; das Speichern, Verändern oder Nutzen muss zu diesem Zweck erforderlich sein; die Zweckbindung der Daten muss dabei beachtet werden.

- Daten müssen zuvor rechtmäßig erhoben oder unaufgefordert von Dritten erlangt worden sein.

Erhoben: vgl. § 4 II Nr. 1 BlnDSG: das Beschaffen von Daten über den Betroffenen.

Rechtmäßig erhoben: gemäß einer entsprechenden Befugnisnorm, z.B. § 23 ASOG oder § 18 ASOG.

Dritter: vgl. § 4 III Nr. 3 BlnDSG: jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene und Stellen in der EU, die Daten im Auftrag verarbeiten.

Unaufgefordert erlangt: nicht erhoben, also kein aktives Beschaffen. Beispiele: Unaufgeforderte Übermittlung von Daten durch den Verfassungsschutz an die Polizei gem. § 21 BlnVerfSchG; Anzeige durch einen Bürger auf eigene Initiative.

- Zweck der Speicherung, Veränderung oder Nutzung: Erfüllung der polizeilichen Aufgaben, zeitlich befristete Dokumentation oder Vorgangsverwaltung.

Erfüllung der polizeilichen Aufgaben: gemeint sind die Aufgaben gem. § 1 ASOG. Ergibt sich eine polizeiliche Aufgabe aus einem anderen Gesetz (§ 1 II ASOG), so stehen der Polizei grundsätzlich die dort geregelten Befugnisse zu (vgl. § 17 II ASOG). Das gilt auch für das Speichern, Verändern und Nutzen von Daten. In vielen Spezialgesetzen finden sich inzwischen entsprechende Befugnisse (z.B. § 12a VersG). Nur wenn ein Spezialgesetz ausnahmsweise zwar die polizeiliche Aufgabe eröffnet, aber keine Befugnisse zum Speichern, Verändern und Nutzen von Daten enthält, ist insoweit ein Rückgriff auf § 42 ASOG möglich.

zeitlich befristete Dokumentation: Beispiele: Speicherung von telefonischen Notrufen, Videoaufzeichnung des taktischen Verhaltens der Polizei bei Geiselnahmen. Im ASOG gibt es keine Befugnis zur Datenerhebung zum alleinigen Zweck der Dokumentation. Daher meint diese Tatbestandsalternative nur die Dokumentation von Daten, die im Rahmen der sonstigen Aufgabenerfüllung erhoben wurden. In dieser Dokumentation liegt auch keine Zweckänderung i.S.v. § 42 II ASOG: Die Dokumentation einer polizeilichen

Maßnahme ist Bestandteil der Aufgabenerfüllung, im Rahmen derer diese Maßnahme ergriffen wird. Die Erwähnung der Dokumentation in § 42 I ASOG dient daher v.a. der Klarstellung und hat allenfalls Folgen für die Speicherfrist. Diese ist zwar nicht unbeschränkt (die Dokumentation muss „zeitlich befristet“ sein), kann aber über die endgültige Beseitigung einer Gefahr hinausreichen. Das ist z.B. dann der Fall, wenn ein Gerichtsverfahren zu erwarten ist, für das die dokumentierten Daten als Beweis benötigt werden. Maximal wird die Speicherung für Dokumentationszwecke jedoch wohl nicht über 1 bis 6 Monate hinausgehen dürfen; in jedem Fall sind die Grenzen des § 48 ASOG zu beachten.

Vorgangsverwaltung: gemeint sind v.a. Aktenerschließungssysteme bzw. Aktennachweise. Ihre Führung ist unverzichtbar für eine geordnete Verwaltung und daher Bestandteil der jeweiligen Aufgabe, im Rahmen derer Daten in Akten erfasst werden.

- Erforderlichkeit der Maßnahme zu diesem Zweck.

Das heißt: Der Zweck (Aufgabenerfüllung, Dokumentation oder Vorgangsverwaltung) kann durch keine milderen Mittel als Speicherung, Veränderung oder Nutzung der Daten erfüllt werden. Auch der Umfang der Daten muss erforderlich sein in diesem Sinne, d.h. der Zweck darf nicht durch die Speicherung, Veränderung oder Nutzung von weniger Daten ebenso gut erfüllt werden können.

- Zweckbindung der Daten (Abs. 2, 3)

- Grundsatz der Zweckbindung: § 42 II 1. Speicherung, Veränderung und Nutzung von Daten ist nur zu dem Zweck zulässig, zu dem die Daten erlangt wurden.

Zweck: muss wegen der Anforderungen des Volkszählungsurteils eng ausgelegt werden. Der Betroffene muss erkennen können, zu welchem Zweck seine Daten später verwendet werden. Unterschiedliche Zwecke liegen daher i.d.R. dann vor, wenn die Datenerhebung nach verschiedenen Spezialgesetzen erfolgt (z.B. VersG, WaffG). Im Anwendungsbereich des ASOG ist Zweck nicht die Gefahrenabwehr schlechthin, sondern der mit der konkreten Befugnisnorm für die Datenerhebung verfolgte Zweck. So sind Gefahrenvorsorge (§ 19 ASOG) und vorbeugende Straftatenbekämpfung (§ 18 I 3 ASOG) verschiedene Zwecke.

erlangt: z.B. erhoben, übermittelt oder unaufgefordert erlangt.

- allgemeine Zweckänderung: § 42 II 2. Die Speicherung, Veränderung und Nutzung zu einem anderen als dem Erhebungszweck ist zulässig, wenn die Daten auch zu diesem Zweck hätten erhoben oder genutzt werden dürfen. Es muss also geprüft werden, ob auch die Voraussetzungen der zu dem neuen Zweck passenden anderen Befugnisnorm für die Datenerhebung erfüllt waren.
- keine Zweckänderung liegt vor bei der Wahrnehmung von Aufsichts- und Kontrollbefugnissen sowie bei der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen (§ 42 II 3). Dabei dürfen personenbezogene Daten aber nur im unverzichtbaren Umfang verwendet werden.
- spezielle Zweckänderung: § 42 III. Speicherung, Veränderung und Nutzung von im Rahmen strafrechtlicher Ermittlungen gewonnenen Daten zu Zwecken der Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten, wenn dies erforderlich ist und wenn andere Bestimmungen nicht entgegenstehen.

strafrechtliche Ermittlungen: nur Ermittlungen zu Straftaten, nicht zu Ordnungswidrigkeiten.

gewonnene Daten: selbst erhobene, übermittelte oder unaufgefordert erlangte Daten.

vorbeugende Bekämpfung von Straftaten: vgl. § 1 III ASOG.

erforderlich: es gibt kein milderes Mittel, um den jeweiligen Zweck der Gefahrenabwehr zu erreichen.

andere Bestimmungen stehen nicht entgegen: z.B. § 100b VI StPO: Pflicht zur Vernichtung von Telekommunikationsdaten, sobald diese nicht mehr für das Strafverfahren benötigt werden. Eine weitere Speicherung dieser Daten für die Gefahrenabwehr ist damit ausgeschlossen.

§ 42 III stellt eine „Einlassklausel“ für die gefahrenabwehrende Verwendung von Daten dar, die nach der StPO gewonnen wurden. Dem korrespondiert die „Öffnungsklausel“ bzw. „Entlassklausel“ des § 481 I StPO: Verwendung personenbezogener Daten aus Strafverfahren durch die Polizeibehörden „nach Maßgabe der Polizeigesetze“ und Übermittlung an die Polizeibehörden zu den in den den Polizeigesetzen genannten Zwecken (also insbesondere Gefahrenabwehr).

- keine Zweckänderung (und damit erlaubt) ist die Nutzung von Daten über die zulässige Speicherdauer hinaus zur Aus- oder Fortbildung oder zu statistischen Zwecken in anonymisierter Form (§ 42 IV).

Die Vorschrift muss richtig wohl so ausgelegt werden, dass die Nutzung für diese Zwecke auch schon während der zulässigen Speicherdauer erlaubt ist, wenn die Daten anonymisiert sind.

zulässige Speicherdauer: vgl. §§ 43 I 2, 48 IV ASOG.

Anonymisierung: vgl. § 4 III Nr. 7 BlnDSG: 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 bestimmaren natürlichen Person zugeordnet werden können.

C. Adressat

Bei den rechtmäßig erhobenen Daten ergibt sich der Adressat der Speicherung, Veränderung oder Nutzung aus der jeweiligen Adressatenregelung der Datenerhebungsbefugnis (also z.B. aus § 23 ASOG oder § 18 ASOG).

Bei den unaufgefordert erlangten Daten ist Adressat der jeweils Betroffene.

D. Zuständigkeit

Abs. 3 (Zweckänderung strafprozessualer Daten): nur die Polizei.

Im Übrigen Ordnungsbehörden und Polizei.

E. Verfahrensvorschriften

- § 42 V: Unterrichtung der Sorgeberechtigten bei der Speicherung von Daten über Kinder, wenn die Daten ohne Kenntnis der Sorgeberechtigten erhoben worden sind

Kind: Altersgrenze nicht ausdrücklich geregelt; Übertragung entsprechender Altersgrenzen aus anderen Gesetzen wohl nicht möglich. Daher Altersgrenze bei 18 Jahren.

Ausnahmen von der Unterrichtungspflicht:

- Gefährdung der Aufgabenerfüllung. Beispiel: Kind wird von Eltern als Drogenkurier eingesetzt.
- erhebliche Nachteile für das Kind zu besorgen. Beispiel: Kind informiert die Polizei über seine Eltern.

F. Bezüge zu anderen Vorschriften

Spezialvorschriften (mit Vorrang gegenüber § 42 ASOG):

- § 43 I ASOG: Speicherung von Daten über Kontakt- und Begleitpersonen sowie Zeugen, Hinweisgeber und sonstige Auskunftspersonen zum Zwecke der vorbeugenden Straftatenbekämpfung in Dateien
- § 23 II ASOG: Aufbewahrung erkennungsdienstlicher Unterlagen zur vorbeugenden Straftatenbekämpfung oder nach anderen Rechtsvorschriften (bezüglich Letzterem ist wiederum § 42 I ASOG anwendbar).
- §§ 483-486 StPO (Datenverarbeitung für Zwecke des Strafverfahrens und des künftigen Strafverfahrens). Beachte insb. § 484 IV StPO mit der Verweisung auf die Länderpolizeigesetze (in Berlin das ASOG) bezüglich der (präventiven) Verwendung der Daten, die für künftige Strafverfahren gespeichert werden.
- §§ 12a II, 19a VersG: Bild- und Tonaufnahmen bei Versammlungen
- § 80 AuslG i.V.m. der entsprechenden Rechtsverordnung (Speicherung und Löschung personenbezogener Daten im Anwendungsbereich des AuslG)
- §§ 31, 33 StVG (Fahrzeugregister); §§ 3-5 Fahrzeugregister-Verordnung (Speicherung von Fahrzeug- und Halterdaten)
- § 2 MRRG i.V.m. § 2 BlnMeldeG (Speicherung von Einwohnerdaten)
- § 2a PersAuswG (Personalausweisregister)
- § 46 BImSchG i.V.m. § 2 des Ausführungsgesetzes zum BImSchG und der Verordnung über die Verarbeitung personenbezogener Daten im Zusammenhang mit nicht genehmigungsbedürftigen Anlagen vom 18.10.1994 (GVBl. S. 464) (Emissionskataster)
- §§ 12a und 12b BlnStadtReinG (mit Anlage zu § 12b); §§ 113a bis 113c BlnWasserG (mit Anlage zu § 113a); § 6a BlnStrReinG (mit Anlage zu § 6a)

G. Probleme

Durch die weitgehenden Möglichkeiten der Zweckänderung (§ 42 II 2, III) wird der Grundsatz der Zweckbindung (§ 42 II 1) stark relativiert. Das ist problematisch, weil die Betroffenen über eine solche Zweckänderung nicht benachrichtigt werden müssen und daher möglicherweise darüber nicht informiert sind. Sie wissen dann nicht mehr, zu welchen Zwecken ihre Daten verwendet werden. Das widerspricht den Anforderungen des Volkszählungsurteils.

Die Problematik wird etwas abgemildert durch korrespondierende Öffnungs- oder Entlassklauseln in den Befugnisnormen zur ursprünglichen Datenerhebung, z.B. § 481 StPO. Dadurch wird die mögliche Zweckänderung für Betroffene leichter erkennbar.

Kapitel 10: Besondere Regeln für die Speicherung, Veränderung und Nutzung
von Daten in Dateien (§ 43 ASOG)

**§ 43 Besondere Regeln für die Speicherung, Veränderung und
Nutzung von Daten in Dateien**

- (1) Die Polizei kann zur vorbeugenden Bekämpfung von Straftaten personenbezogene Daten über die in § 25 Abs. 2 Satz 1 Nr. 2 genannten Personen sowie über Zeugen, Hinweisgeber und sonstige Auskunftspersonen in Dateien nur speichern, verändern und nutzen, soweit das zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist. Die Speicherdauer darf drei Jahre nicht überschreiten. Nach jeweils einem Jahr, gerechnet vom Zeitpunkt der letzten Speicherung, ist zu prüfen, ob die Voraussetzungen nach Satz 1 noch vorliegen.
- (2) Werden wertende Angaben über eine Person in Dateien gespeichert, muss feststellbar sein, bei welcher Stelle die den Angaben zugrunde liegenden Informationen vorhanden sind.

§ 43 I 1 ist lex specialis gegenüber § 42 I; § 43 I 2, 3 ist lex specialis gegenüber § 48. § 43 II ist sowohl für Speicherungen nach § 42 als auch für solche nach § 43 I anwendbar.

Zu § 43 I:

A. Rechtsfolge

Speicherung, Veränderung und Nutzung von personenbezogenen Daten über die in § 25 II 1 Nr. 2 genannten Personen sowie über Zeugen, Hinweisgeber und sonstige Auskunftspersonen in Dateien zur vorbeugenden Bekämpfung von Straftaten.

- Speicherung, Veränderung und Nutzung personenbezogener Daten: wie in § 42 I.
- in Dateien: Begriff wie in § 42 I, d.h. Dateibegriff des § 4 III Nr. 5 BlnDSG. Hier unterscheidet sich § 43 von § 42. § 42 erfasst neben den Dateien auch Akten; § 43 beschränkt sich dagegen auf Dateien. Die Verarbeitung der in § 43 I genannten Daten in Akten richtet sich daher nicht nach § 43, sondern nach § 42 ASOG. Die erhöhten Anforderungen des § 43 gelten nur für die „gefährlichere“ Verarbeitung der entsprechenden Daten in Dateien.
- die in § 25 II 1 Nr. 2 genannten Personen:
§ 25 II 1 lautet:

»...

1. Personen, wenn Tatsachen die Annahme rechtfertigen, daß sie Straftaten von erheblicher Bedeutung begehen werden,

2. andere Personen, wenn Tatsachen die Annahme rechtfertigen, daß sie mit einer der in Nummer 1 genannten Personen in einer Weise in Verbindung stehen, die erwarten läßt, daß die Maßnahme zur vorbeugenden Bekämpfung der Straftaten beitragen wird

...“

Gemeint sind Kontakt- oder Begleitpersonen von potentiellen zukünftigen Straftätern; dabei muss es sich um Straftaten von erheblicher Bedeutung handeln (vgl. § 17 III A

SOG). Die Kontakt- und Begleitpersonen sind hier Nichtstörer; wären sie (gleichzeitig) Störer, also selbst potentielle Straftäter, so würde die Speicherung ihrer Daten unter § 42 fallen. Die Verbindung zu den potentiellen Straftätern muss so beschaffen sein, dass eine Datenerhebung bei den Kontakt- oder Begleitpersonen Aufschlüsse hinsichtlich künftiger Straftaten erwarten lässt. Das ist der Fall z.B. bei Verbindungen, die über einen längeren Zeitraum bestehen oder unter konspirativen Umständen hergestellt bzw. gepflegt werden. Zufallsbekanntschaften werden dagegen nicht erfasst.

- Zeugen, Hinweisgeber und sonstige Auskunftspersonen:

Zeugen: gemeint sind Zeugen im strafverfahrensrechtlichen Sinne.

Hinweisgeber und sonstige Auskunftspersonen: beliebige Personen, die sachdienliche Hinweise oder Auskünfte geben.

- zur vorbeugenden Bekämpfung von Straftaten: Begriff definiert in § 1 III ASOG. Dieses Merkmal ist hier Teil der Rechtsfolge, d.h. der rechtlichen Umschreibung der Maßnahme. Die zweite Erwähnung in § 43 I 1 (... soweit zur vorbeugenden Bekämpfung ... erforderlich) gehört dagegen zum Tatbestand.

Maßnahmen nach § 43 I 1 sind also nur solche, deren Zweck die vorbeugende Straftatenbekämpfung ist. Werden die entsprechenden Daten dagegen zu anderen Zwecken (z.B. allgemeine Gefahrenabwehr) erhoben, dann ist statt der Spezialregelung des § 43 I 1 die allgemeinere Regelung des § 42 I anzuwenden.

B. Tatbestand

Erforderlichkeit zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung.

- Straftaten von erheblicher Bedeutung: definiert in § 17 III. Problematisch ist dabei, ob auch die in § 17 IV genannten Ordnungswidrigkeiten zur Erfüllung des Tatbestands ausreichen. Das ist wohl abzulehnen. § 1 III ASOG eröffnet der Polizei lediglich die Aufgabe der vorbeugenden Bekämpfung von Straftaten, nicht von Ordnungswidrigkeiten; daher fehlt es schon an der Aufgabeneröffnung. Außerdem wäre die Verarbeitung personenbezogener Daten von Unbeteiligten als reine Vorsorge für die Verfolgung künftiger Ordnungswidrigkeiten (zweite Komponente der vorbeugenden Straftatenbekämpfung gem. § 1 III ASOG) unverhältnismäßig, und die Verhütung künftiger Ordnungswidrigkeiten (erste Komponente der vorbeugenden Straftatenbekämpfung gem. § 1 III ASOG) ist eine Form der Gefahrenabwehr und fällt daher unter § 42 I; in diesem Fall ist für den fraglichen Personenkreis die Adressatenregelung des § 16 III ASOG anzuwenden. Ob § 16 III auch Unbeteiligte in den Adressatenkreis einbezieht, ist dabei umstritten; die Einbeziehung der Kontakt- und Begleitpersonen, Zeugen, Hinweisgeber und sonstigen Auskunftspersonen kommt nur dann in Betracht, wenn die Formulierung „grundsätzlich nur“ in § 16 III so ausgelegt wird, dass ausnahmsweise auch Unbeteiligte Adressat sein können.
- Erforderlichkeit: bezieht sich auf Art der Datenverarbeitung (Speichern, Verändern, Nutzen) sowie auf den Umfang der verarbeiteten Daten. So genügt es bei Hinweisgebern und Auskunftspersonen i.d.R., die Personalien zu speichern, während bei Kontakt- und Begleitpersonen auch die Speicherung von weiteren, z.B. tat- oder gefahrenbezogenen Informationen erforderlich sein kann.
- Wohl zu ergänzen ist als Tatbestandsmerkmal die Art der Erlangung der Daten. § 43 I 1 macht dazu keine Aussage; aus rechtsstaatlichen Gründen muss aber wohl vorausgesetzt werden, dass die Daten – wie bei § 42 I 1 ASOG – rechtmäßig erhoben oder unaufgefor

dert von Dritten erlangt sind. Andernfalls könnten rechtswidrig erhobene Daten durch eine zulässige Speicherung „legalisiert“ werden.

C. Adressat

Der Adressat ergibt sich direkt aus § 43 I. Obwohl es sich um Nichtstörer handelt, ist § 16 ASOG daher nicht anzuwenden (auch nicht § 16 III).

D. Zuständigkeit

Nur die Polizei.

E. Verfahrensvorschriften

- Speicherdauer (§ 43 I 2): Die nach § 43 I 1 gespeicherten Daten dürfen maximal 3 Jahre lang gespeichert werden. Daneben muss auch die Lösungsregelung des § 48 II 1 Nr. 2 beachtet werden: wenn bei der nach bestimmten Fristen vorzunehmenden Überprüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass die Kenntnis der Daten für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist, müssen die Daten gelöscht werden. Die Regelung des § 43 I 2 ist also eine Maximalspeicherdauer, die nach § 48 II 1 Nr. 2 ggf. unterschritten werden muss.
- Jährliche Überprüfung (§ 43 I 3): Nach jeweils einem Jahr ist zu überprüfen, ob die Tatbestandsvoraussetzungen des § 43 I 1, die zur Speicherung ermächtigen, noch erfüllt sind. Ist dies nicht mehr der Fall, muss die Speicherung beendet werden, d.h. die Daten sind zu löschen.
- Zu beachten ist § 43 II (s.u.).

F. Bezüge zu anderen Vorschriften

Verhältnis zu § 42: § 43 I ist lex specialis bezüglich des Speicherns, Veränderns und Nutzens personenbezogener Daten des hier genannten Personenkreises (Kontakt- und Begleitpersonen sowie Zeugen, Hinweisgeber und sonstige Auskunftspersonen) in Dateien. Daher ist § 42 anstelle von § 43 I anwendbar, wenn es um Daten anderer Personen geht (z.B. des potentiellen Straftäters selbst) oder um die Verarbeitung dieser Daten in Akten.

§ 43 betrifft nicht die Datenerhebung. Daten zu dem genannten Personenkreis können ggf. nach § 25 II 1 Nr. 2 oder nach § 18 I 3 Alt. 1 i.V.m. § 16 III ASOG erhoben werden. Die Anwendung von § 16 III auf Unbeteiligte ist dabei umstritten; sie kommt nur dann in Betracht, wenn die Formulierung „grundsätzlich nur“ in § 16 III so ausgelegt wird, dass ausnahmsweise auch Unbeteiligte Adressat sein können.

G. Probleme

Verfassungsrechtlich problematisch ist die Einbeziehung von Nichtstörern, v.a. den „sonstigen Auskunftspersonen“ in den Adressatenkreis. Im Zusammenhang mit § 19 ASOG (Vorbereitung für die Hilfeleistung in Gefahrenfällen) kann das mit der Schwere der Gefahren zu rechtfertigen sein; bei der bloßen Vorsorge für die künftige Straftatenverfolgung (erst recht natürlich bei Erstreckung der Maßnahmen auf die Ordnungswidrigkeiten nach § 17 IV) ist die Verhältnismäßigkeit solcher Maßnahmen zweifelhaft.

Zu § 43 II:

Es handelt sich um eine Verfahrensvorschrift für alle Speicherungen, also sowohl für solche nach § 43 I 1 als auch für solche nach § 42 I 1.

Die Vorschrift gilt für Ordnungsbehörden und Polizei.

Zweck: Der Grund für die gespeicherten Wertungen soll nachvollziehbar sein; Ausgleich für die Verkürzung von Informationen, die dadurch zustande kommt, dass Daten aus Akten nur teilweise und zusammenfassend in Dateien übernommen werden.

Voraussetzungen für die Anwendung der Vorschrift:

- Speicherung personenbezogener Angaben in Dateien (Dateibegriff des § 4 III Nr. 5 BlnDSG)
- Wertende Angaben: Urteile über Personen, Eigenschaften und Handlungen. Beispiele: „gebrechlich“, „geistesgestört“, „aus einem Heim abgängig“, „suizidgefährdet“, „gefährlicher Gewaltverbrecher“, „Intensivtäter“, „BTM-Konsument“, „Ausbrecher“, „Schusswaffentträger“. Auch die Ausschreibung zur Fahndung ist eine wertende Angabe in diesem Sinne.

Folge:

Angabe der Stelle, bei der die der Wertung zugrunde liegenden Informationen vorhanden sind. Es genügt eine Angabe mit Hilfe des Behördenschlüssels. Ebenfalls genügt ein Hinweis auf die zugehörige Akte, wenn sich aus dieser die Stelle ermitteln lässt.

Stelle kann dabei jede öffentliche (auch ausländische, zwischen- oder überstaatliche) oder nichtöffentliche Einrichtung (z.B. ein privater Träger einer Jugendeinrichtung) sein.

Kapitel 11: Datenübermittlung innerhalb des öffentlichen Bereichs (§ 44 ASOG)

Normadressart der Übermittlungsvorschriften ist grundsätzlich die übermittelnde Stelle. Aus der Sicht der empfangenden Stelle ist die Übermittlung personenbezogener Daten, wenn sie die Daten angefordert hat, eine Datenerhebung; deren Zulässigkeit beurteilt sich nach den entsprechenden Datenerhebungsvorschriften, nicht nach § 44. Eine Ausnahme stellt § 44 VI dar: Diese Regelung in der Übermittlungsvorschrift des § 44 richtet sich an den Empfänger der übermittelten Daten.

A. Rechtsfolge

- die Übermittlung personenbezogener Daten zwischen den Ordnungsbehörden sowie zwischen den Ordnungsbehörden und der Polizei; ebenso die Übermittlung personenbezogener Daten an Gefahrenabwehr- oder Polizeibehörden eines anderen Landes oder des Bundes (§ 44 I)
- die Übermittlung personenbezogener Daten an andere Behörden oder sonstige öffentliche Stellen (§ 44 II)
- die Übermittlung personenbezogener Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen (§ 44 III)

Übermittlung: vgl. § 4 II Nr. 4 BlnDSG: das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die datenverarbeitende Stelle an den Dritten weitergegeben werden oder dass der Dritte zum Abruf bereitgehaltene Daten abrufen.

§ 44 I 3 ASOG regelt dazu ergänzend, dass Datenübermittlung auch die Weitergabe personenbezogener Daten innerhalb einer Behörde zwischen Stellen ist, die unterschiedliche gesetzliche Aufgaben wahrnehmen. Diese Regelung dient nur der Klarstellung. Sie ergibt sich inhaltlich bereits aus § 4 III Nr. 1 BlnDSG, wonach für den Fall, dass eine Behörde unterschiedliche gesetzliche Aufgaben wahrnimmt, diejenige Organisationseinheit als datenverarbeitende Stelle gilt, der die Aufgabe zugewiesen ist.

Demnach ist klar, dass die Weitergabe von Daten zwischen verschiedenen Ordnungsbehörden (z.B. Gesundheitsamt und Wirtschaftsamt) eine Datenübermittlung darstellt, auch wenn beide Behörden demselben Bezirk angehören (insoweit könnte man nämlich auch vom Bezirksamt als Behörde sprechen).

Innerhalb der Polizei, d.h. des Polizeipräsidenten von Berlin als Behörde, stellt eine Datenweitergabe keine Übermittlung dar, soweit verschiedene Organisationseinheiten der Polizei identische Aufgaben haben. So ist die Gefahrenabwehr und die Verfolgung von Straftaten Aufgabe sowohl der Schutz- als auch der Kriminalpolizei. Nehmen dagegen bestimmte Dienststellen des Polizeipräsidenten in Berlin spezielle Ordnungsaufgaben wahr (diese ergeben sich aus § 2 IV 1 ASOG i.V.m. dem ZustKat Ord), so stellt eine Datenweitergabe zwischen bzw. zu oder von diesen Dienststellen eine Übermittlung dar. Beispiel: Weitergabe von Daten, die der Polizeipräsident im Rahmen der ordnungsbehördlichen Aufsicht über die Angelegenheiten des Waffenrechts (Nr. 23 II ZustKat Ord) gespeichert hat, an die Schutz- oder Kriminalpolizei zur Durchführung einer Razzia zur Bekämpfung des illegalen Waffenhandels.

Die Übermittlung kann auch z.B. mündlich, per Brief oder durch „Lesenlassen“ erfolgen. Auch das Abrufen bereitgehaltener Daten (§ 46 ASOG) ist eine Übermittlung in diesem Sinne.

Die Übermittlung kann sowohl auf Ersuchen der empfangenden Stelle als auch von Amts wegen erfolgen („Spontanübermittlung“).

Ordnungsbehörden: vgl. § 2 II, III ASOG: Senatsverwaltungen, Bezirksämter und Sonderbehörden der Hauptverwaltung, die für Ordnungsaufgaben zuständig sind.

Polizei: vgl. § 5 I ASOG: der Polizeipräsident in Berlin (als Behörde).

Gefahrenabwehr- oder Polizeibehörden eines anderen Landes oder des Bundes: Bei der Auffindung der gesetzlichen Regelungen über die Gefahrenabwehr- und Polizeibehörden eines anderen Bundeslandes ist zu beachten, dass häufig Polizei und Ordnungsbehörden in verschiedenen Gesetzen geregelt sind; darüber hinaus gibt es manchmal verschiedene Gesetze zu den Aufgaben und Befugnissen einerseits und zur Organisation und Zuständigkeit andererseits. Beispiel Brandenburg: Gesetz über Aufgaben und Befugnisse der Polizei im Land Brandenburg (Brandenburgisches Polizeigesetz); Gesetz über die Organisation und Zuständigkeit der Polizei im Land Brandenburg; Gesetz über Aufbau und Befugnisse der Ordnungsbehörden des Landes Brandenburg.

Als Gefahrenabwehr- oder Polizeibehörden des Bundes kommen in Betracht z.B. der Bundesgrenzschutz und das Bundeskriminalamt.

andere **Behörden oder sonstige öffentliche Stellen** (§ 44 II): vgl. § 1 IV VwVfG: alle deutschen Stellen, die Aufgaben der öffentlichen Verwaltung oder sonstige öffentliche Aufgaben wahrnehmen, ausgenommen Ordnungs- und Polizeibehörden des Bundes und der Länder. Der Sitz dieser Stellen kann auch im Ausland liegen (z.B. deutsche Konsulate oder Botschaften). Die Definition ergibt sich aus einer Abgrenzung von § 44 II gegenüber § 44 I und § 44 III.

ausländische öffentliche Stellen (§ 44 III): z.B. Polizeibehörden anderer Staaten, ausländische Streitkräfte, ausländische Botschaften oder Konsulate (unabhängig vom Sitz).

über- und zwischenstaatliche Stellen (§ 44 III): z.B. Interpol, Nato-Dienststellen.

B. Tatbestand

3 Alternativen für die unterschiedlichen Adressaten der Übermittlung (§ 44 I, II und III):

- § 44 I (Übermittlung an deutsche Ordnungsbehörden und Polizei): Übermittlung erforderlich zur Erfüllung ordnungsbehördlicher oder polizeilicher Aufgaben; dabei Zweckbindung entsprechend § 42 II.

Aufgabenerfüllung: bezieht sich auf die Aufgaben der übermittelnden oder der empfangenden Stelle. Gemeint sind die Aufgaben gem. § 1 ASOG. Ergibt sich eine polizeiliche Aufgabe aus einem anderen Gesetz (§ 1 II ASOG), so stehen der Polizei grundsätzlich die dort geregelten Befugnisse zu (vgl. § 17 II ASOG). Das gilt auch für das Übermitteln. In vielen Spezialgesetzen finden sich entsprechende Befugnisse (z.B. § 76 AuslG). Nur wenn ein Spezialgesetz ausnahmsweise zwar die polizeiliche Aufgabe eröffnet, aber keine Befugnisse zum Übermitteln von Daten enthält, ist insoweit ein Rückgriff auf § 44 I ASOG möglich.

erforderlich: der Zweck darf nicht durch einen geringeren Eingriff als durch Übermittlung erreicht werden können. Außerdem muss sich der Umfang der Daten auf das zur Zweckerfüllung notwendige Maß beschränken.

Zweckbindung: § 44 I 2 ordnet die entsprechende Anwendung von § 42 II an. Grundsätzlich dürfen die Daten also nur zu dem Zweck übermittelt werden, zu dem sie auch erlangt wurden. Ausnahmsweise ist eine Zweckänderung bei der Übermittlung zulässig, wenn der Empfänger selbst die Daten auch zu dem neuen Zweck hätte erheben können.

Keine Zweckänderung liegt vor bei der Übermittlung zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen sowie bei der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen (§ 42 II 3 analog).

Umstritten ist, ob die Zweckbindung so weit geht, dass bei der Übermittlung vorausgesetzt werden muss, dass der Empfänger die Daten auch *mit seinen Mitteln* hätte erheben dürfen. Dann wäre z.B. die Übermittlung von Daten, die durch die Polizei nach § 25 erhoben wurden (längerfristige Observation und Einsatz technischer Mittel) an die Ordnungsbehörden auch dann nicht zulässig, wenn diese die Daten zu dem neuen Zweck eigentlich nutzen dürften; denn den Ordnungsbehörden stehen die Datenerhebungsmittel des § 25 nicht zur Verfügung (so Berg/Knape/Kiworr § 44 III.A.1.b). Ein solches Verständnis der Zweckbindung geht jedoch zu weit. Die in der Rspr. des BVerfG entwickelte Zweckbindung verlangt lediglich eine Bindung der weiteren Verarbeitung und Nutzung von Daten an deren Erhebungszweck, unabhängig davon, mit welchen (Zwangs-)mitteln die Daten rechtmäßig erhoben wurden.

Weil § 44 I 2 nur auf § 42 II, nicht auf § 42 III verweist, gilt die generelle Zulässigkeit der Zweckänderung gem. § 42 III nicht im Fall der Übermittlung. Der Wechsel vom Strafverfolgungszweck zum Gefahrenabwehrzweck beurteilt sich daher bei der Übermittlung ebenfalls nach § 42 II, ist also nur zulässig, wenn die Daten vom Empfänger für Zwecke der Gefahrenabwehr hätten erhoben werden dürfen (a.A. wohl Berg/Knape/Kiworr, § 44 III.A.1.a: die Übermittlung von Daten, die ursprünglich zu Zwecken der Strafverfolgung erhoben wurden, an Ordnungsbehörden sei generell unzulässig).

Wegen ihrer verfassungsrechtlichen Verankerung (Recht auf informationelle Selbstbestimmung nach dem Volkszählungsurteil des BVerfG) gilt die Zweckbindung in Gestalt der Verweisung auf § 42 II nicht nur für die Fälle des § 44 I, sondern auch für Übermittlungen nach § 44 II und III.

- § 44 II (Übermittlung an Behörden oder sonstige Stellen):

Übermittlung erforderlich ...

1. zur Erfüllung ordnungsbehördlicher oder polizeilicher Aufgaben,
2. zur Abwehr einer Gefahr für oder durch den Empfänger,
3. zur Abwehr erheblicher Nachteile für das Gemeinwohl oder
4. zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer Person

ordnungsbehördliche oder polizeiliche Aufgaben: vgl. § 1 ASOG. Es muss sich noch nicht um eine *bestimmte* Aufgabe handeln; vielmehr genügt die Aufgabenerfüllung schlechthin (anders als bei § 44 III 1 Nr. 1). Weil die Behörden und sonstigen Stellen gerade keine Gefahrenabwehrbehörden sind, muss die Übermittlung der Erfüllung der Aufgaben der übermittelnden Ordnungsbehörde oder Polizei dienen. Eine Übermittlung zur Erfüllung der Aufgaben des *Empfängers* kommt hier – anders als bei § 44 I – nicht in Betracht.

Abwehr einer Gefahr für oder durch den Empfänger: gemeint ist konkrete Gefahr i.S.v. § 17 I ASOG. Die Gefahr kann dem Empfänger drohen oder von ihm abgewehrt werden.

erhebliche Nachteile für das Gemeinwohl: Der Begriff des Nachteils liegt unterhalb der Gefahrenschwelle. Gemeint sind Nachteile von einigem Gewicht für Gemeinschaftsgüter wie z.B. die Volksgesundheit.

schwerwiegende Beeinträchtigung der Rechte einer Person: Es muss ein besonders umfangreicher Schaden für Rechtsgüter einer Person zu besorgen sein. Die Schwelle der konkreten Gefahr muss dabei noch nicht überschritten sein.

Es kommt v.a. der Schutz privater Rechte in Betracht (z.B. auch durch eine Datenübermittlung an Gerichte). Die Aufgabeneröffnung hierfür ergibt sich aus § 1 IV ASOG; dabei sind die dort geregelten Einschränkungen zu beachten. Aber auch der Schutz von Rechtsgütern der öffentlichen Sicherheit (Leib, Leben, Gesundheit, Freiheit, Vermögen, Eigentum) kann unter diese Alternative fallen (wichtig, wenn die Gefahrenschwelle noch nicht erreicht ist).

- § 44 III (Übermittlung an ausländische, über- und zwischenstaatliche Stellen):

Übermittlung erforderlich ...

1. zur Erfüllung einer Aufgabe der Ordnungsbehörde oder der Polizei oder
2. zur Abwehr einer erheblichen Gefahr für oder durch den Empfänger oder
3. Berechtigung oder Verpflichtung zur Übermittlung auf Grund über- oder zwischenstaatlicher Vereinbarungen

keine Übermittlung, wenn Grund zu der Annahme besteht, dass

- Verstoß gegen den Zweck eines deutschen Gesetzes oder
- Beeinträchtigung schutzwürdiger Belange des Betroffenen vorliegt.

eine Aufgabe der Ordnungsbehörde oder der Polizei: vgl. § 1 ASOG. Gemeint sind hier die Aufgaben der übermittelnden Ordnungsbehörde oder Polizei; eine Übermittlung zur Erfüllung der Aufgaben des *Empfängers* ist nach Nr. 2 zulässig. Aus der Bezeichnung „eine Aufgabe“ lässt sich entnehmen, dass es sich um eine *bestimmte* Aufgabe handeln muss – anders als bei § 44 II Nr. 1.

Abwehr einer erheblichen Gefahr für oder durch den Empfänger: Erhebliche Gefahr ist eine Gefahr für ein bedeutsames Rechtsgut. Die Gefahr kann dem Empfänger drohen oder von ihm abgewehrt werden.

über- oder zwischenstaatliche Vereinbarungen: durch solche Vereinbarungen kann eine Berechtigung oder Verpflichtung zur Datenübermittlung begründet werden. Beispiel: Schengener Durchführungsübereinkommen (SDÜ) mit Regelungen zum Schengener Informationssystem (SIS).

Verstoß gegen den Zweck eines deutschen Gesetzes: z.B. Art. 1 I i.V.m. 2 I GG und Art. 33 VvB (Recht auf informationelle Selbstbestimmung, gilt auch für Ausländer), die Datenschutzgesetze des Bundes und der Länder, die Datenschutzbestimmungen der StPO.

Beeinträchtigung schutzwürdiger Belange des Betroffenen: z.B. ungerechtfertigte Nachteile in rechtlicher, wirtschaftlicher oder ideeller Hinsicht. Beispiel: Gefahr des Todes.

C. Adressat

Die Adressatenregelung ergibt sich aus den Adressatenregelungen der Datenerhebungs- bzw. Speichervorschriften, aufgrund derer die übermittelnde Stelle die Daten jeweils erlangt hat. Soweit in § 44 die Übermittlung zur „Aufgabenerfüllung“ erfolgt und soweit dabei die Aufgabe in der vorbeugenden Straftatenbekämpfung besteht (§ 1 III ASOG), ergibt sich die Adressatenregelung aus § 16 III ASOG.

D. Zuständigkeit

Ordnungsbehörden und Polizei.

E. Verfahrensvorschriften

- § 44 III 3 (Übermittlung an ausländische, zwischen- oder überstaatliche Stellen): Der Empfänger ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck genutzt werden dürfen, zu dessen Erfüllung sie ihm übermittelt wurden. Dies ist eine reine Verfahrensvorschrift; der Hinweis kann keine Verpflichtung der ausländischen Stelle zur Zweckbindung begründen. Bei Zweifel an der Einhaltung der Zweckbindung muss die Übermittlung aber u.U. unterbleiben, wenn Grund zu der Annahme besteht, dass wegen mangelnder Zweckbindung beim Empfänger die Übermittlung gegen den Zweck der deutschen Datenschutzvorschriften verstoßen würde (§ 44 III 2).
- § 44 IV: Personenbezogene Daten über Kontakt- und Begleitpersonen (§ 25 II 1 Nr. 2), Zeugen, Hinweisgeber und sonstige Auskunftspersonen sowie wertende Angaben dürfen nur an andere Ordnungsbehörden und Polizeibehörden übermittelt werden.

Zweck der Regelung: Daten über andere Personen (Nichtstörer, Unbeteiligte) sowie sensible Daten sollen nur den Ordnungsbehörden und der Polizei zur Verfügung gestellt werden. Dadurch wird der potenzielle Nutzerkreis dieser Daten von vornherein eingeschränkt.

Wertende Angaben: wie bei § 43 II. Z.B. gefährliche Verhaltensweisen, krankheitsbedingte Gemütsverfassungen, Suchtneigungen.

- § 44 V: Prüfungspflicht der übermittelnden Stelle. Satz 1 regelt den Grundsatz, dass die übermittelnde Stelle die Zulässigkeit der Übermittlung zu prüfen habe. Das ergibt sich schon daraus, dass die übermittelnde Stelle Adressat der Übermittlungsregelungen ist. Satz 2 bestimmt, dass im Falle des Ersuchens seitens des Empfängers die Prüfung grundsätzlich nur die Frage umfasst, ob die beabsichtigte Datennutzung zu den Aufgaben des Empfängers gehört. Bestehen jedoch (durch konkrete Anhaltspunkte gestützte) Zweifel an der Rechtmäßigkeit der Nutzung durch den Empfänger, so ist die übermittelnde Stelle ausnahmsweise zur vollen Überprüfung der Zulässigkeit der Übermittlung verpflichtet (Satz 3). Dabei hat der Empfänger die erforderlichen Angaben zu machen (Satz 4).

F. Bezüge zu anderen Vorschriften

Es gibt zahlreiche Übermittlungsvorschriften in Spezialgesetzen, die Vorrang gegenüber § 44 ASOG haben (vgl. § 44 VIII), z.B.:

§§ 161, 163 II StPO (Datenübermittlung der Polizei an die Staatsanwaltschaft)

§§ 11, 13 BKAG (Datenübermittlung in INPOL)

§ 18 I, II (Übermittlung an die Verfassungsschutzbehörden)

§ 22 BVerfSchG (Übermittlung durch StA u. Polizei an den Militärischen Abschirmdienst)

§ 8 II BND-Gesetz (Übermittlung an den Bundesnachrichtendienst)

§ 27 I, II BlnVSG (Übermittlung an das Landesamt für Verfassungsschutz)

§ 29d III 2 LuftverkehrsG (Übermittlung an die Luftfahrtbehörde für die Beurteilung der Zuverlässigkeit des Flughafenpersonals)

G. Probleme

- **§ 44 VI** regelt die Zweckbindung des Empfängers der Daten. Adressat dieser Regelung ist daher nicht die übermittelnde Stelle, sondern der Empfänger. Das ist problematisch, soweit der Landesgesetzgeber überhaupt nicht zuständig ist für Regelungen hinsichtlich des Empfängers, z.B. wenn der Empfänger eine Bundesbehörde ist. Insoweit ist die Regelung verfassungswidrig bzw. muss verfassungskonform ausgelegt und auf diejenigen Behörden beschränkt werden, für die der Berliner Gesetzgeber die Regelungskompetenz hat. Aber auch insoweit ist die Regelung problematisch, weil es ihr an Normklarheit mangelt – das ASOG richtet sich sonst nur an Ordnungsbehörden und Polizei, und eine Regelung über andere Behörden ist im ASOG zumindest unvermutet und überraschend.
„soweit gesetzlich nichts anderes bestimmt ist“: z.B. in § 44 I 2 i.V.m. § 42 II ASOG ist die Möglichkeit einer Zweckänderung vorgesehen; Ähnliches kann sich aus Spezialgesetzen ergeben.
- **§ 44 VII** trifft scheinbar eine Regelung hinsichtlich der Zulässigkeit der Übermittlung durch andere Behörden an die Polizei und spricht sogar eine Verpflichtung zu einer solchen Übermittlung in bestimmten Fällen aus. Diese Regelung ist jedoch rechtlich bedeutungslos, wenn nicht verfassungswidrig. Die Befugnisse der anderen Behörden (also gerade nicht der Ordnungsbehörden und der Polizei) sind nämlich nicht im ASOG, sondern in – vorrangigen – Spezialgesetzen geregelt. Soweit unter diesen anderen Behörden auch z.B. Behörden des Bundes oder anderer Bundesländer verstanden werden, hat der Berliner Gesetzgeber schon keine Kompetenz für eine solche Regelung. § 44 VII hat daher allenfalls eine Auffangfunktion für solche anderen Berliner Landesbehörden, für die keine spezialgesetzliche Übermittlungsregelung existiert. Welche Fälle das sein sollten, ist unklar.

Kapitel 12: Datenübermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs (§ 45 ASOG)

Normadressat dieser Regelung sind die Ordnungsbehörden und die Polizei als übermittelnde Stellen. Übermittlungsempfänger sind Private; aus ihrer Sicht stellt die Übermittlung einer Erhebung bzw. Speicherung von Daten dar. Regelungen über die Zulässigkeit solcher privater Datenverarbeitung enthält das BDSG.

A. Rechtsfolge

Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs

Übermittlung: vgl. § 4 II Nr. 4 BlnDSG: das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die datenverarbeitende Stelle an den Dritten weitergegeben werden oder dass der Dritte zum Abruf bereitgehaltene Daten abrufen.

Das Abrufen bereitgehaltener Daten fällt nicht unter § 45, weil hierfür die Spezialvorschrift des § 46 gilt; demnach ist ein automatisiertes Abrufverfahren nur zwischen Polizeibehörden zulässig (also nicht zwischen Polizei und privaten Stellen).

Personen oder Stellen außerhalb des öffentlichen Bereichs: natürliche Personen (als solche, nicht als Amtsträger) und juristische Personen oder sonstige (auch nicht rechtsfähige) Personenvereinigungen des Privatrechts. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, so fällt sie nicht unter § 45; die Übermittlung an sie richtet sich vielmehr nach § 44 (vgl. dazu den – allerdings hier nicht direkt anwendbaren – § 2 IV 2 BDSG).

Es kann sich um in- oder ausländische Personen oder Stellen handeln.

B. Tatbestand

5 Alternativen:

Erforderlichkeit der Übermittlung ...

1. zur Erfüllung ordnungsbehördlicher oder polizeilicher Aufgaben,
2. zur Abwehr erheblicher Nachteile für das Gemeinwohl,
3. zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer Person
oder wenn
4. der Auskunftsbeghernde ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und die schutzwürdigen Interessen der betroffenen Person nicht überwiegen oder
5. der Auskunftsbeghernde ein berechtigtes Interesse geltend macht und offensichtlich ist, dass die Datenübermittlung im Interesse der betroffenen Person liegt, die betroffene Person eingewilligt hat oder in Kenntnis der Sachlage ihre Einwilligung hierzu erteilen würde.

zu 1.: Aufgabenerfüllung: nach § 1 ASOG, also insbesondere Gefahrenabwehr.

Beispiele:

- Gefahrenabwehr bei bevorstehender Entführung durch Übermittlung von Daten potenzieller Täter (auch Lichtbilder) an das potenzielle Entführungsoffer.
- Öffentlichkeitsfahndung (Zeitung, Fernsehen, Radio) nach vermissten geistig verwirrten Personen (z.B. aus einem Altenheim Abgängige). Wegen des mit der Einbeziehung der Öffentlichkeit verbundenen tiefen Eingriffs in das Recht auf informationelle Selbstbestimmung ist besonders der Grundsatz der Verhältnismäßigkeit zu beachten; diese Maßnahme ist daher wohl nur bei gegenwärtiger Gefahr für Leib oder Leben zulässig.
- Auskünfte an die Presse erfolgen *nicht* nach § 45 ASOG, sondern nach der Spezialregelung des § 4 PresseG. Demnach besteht zwar nach § 4 I PresseG eine allgemeine Auskunftspflicht der Polizei gegenüber der Presse; diese Pflicht wird aber eingeschränkt durch § 4 II Nr. 4 PresseG, wonach die Auskunft verweigert werden kann, wenn ein schutzwürdiges privates Interesse verletzt werden kann. Ein solches Interesse ist das Recht auf informationelle Selbstbestimmung des Betroffenen. Daher dürfen Mitteilungen an die Presse i.d.R. keine personenbezogenen Angaben enthalten, der Betroffene darf also nicht einmal bestimmbar sein. Auskünfte über Ereignisse müssen sich daher i.d.R. beschränken auf Ereignis, Wohnbezirk, Geschlecht und Alter. Etwas anderes gilt nur für absolute oder relative Personen der Zeitgeschichte, d.h. für Personen, die selbst im Interesse der Öffentlichkeit stehen oder die im Zusammenhang mit einem Ereignis stehen, an dem die Öffentlichkeit ein gesteigertes Interesse hat. Hier muss aber eine Abwägung zwischen dem Informationsinteresse der Öffentlichkeit und dem Recht auf informationelle Selbstbestimmung des Betroffenen stattfinden.

zu 2.: erhebliche Nachteile für das Gemeinwohl: Tatbestand wie bei § 44 II Nr. 3. Der Begriff des Nachteils liegt unterhalb der Gefahrenschwelle. Gemeint sind Nachteile von einigem Gewicht für Gemeinschaftsgüter wie z.B. die Volksgesundheit.

Beispiele:

- Öffentliche Warnung vor gesundheitsschädlichem Speiseöl
- Öffentlichkeitsfahndung nach gemeingefährlichen Geisteskranken oder Personen mit ansteckenden Krankheiten
- Übermittlung der Daten von öfter in Erscheinung getretenen gewaltbereiten Hooligans an den Veranstalter eines Fußballspiels, damit dieser ggf. Teilnahmeverbote aussprechen kann

zu 3.: schwerwiegende Beeinträchtigung der Rechte einer Person: Tatbestand wie bei § 44 II Nr. 4; es muss ein besonders umfangreicher Schaden für Rechtsgüter einer Person zu besorgen sein. Dabei kommt v.a. der Schutz privater Rechte in Betracht. Die Aufgabeneröffnung hierfür ergibt sich aus § 1 IV ASOG; dabei sind die dort geregelten Einschränkungen zu beachten. Aber auch der Schutz von Rechtsgütern der öffentlichen Sicherheit (Leib, Leben, Gesundheit, Freiheit, Vermögen, Eigentum) kann unter diese Alternative fallen (wichtig, wenn die Gefahrenschwelle noch nicht erreicht ist).

zu 4.: rechtliches Interesse des Auskunftsbefragenden an der Kenntnis der Daten: Es muss ein Auskunftsbegehren, d.h. ein schriftlicher oder mündlicher Antrag auf Datenübermittlung vorliegen. „Rechtliches Interesse“ setzt das Bestehen eines Rechtsverhältnisses voraus. Der Empfänger muss die Daten zur Rechtswahrung benötigen, z.B. weil er eine Zivilklage oder eine strafrechtliche Privatklage (§§ 374 ff. StPO) erheben will.

Da es sich um den Schutz privater Rechte handelt, sind die zusätzlichen Voraussetzungen des § 1 IV ASOG zu beachten. Dabei ist zu bedenken, dass rechtzeitiger gerichtlicher Schutz für den Geschädigten zumindest bei Privatklagedelikten gem. § 403 ff. StPO auch dann zu erlangen ist, wenn die Polizei die benötigten Daten nicht dem Auskunftsbefragenden selbst, son

dem z.B. dem zuständigen Gericht übermittelt und dem Auskunftsbeghernden nur das gerichtliche Aktenzeichen mitteilt. Ist eine solche Möglichkeit gegeben, so ist eine Übermittlung der Daten an den privaten Geschädigten nach § 1 IV ASOG unzulässig.

Beispiele:

- Bei einem Verkehrsunfall wäre die Bekanntgabe der Daten des Schädigers an den Geschädigten nur dann zulässig, wenn voraussichtlich kein Strafverfahren eröffnet wird.
- Zahlungsstreitigkeiten zwischen Schankwirt und Gast oder Taxifahrer und Fahrgast
- Hundebiss, Beschädigung eines Mantels durch Zigarette

glaubhaft machen: bloße Behauptung genügt nicht. Andererseits sind nicht allzu hohe Anforderungen an den Nachweis des rechtlichen Interesses zu stellen; ein Beweis im strengen Sinne ist sicher nicht erforderlich.

schutzwürdige Interessen des Betroffenen: v.a. das Recht auf informationelle Selbstbestimmung, aber evtl. auch andere Interessen. Es muss eine Abwägung mit den Interessen des Auskunftsbeghernden stattfinden. Dabei ist auch zu berücksichtigen, wie „sensibel“ die übermittelten Daten sind.

zu 5.: berechtigtes Interesse des Auskunftsbeghernden: muss kein rechtliches Interesse sein (vgl. Nr. 4); es genügt auch z.B. ein rein wirtschaftliches oder ideelles Interesse.

im Interesse der betroffenen Person: wenn eine Person bei der Polizei anfragt, ob ein Angehöriger, der dringend Medikamente benötigt, sich im Gewahrsam der Polizei befindet.

Einwilligung der betroffenen Person: z.B. gebrechliche Person bittet die Polizei, bei einem Verwandten anzurufen, damit dieser sie nach Hause bringe.

die betroffene Person würde in Kenntnis der Sachlage ihre Einwilligung erteilen: z.B. wenn sich ein Angehöriger danach erkundigt, in welches Krankenhaus ein Unfallopfer eingeliefert wurde.

C. Adressat

Die Adressatenregelung ergibt sich aus den Adressatenregelungen der Datenerhebungs- bzw. Speichervorschriften, aufgrund derer die übermittelnde Stelle die Daten jeweils erlangt hat.

D. Zuständigkeit

Ordnungsbehörden und Polizei.

E. Verfahrensvorschriften

- §§ 45 II i.V.m. 44 V analog: Die Prüfungspflicht für die Zulässigkeit der Übermittlung liegt grundsätzlich bei der übermittelnden Stelle. Ausnahmen dürften bei Privaten als Übermittlungsempfänger kaum in Betracht kommen – anders als bei öffentlichen Stellen, die selbst für die Rechtmäßigkeit ihrer Datenerhebung und -nutzung verantwortlich sind.
- § 45 III: Der Empfänger ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck genutzt werden dürfen, zu dessen Erfüllung sie ihm übermittelt wurden.

F. Bezüge zu anderen Vorschriften

§ 39 StVG: Übermittlung von Fahrzeug- oder Halterdaten durch die (örtliche) Zulassungsbehörde oder das Kraftfahrt-Bundesamt an Private.

G. Probleme

Aus § 45 II i.V.m. § 44 VI analog ergibt sich, dass der Empfänger die Daten nur zu dem Zweck nutzen darf, zu dem sie ihm übermittelt wurden. Diese Regelung ist wohl als unwirksam anzusehen. Denn Übermittlungsempfänger sind private Stellen. Die Nutzung von Daten durch private Stellen ist aber im BDSG geregelt (z.B. in § 28 BDSG), das als Bundesrecht Vorrang vor dem ASOG hat (Art. 31 GG). Werden die Daten an private Stellen im Ausland übermittelt, kann deutsches Recht ohnehin die Nutzung durch den Empfänger nicht regeln.

A. Beschreibung des automatisierten Abrufverfahrens

Beim automatisierten Abrufverfahren werden Daten von der speichernden Stelle für Dritte zum Abruf bereitgehalten. Der Abruf erfolgt dann online ohne weiteres Zutun der speichernden Stelle; er stellt aus der Sicht der speichernden Stelle eine Übermittlung dar. Das bloße Bereithalten von Daten zum Abruf ist dagegen noch keine Übermittlung; vgl. dazu die Definition der Übermittlung in § 4 II Nr. 4 BlnDSG: „Übermitteln (ist) das Bekanntgeben gespeicherter ... Daten in der Weise, dass die Daten durch die datenverarbeitende Stelle an den Dritten weitergegeben werden oder dass der Dritte zum Abruf bereitgehaltene Daten abruft“.

B. Regelungsgehalt des § 46 ASOG

Es ist umstritten, ob schon die Einrichtung eines automatisierten Abrufverfahrens einen Eingriff darstellt oder der Eingriff erst beim jeweiligen Abruf erfolgt und ob demnach § 46 ASOG eine Befugnisnorm darstellt oder nicht. Jedenfalls regelt § 46 ASOG besondere Voraussetzungen für die Übermittlung von Daten durch automatischen Abruf.

C. Voraussetzungen der Einrichtung eines automatisierten Abrufverfahrens (§ 46 I)

- Es muss sich um eine von der Polizei geführte Datei handeln. Für den Abruf aus Dateien von Ordnungsbehörden bietet § 46 keine Grundlage.
- Das Abrufverfahren muss der Erfüllung polizeilicher Aufgaben (§ 1 ASOG) dienen.
- Die Abwägung der Vorteile des Abrufverfahrens für die Aufgabenerfüllung gegenüber den schutzwürdigen Belangen der Betroffenen muss zugunsten der Aufgabenerfüllung ausfallen. Die Vorteile des Abrufverfahrens liegen v.a. in der Beschleunigung der Datenübermittlung; schutzwürdiger Belang der Betroffenen ist v.a. deren Recht auf informationelle Selbstbestimmung.
- Der Abruf darf nur anderen Polizeibehörden gestattet werden (§ 46 I 2), d.h. deutschen Polizeidienststellen.

D. Notwendige Maßnahmen zur Sicherung des Datenschutzes

- Gem. 46 II die nach § 5 BlnDSG erforderlichen technischen und organisatorischen Maßnahmen, also z.B. die Zugangsbeschränkung auf Befugte. Die zu treffenden Maßnahmen müssen schriftlich festgehalten werden. Das geschieht i.d.R. in der nach § 49 ASOG notwendigen Errichtungsanordnung.
- Gewährleistung von stichprobenmäßigen Überprüfungen (§ 46 III). Das geschieht v.a. mit Hilfe von Protokolldateien; diese müssen nicht jeden Abruf erfassen, es genügen Stichproben.
- Rechtsverordnung zur Einrichtung automatisierter Abrufverfahren (§ 46 IV). Eine solche Rechtsverordnung ist bisher nicht ergangen. Nach einhelliger Auffassung führt das aber nicht zur Rechtswidrigkeit der bereits jetzt durchgeführten Abrufverfahren.

E. Datenverbund

Nach § 46 V kann die Berliner Polizei den Polizeien anderer Länder und mit dem Bund (BKA) einen Datenverbund vereinbaren. Beispiele: INPOL, KAN-Bund (teilweise wird aber bestritten, dass es sich hier um einen Verbund im Sinne des § 46 V handele, weil das BKA seinerseits keine Daten aus den Länderdateien abrufe).

Kapitel 14: Datenabfragen, Datenabgleich (§ 28 ASOG)

Die Maßnahmen nach § 28 stellen regelmäßig Folgeeingriffe zu einer Identitätsfeststellung (§ 21), Befragung (§ 18 III 3) oder einer erkennungsdienstlichen Maßnahme (§ 23) dar. Nach der Regelungssystematik des ASOG handelt es sich dennoch um eigenständige Maßnahmen, für die § 28 ASOG eine Befugnisnorm darstellt.

A. Rechtsfolge

- Datenabfrage und Datenabgleich in einer von derselben Behörde geführten automatisierten Datei (§ 28 I 1)
- Datenabfrage und Datenabgleich im Fahndungsbestand (§ 28 I 2)
- Anhalten für die Dauer der Abfrage oder des Abgleichs (§ 28 I 3)

Datenabgleich: Ein vorhandenes Merkmal wird mit Merkmalen gleicher Kategorie in einem vorhandenen Datenbestand verglichen; das Ergebnis ergibt nur, ob dieses Merkmal vorhanden (gespeichert) ist oder nicht.

Datenabfrage: Auch hier findet zunächst ein Datenabgleich mit einem vorhandenen Merkmal statt, jedoch mit dem Ziel, weitere mit diesem Merkmal gespeicherte oder verknüpfte Daten zu erlangen.

von derselben Behörde geführt: § 28 regelt nur die Befugnis der Polizei und der Ordnungsbehörden zu Abgleich und Abfrage in jeweils den eigenen Dateien. Befugnisse zu Abgleich und Abfragen in Dateien anderer Behörden (z.B. der Meldebehörden) sind in Spezialgesetzen geregelt (z.B. § 26 MeldeG i.V.m. der DVO-MeldeG).

automatisierte Datei: vgl. § 4 III Nr. 5 BlnDSG: Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann. Nicht automatisierte Dateien (z.B. Karteien) fallen nicht unter § 28. Abgleich und Abfrage von nicht automatisierten Dateien sind nach § 42 (als Nutzung) bzw. nach § 18 I (als Datenerhebung) zulässig.

Fahndungsbestand: Dateien zur Sach- und Personenfahndung; z.B. ISVB, INPOL.

Anhalten: kurzzeitig, für die Dauer der Abfrage oder des Abgleichs. Stellt lediglich eine Freiheitsbeschränkung dar (Art. 104 I GG), keine Freiheitsentziehung (Art. 104 II GG).

B. Tatbestand

- **§ 28 I 1:** Tatsachen müssen die Annahme rechtfertigen, dass Abgleich bzw. Abfrage für die Erfüllung einer bestimmten ordnungsbehördlichen oder polizeilichen Aufgabe im Rahmen der Zweckbestimmung der Datei erforderlich ist.

Tatsachen: tatsächliche einzelfallbezogene Anhaltspunkte.

bestimmte ordnungsbehördliche oder polizeiliche Aufgabe: eine konkrete Aufgabe gem. § 1 ASOG. Es muss schon eine bestimmte Angelegenheit vorliegen, die allgemeine Aufgabenerfüllung genügt nicht.

im Rahmen der Zweckbestimmung der Datei: auch innerhalb einer Behörde (Ordnungsbehörde oder Polizei) werden Dateien mit verschiedenen Zweckbestimmungen geführt. Entsprechend dem Grundsatz der Zweckbindung beschränkt § 28 I 1 den Abgleich und die Abfrage auf die Fälle, in denen die ursprüngliche Zweckbindung beachtet wird.

Beispiel: Daten von gewaltbereiten Personen dürfen nicht mit der Rauschgiftdatei abgeglichen werden.

Erforderlichkeit: muss hinsichtlich des Umfangs der abgefragten bzw. abgeglichenen Daten und hinsichtlich der Abfrage bzw. des Abgleichs als solchem gegeben sein.

- **§ 28 I 2:** Abfrage bzw. Abgleich müssen im Rahmen der Aufgabenerfüllung erfolgen; die abgefragten bzw. abgeglichenen Daten müssen rechtmäßig erlangt sein. Die Annahme muss gerechtfertigt sein, dass die Abfrage oder der Abgleich sachdienliche Hinweise erwarten lässt.

im Rahmen der Aufgabenerfüllung: vgl. § 1 ASOG. Es ist also zulässig, im Rahmen der Gefahrenabwehr gewonnene Daten mit dem Fahndungsbestand, der meist einen repressiven Zweck hat, abzugleichen bzw. eine entsprechende Abfrage vorzunehmen. Insoweit lässt § 28 I 2 eine Zweckänderung zu.

rechtmäßig erlangt: z.B. durch vorhergehende Datenerhebung nach § 18 ASOG oder auch unaufgefordert durch Dritte (vgl. § 42 I 2).

Annahme gerechtfertigt: Im Unterschied zu § 28 I 1 ist hier das Vorliegen von einzelfallbezogenen Tatsachen, auf denen die Annahme beruht, nicht erforderlich. Dennoch müssen Anhaltspunkte vorliegen, die aber auch allgemeiner Art sein können, z.B. das Antreffen einer Person an einem Ort, an dem nach kriminalistischer Erfahrung häufig Personen aus bestimmten Milieus angetroffen werden.

sachdienliche Hinweise: die Hinweise müssen sich auf eine konkrete Angelegenheit beziehen. Damit sind Routine- und Regelabfragen ausgeschlossen.

- **§ 28 I 3:** Anhalten ist zulässig, wenn die Voraussetzungen von § 28 I 1 oder von § 28 I 2 erfüllt sind.

C. Adressat

Ergibt sich nicht aus den allgemeinen Vorschriften, sondern aus der Adressatenregelung der vorhergehenden Maßnahme (z.B. einer Maßnahme nach §§ 21, 18 III oder 23).

D. Zuständigkeit

§ 28 I 1: Ordnungsbehörden und Polizei

§ 28 I 2: Nur die Polizei

E. Verfahrensvorschriften

keine besonderen.

F. Bezüge zu anderen Vorschriften

Nach § 28 II bleiben besondere Rechtsvorschriften über den Datenabgleich unberührt.

Beispiele für diese spezialgesetzlichen Regelungen:

- § 98c StPO
- §§ 30 ff., 35 ff., 52 ff. StVG
- §§ 25 ff. MeldeG
- § 17 PaßG.

Kapitel 15: Besondere Formen des Datenabgleichs (§ 47 ASOG: „Rasterfahndung“)

Bei der im Zuge der Terroristenfahndung in den 70er Jahren eingeführten Rasterfahndung werden große Datenmengen (z.B. von Energieversorgungsunternehmen, Wohnungsbaugesellschaften, Banken) nach bestimmten Merkmalen (Raster) abgesucht, um bei Übereinstimmung entweder bestimmte Datensätze herauszufiltern (positive Rasterfahndung) oder auszuschließen (negative Rasterfahndung). Dieser Methode liegt die Annahme zugrunde, dass ein bestimmter Kreis von Tätern (bzw. Störern) sich durch ein bestimmtes Raster von Merkmalen auszeichnet.

Die Rasterfahndung wurde zuletzt im Zusammenhang mit den Anschlägen des 11. September 2001 in größerem Umfang durchgeführt. Vgl. dazu den Sonderbericht des Berliner Datenschutzbeauftragten; der Bericht ist im Internet zugänglich unter

<http://www.datenschutz-berlin.de/infomat/sonderbericht/rasterfahndung.pdf>

A. Rechtsfolge

Das Verlangen der Übermittlung von personenbezogenen Daten (Namen, Anschriften, Tag und Ort der Geburt sowie im Einzelfall festzulegende Merkmale) bestimmter Personengruppen aus Dateien von öffentlichen Stellen oder Stellen außerhalb des öffentlichen Bereichs sowie der Abgleich dieser Daten mit anderen Datenbeständen.

Verlangen: § 47 I ASOG begründet nicht nur die Befugnis, die Übermittlung von Daten zu verlangen; die ersuchte Stelle ist vielmehr aufgrund eines solchen Verlangens auch zur Übermittlung verpflichtet (§ 47 I 2).

Übermittlung: vgl. § 4 II Nr. 4 BlnDSG.

personenbezogene Daten: Die personenbezogenen Daten, deren Übermittlung verlangt werden kann, sind in § 47 II aufgezählt: grundsätzlich sind dies nur Namen, Anschriften und Tag und Ort der Geburt. Darüber hinaus können weitere personenbezogene Merkmale verlangt werden, soweit sie zur Abwehr der Gefahr erforderlich sind (vgl. Tatbestand).

bestimmte Personengruppen: Die Polizei muss bei ihrem Übermittlungsverlangen die Personengruppe möglichst genau spezifizieren, deren Daten übermittelt werden soll. Diese Personen müssen zumindest einem groben Merkmalsraster entsprechen, das für die Gefahrenabwehr relevant ist.

aus Dateien: gemeint sind automatisierte und nicht automatisierte Dateien (vgl. § 4 III Nr. 5 BlnDSG). Die Vorschrift gilt also auch für Daten, die z.B. in Karteien niedergelegt sind.

öffentliche Stellen: gemeint sind Behörden und andere öffentliche Stellen. Problematisch ist dabei, ob die Polizei bei einer Weigerung einer öffentlichen Stelle ihr Übermittlungsverlangen auch vollstrecken könnte. Nach § 17 VwVG sind Zwangsmittel gegen Behörden unzulässig, „soweit nicht etwas anderes bestimmt ist“. Nach einer Ansicht (Berg/Knape/Kiworr) kann aus § 47 I 2 ASOG abgeleitet werden, dass hier eine Vollstreckung gegen Behörden zulässig sein soll. Das ist jedoch zweifelhaft, weil sich aus § 47 I 2 ASOG lediglich die Verpflichtung der Behörde zur Übermittlung ableiten lässt, nicht aber eine weitergehende Vollstreckungsbefugnis der Polizei. Im Weigerungsfalle muss ggf. die jeweilige Aufsichtsbehörde eingeschaltet werden (str.).

Stellen außerhalb des öffentlichen Bereichs: gemeint sind Private (natürliche und juristische Personen). Das Übermittlungsverlangen kann hier unproblematisch auch vollstreckt werden: Es stellt einen Verwaltungsakt dar, der eine Handlung anordnet, und ist eine unau

schiebbare vollzugspolizeiliche und daher gem. § 80 II Nr. 2 VwGO vollziehbare Maßnahme; daher sind die Voraussetzungen des § 6 I VwVG erfüllt. Ggf. ist auch ein Sofortvollzug unter den Voraussetzungen des § 6 II VwVG zulässig.

Abgleich mit andere Datenbeständen: „andere Datenbestände“ können sowohl polizeieigene als auch externe Dateien sein. „Abgleich“ bedeutet die Überprüfung auf Übereinstimmung bestimmter Merkmale. Beim negativen Abgleich werden die Datensätze ohne Übereinstimmung gelöscht, beim positiven Abgleich wird eine neue Datei mit den übereinstimmenden Datensätzen erstellt.

Die Nutzung dieser Ergebnisdaten für weitere Ermittlungen kann unter den Voraussetzungen der jeweils einschlägigen Befugnisnormen erfolgen (z.B. längerfristige Observation etc.).

B. Tatbestand

zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person, soweit Tatsachen die Annahme rechtfertigen, dass die Maßnahme zur Abwehr der Gefahr erforderlich ist.

gegenwärtige Gefahr: Es gilt grds. die übliche Definition; daher muss eigentlich ein schädigendes Ereignis bereits begonnen haben oder dieses unmittelbar oder in nächster Zeit mit an Sicherheit grenzender Wahrscheinlichkeit bevorstehen. Das Vorliegen einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person wurde anlässlich der Rasterfahndungen in der Folge des 11. September 2001 von den Gerichten in verschiedenen Bundesländern unterschiedlich beurteilt. Einige Gerichte (z.B. in Hessen) lehnten eine gegenwärtige Gefahr mit dem Hinweis darauf ab, es könne nicht mit an Sicherheit grenzender Wahrscheinlichkeit angenommen werden, dass ein weiterer Terrorakt in nächster Zeit bevorsteht. Andere Gerichte (u.a. KG Berlin, Beschl. v. 16.4.2002) bejahten dagegen die gegenwärtige Gefahr, weil eine „Dauergefahr“ vorliege, bei der eine Wahrscheinlichkeitsprognose über den Zeitpunkt des Schadenseintritts gerade nicht möglich sei, die aber jederzeit in einen Schadenseintritt umschlagen könne und bei der das Ausmaß der zu erwartenden Schäden besonders hoch sei. In diesen Fällen seien die Anforderungen an eine „gegenwärtige Gefahr“ geringer.

Bestand oder Sicherheit des Bundes oder eines Landes: zu den Begriffen vgl. §§ 81, 82, 92 StGB.

Tatsachen rechtfertigen die Annahme, dass die Maßnahme zur Abwehr der Gefahr erforderlich ist: bloße Vermutungen genügen nicht; es müssen tatsächliche Anhaltspunkte vorliegen. Die Maßnahme muss hinsichtlich des Umfangs der Personengruppe, über die Daten übermittelt werden, sowie hinsichtlich des Umfangs der übermittelten Datenfelder und auch hinsichtlich der Art der Maßnahme (gibt es geringer beeinträchtigende Alternativen?) erforderlich sein.

C. Adressaten

Adressaten sind nach § 47 I ASOG zum einen die Stellen, von denen die Übermittlung der Daten verlangt wird.

Adressaten sind aber auch die Betroffenen, deren Daten übermittelt und abgeglichen werden. Die Adressatenregelung ergibt sich bei § 47 also vollständig aus der Vorschrift selbst.

D. Zuständigkeit

Nur die Polizei.

E. Verfahrensvorschriften

- **§ 47 IV (Anordnungsbefugnis):** Die Maßnahme darf grds. nur durch den Richter (Amtsgericht Tiergarten) angeordnet werden, bei Gefahr im Verzug ausnahmsweise durch den Polizeipräsidenten oder dessen Vertreter. Die Anordnung muss den zur Übermittlung Verpflichteten sowie alle benötigten Daten und Merkmale bezeichnen. Bei Gefahr im Verzug kann ausnahmsweise der Polizeipräsident oder sein Vertreter im Amt die Maßnahme anordnen. Er muss dann unverzüglich die richterliche Bestätigung der Anordnung beantragen; das gilt auch, wenn die Maßnahme bereits beendet ist. Die Maßnahme wird rechtswidrig, wenn die Anordnung nicht binnen drei Tagen vom Richter bestätigt wird.

Für das gerichtliche Verfahren gilt das FGG analog.

Der Berliner Datenschutzbeauftragte muss durch die Polizei über die Maßnahmen unterrichtet werden.

- **§ 47 II 2 (überflüssige Daten):** Werden wegen technischer Schwierigkeiten (z.B. weil einzelne Datenfelder in den Datensätzen nicht ohne weiteres gelöscht werden können) weitere Daten übermittelt, dürfen diese (z.B. im Rahmen der an die Maßnahme anschließenden weiteren Ermittlungen) nicht verwertet werden.
- **§ 47 III (Löschung und Vernichtung):** Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten auf dem Datenträger zu löschen und die Unterlagen, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind, unverzüglich zu vernichten.

Über die getroffenen Maßnahmen ist eine Niederschrift anzufertigen. Diese Niederschrift ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des der Vernichtung der Unterlagen folgenden Jahres zu vernichten.

zusätzlich angefallene Daten: z.B. die durch Kombination verschiedener Datensätze erzeugte Verknüpfung von Daten; aber auch die wegen technischer Schwierigkeiten „mitübermittelten“ eigentlich überflüssigen Daten (vgl. § 47 II 2).

Löschen: vgl. § 4 II Nr. 6 BlnDSG: das Beseitigen der Daten, d.h. die zukünftige Verwendung muss unmöglich gemacht werden.

Unterlagen: sehr weiter Begriff; umfasst sowohl Akten als auch einzelne Karteiblätter, Notizzettel oder Vermerke.

erforderlich für ein mit dem Sachverhalt zusammenhängendes Verfahren: v.a. ein anschließendes Gerichtsverfahren. Es müssen objektive Anhaltspunkte dafür vorliegen, dass ein solches Verfahren zu erwarten ist.

unverzügliche Vernichtung der Unterlagen: die Unterlagen müssen, sobald die Voraussetzungen der Löschung erfüllt sind und soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind, ohne vermeidbares Zögern unbrauchbar gemacht werden.

Niederschrift über die getroffenen Maßnahmen: mit „Maßnahmen“ sind hier die Löschung der Daten bzw. Vernichtung der Unterlagen gemeint.

gesonderte Aufbewahrung und technische und organisatorische Sicherung der Niederschrift: z.B. in einem Tresor.

F. Bezüge zu anderen Vorschriften

§§ 98a, 98b StPO: Rasterfahndung im Rahmen der Strafverfolgung; Anordnungscompetenz liegt hier auch beim Richter, bei Gefahr im Verzug aber bei der Staatsanwaltschaft.

Datenerhebungsvorschriften: Wenn die nach dem Abgleich verbleibenden und weiter zu nutzenden Daten vor der Rasterfahndung der Polizei noch nicht zur Verfügung standen, müssen hinsichtlich dieser Daten zusätzlich die Voraussetzungen der Datenerhebungsvorschriften (z.B. § 18 ASOG) erfüllt sein.

§ 48 ASOG: Diese Vorschrift tritt zurück gegenüber den spezielleren Lösungs- und Vernichtungsvorschriften des § 47 III ASOG.

G. Probleme

Problematisch an der Rasterfahndung ist zunächst, dass Zweifel an ihrer Geeignetheit bestehen (maßgebliche Erfolge konnten mit ihr bisher nicht erzielt werden). Darüber hinaus ist die Einbeziehung einer Vielzahl von Unbeteiligten in die Maßnahme problematisch; erst recht dann, wenn Unbeteiligte zufällig dem Raster entsprechen und deswegen z.B. observiert oder anderen Maßnahmen unterzogen werden. Daher ist die Rasterfahndung nur unter besonderer Beachtung des Verhältnismäßigkeitsgrundsatzes und strenger Einhaltung der verfahrensmäßigen Vorkehrungen zulässig.

Kapitel 16: Berichtigung, Löschung und Sperrung von Daten (§ 48 ASOG)

§ 48 ASOG stellt keine Befugnisnorm dar, sondern eine Vorschrift, die bestimmte Maßnahmen, die dem Schutz des jeweils Betroffenen dienen, unter bestimmten Voraussetzungen zwingend anordnet.

A. Berichtigung (Abs. 1)

I. Begriff

Für den Begriff der Berichtigung gibt es keine Legaldefinition, weder im ASOG noch im BlnDSG. Es muss darunter jede Anpassung des Datei- bzw. Akteninhalts an die Wirklichkeit verstanden werden. Möglich ist also z.B. eine Änderung der Daten oder die zusätzliche Speicherung weiterer Daten

Für Daten in Akten legt die Spezialregelung des § 48 I 2 ein bestimmtes Berichtigungsverfahren fest: Die Berichtigung erfolgt hier durch Vermerk oder Festhalten auf sonstige Weise. Es muss also ein Hinweis auf die Fehlerhaftigkeit in der Akte selbst erfolgen. Nachträgliches Radieren, Schwärzen, Überschreiben im Text selbst oder gar das Vernichten einzelner Aktenbestandteile wären dagegen unzulässig. Damit soll der Grundsatz der Aktenvollständigkeit gewahrt werden: Der gesamte Vorgang, einschließlich der Fehlerhaftigkeit der Daten und des Berichtigungsvorgangs, muss aus dem Akteninhalt erkenntlich sein.

II. Voraussetzungen der Berichtigungspflicht

Einzigste Voraussetzung der Berichtigungspflicht ist die Unrichtigkeit der gespeicherten Daten. Unrichtigkeit bedeutet dabei, dass die Daten nicht mit der Wirklichkeit übereinstimmen. Wie die Unrichtigkeit zustande kam, also etwa durch Programm- oder Tippfehler, durch Übermittlung falscher Daten oder auch durch nachträgliche Geschehnisse (Freispruch im Strafverfahren), spielt dabei keine Rolle. Die Berichtigung muss von Amts wegen erfolgen, ein Antrag des Betroffenen ist nicht erforderlich.

B. Löschung von Daten in Dateien und Vernichtung von Unterlagen (Abs. 2)

I. Begriffe

Löschung: vgl. § 4 II Nr. 6 BlnDSG: das Beseitigen gespeicherter Daten. Dieser Begriff ist strenger als der Löschungsbegriff in § 3 IV Nr. 5 BDSG, der nur ein „Unkenntlichmachen“ der Daten verlangt. Nach dem Berliner Recht (und damit auch bei § 48 ASOG) genügt ein Unkenntlichmachen, das möglicherweise wieder rückgängig gemacht werden kann, nicht. Vielmehr müssen die Daten endgültig und unwiderruflich beseitigt werden; sie dürfen also nicht wiederherstellbar oder rekonstruierbar sein.

Ist eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, kann an die Stelle der Löschung die Sperrung treten (§ 48 II 3; zum Begriff der Sperrung s.u.).

Die Regelung in Abs. 2 betrifft nur die Daten, die in (automatisierten oder nicht automatisierten) Dateien gespeichert sind. Für Daten in Akten gilt Abs. 3.

Vernichtung von Unterlagen: Der Begriff der Vernichtung ist nicht näher definiert. Auch hier muss verlangt werden, dass die Daten nicht rekonstruierbar sind. In der Regel wird also die physische Vernichtung notwendig sein (Schredder). Der Begriff „Unterlagen“ ist weit zu

verstehen. Gemeint sind nicht nur Akten und Handakten, sondern auch z.B. einzelne Karteiblätter und Notizzettel.

II. Voraussetzungen der Löschung von Daten und Vernichtung von Unterlagen

§ 48 II unterscheidet zwei alternative Voraussetzungen:

1. Unzulässigkeit der Speicherung (Satz 1 Nr. 1)

Diese Voraussetzung ist zunächst dann erfüllt, wenn die Speicherung von Anfang an unzulässig war, d.h. die Voraussetzungen der jeweiligen Befugnisnorm für die Speicherung (v.a. also §§ 42, 43 ASOG) nicht vorlagen. Unzulässigkeit der Speicherung kann aber auch nachträglich eintreten, z.B. durch Änderung der Sach- oder Rechtslage oder Überschreitung der Speicherdauern (vgl. etwa § 48 IV ASOG i.V.m. der PrüffristenVO).

Nach § 48 II 2 ist die betroffene Person vor der Löschung zu hören, wenn die Speicherung von Anfang an unzulässig war. Dem Betroffenen soll dadurch Gelegenheit gegeben werden, nachteilige Folgen der unzulässigen Speicherung zu erkennen und ggf. im Wege des Rechtsschutzes zu beseitigen.

2. Die Kenntnis der Daten ist nicht mehr erforderlich (Satz 1 Nr. 2)

Maßgeblich für diese Alternative ist die Feststellung, dass die Kenntnis der gespeicherten Daten für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Diese Feststellung kann bei zwei Gelegenheiten getroffen werden: bei der nach bestimmten Fristen vorzunehmenden Überprüfung (vgl. § 48 IV i.V.m. der PrüffristenVO) oder aus Anlass einer Einzelfallbearbeitung, bei der vor Ablauf einer Prüffrist auf die gespeicherten Daten zugegriffen wird. Die Feststellung, ob die weitere Speicherung erforderlich ist, trifft die speichernde Stelle selbst; diese Feststellung liegt nicht in ihrem Ermessen, sondern ist voll gerichtlich überprüfbar.

C. Sperrung von Daten und Vernichtung von Akten (Abs. 3)

Abs. 3 ordnet an, was mit Daten in Akten zu geschehen hat, wenn die Voraussetzungen des Abs. 2 Satz 1 (der ja nur für Daten in Dateien gilt) erfüllt sind.

- Demnach sind im Falle des § 48 III 1 i.V.m. § 48 II 1 Nr. 1 (Unzulässigkeit der Speicherung) die Daten zu sperren.
- im Fall des § 48 III 2 i.V.m. § 48 II 1 Nr. 2 (Daten nicht mehr erforderlich) ist die gesamte Akte zu vernichten, falls auch die gesamte Akte nicht mehr erforderlich ist. Sind nur einzelne Daten nicht mehr erforderlich, andere in der Akte aber nach wie vor, dann darf die Akte schon wegen des Grundsatzes der Aktenvollständigkeit nicht vernichtet werden; vielmehr sind dann nur die nicht mehr erforderlichen Daten (durch Vermerk) zu sperren. Das ist zwar nicht ausdrücklich im Gesetz geregelt, folgt aber daraus, dass eine weitere Speicherung von Daten, die nicht mehr erforderlich sind, unzulässig ist, so dass insoweit auch die Voraussetzungen von § 48 III 1 i.V.m. § 48 II 1 Nr. 1 erfüllt sind.

Sperrung: vgl. § 4 II Nr. 5 BlnDSG: Das Verhindern weiterer Verarbeitung gespeicherter Daten. Dagegen spricht das (hier nicht anzuwendende) BDSG in § 3 IV Nr. 4 vom „Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken“. Das BlnDSG geht also weiter und verlangt, dass (z.B. durch Zugangsbeschränkungen oder Wegschließen eines Datenträgers in einem Tresor) die weitere Datenverarbeitung (vorübergehend) unmöglich gemacht wird.

D. Prüffristen (Abs. 4)

Abs. 4 enthält eine Verordnungsermächtigung, von der der Senat durch Verordnung über die Prüffristen bei polizeilicher Datenverarbeitung (PrüffristenVO) vom 22.2.1993 Gebrauch gemacht hat. In der Verordnung sind Fristen für verschiedene Fälle und Personengruppen genannt, innerhalb derer eine Überprüfung erfolgen muss, ob die weitere Speicherung der entsprechenden Daten noch erforderlich ist. § 48 IV gibt dabei Höchstfristen für die Daten von Kindern, Jugendlichen und Erwachsenen vor; die PrüffristenVO greift diese Unterscheidung auf. Umstritten ist dabei die Bedeutung des Begriffs „Kind“ bzw. „Jugendlicher“. Dazu gibt es weder im ASOG noch in der PrüffristenVO eine Definition. Allerdings kann auf die – im Wesentlichen einheitliche – Definition aus anderen Gesetzen (z.B. § 1 I Nrn. 1, 2 JuSchG) zurückgreifen. Demnach ist Kind eine Person unter 14 Jahre, Jugendlicher eine Person zwischen ab 14 Jahre, aber unter 18, und Erwachsener eine Person ab 18 Jahre. Die Gegenansicht, dass auch Kinder bis 18 Jahre alt sind (so Berg/Knape/Kiworr), ist angesichts der gesetzlichen Regelung, die ja zwischen Kindern und Jugendlichen unterscheiden will, nicht haltbar.

Ergibt die Überprüfung, dass die Daten nicht mehr erforderlich sind, dann sind die Daten zu löschen (§ 48 II 1 Nr. 2) bzw. die Akten zu vernichten (§ 48 III 2 i.V.m. § 48 II 1 Nr. 2).

E. Mitteilung an Übermittlungsempfänger (Abs. 5)

Haben Ordnungsbehörden oder Polizei Daten übermittelt, so sind sie unter bestimmten Voraussetzungen zu besonderen Mitteilungen an den Übermittlungsempfänger verpflichtet.

- Voraussetzung ist die Feststellung, dass unrichtige oder nach § 48 II 1 Nr. 1 zu löschende oder nach § 48 III 1 zu sperrende Daten übermittelt worden sind; der Fall des § 48 II 1 Nr. 2 ist zwar in Abs. 5 nicht erwähnt, aber dennoch auch erfasst, weil die weitere Speicherung von Daten, deren Kenntnis nicht mehr erforderlich ist (§ 48 II 1 Nr. 2), unzulässig ist, so dass dann gleichzeitig ein Fall des § 48 II 1 Nr. 1 vorliegen wird. Unerheblich ist, ob die Voraussetzungen der Löschung oder Sperrung vor der Übermittlung oder danach eingetreten sind.
- Dem Übermittlungsempfänger ist unter dieser Voraussetzung die Berichtigung, Löschung oder Sperrung mitzuteilen.
- Die Mitteilung kann nach Abs. 5 S. 2 unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte bestehen, dass dadurch schutzwürdige Belange der betroffenen Person beeinträchtigt werden können. Dieser Ausnahmefall ist jedoch kaum denkbar, weil die Übermittlung unrichtiger, zu löschender oder zu sperrender Daten fast immer in das Recht auf informationelle Selbstbestimmung und damit in schutzwürdige Belange des Betroffenen eingreift.

F. Ausnahmen von der Löschungs- und Vernichtungspflicht (Abs. 6)

Nach Abs. 6 darf eine Löschung oder Vernichtung in drei Fällen nicht erfolgen:

1. wenn Grund zu der Annahme besteht, dass schutzwürdige Belange der betroffenen Person beeinträchtigt würden,
2. wenn die Daten zur Behebung einer bestehenden Beweisnot unerlässlich sind, oder
3. wenn die Nutzung der Daten zu wissenschaftlichen Zwecken erforderlich ist; in diesem Fall sind die zum frühestmöglichen Zeitpunkt zu anonymisieren.

An die Stelle der Löschung oder Vernichtung tritt dann die Sperrung; die Daten sind mit einem Sperrvermerk zu versehen. Sie dürfen außerdem nur zu genannten Zwecken (Schutz der Belange des Betroffenen, Behebung einer Beweisnot, wissenschaftliche Zwecke) oder (diese Ausnahme gilt immer, der Hinweis in Abs. 6 ist daher nur deklaratorisch) mit Einwilligung der betroffenen Person genutzt werden.

Schutzwürdige Belange i.S. dieser Vorschrift sind durch das Persönlichkeitsrecht geprägt. Beispiel: Schadensersatzansprüche wegen Verletzung des Rechts auf informationelle Selbstbestimmung.

Eine **Beweisnot** (für den Betroffenen oder die Behörde) liegt vor, wenn entscheidungserhebliche Tatsachen nicht anders als durch Vorlage der Daten bewiesen werden können. In Betracht kommen v.a. förmliche gerichtliche oder behördliche Rechtsstreitverfahren.

Anonymisierung: vgl. § 4 III Nr. 7 BlnDSG: 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 bestimmbar natürlichen Person zugeordnet werden können.

G. Abgabe an ein öffentliches Archiv (Abs. 7)

Die Daten, die eigentlich zu löschen oder zu vernichten sind (mit Ausnahme der Daten, deren Speicherung unzulässig ist), können statt dessen auch an ein öffentliches Archiv abgegeben werden, soweit besondere archivrechtliche Regelungen das vorsehen. Solche Regelungen finden sich im Gesetz über die Sicherung und Nutzung von Archivgut des Landes Berlin (Archivgesetz des Landes Berlin (ArchGB) vom 29.11.1993, GVBl. 576.

Kapitel 17: Auskunftsrecht (§ 50 ASOG)

§ 50 regelt den Anspruch des Betroffenen auf Auskunft über seine gespeicherten Daten.

A. Auskunftsanspruch (Abs. 1)

Grundsätzlich hat jeder Betroffene nach § 50 I 1 gegenüber den Ordnungsbehörden und der Polizei Anspruch auf Auskunft über die zu seiner Person bei diesen Behörden jeweils gespeicherten Daten. Die Beschränkung auf die „gespeicherten“ Daten ist deshalb sinnvoll, weil Daten, die zwar verarbeitet worden sind, aber nun nicht mehr gespeichert sind (z.B. weil sie gelöscht wurden) den Behörden i.d.R. nicht mehr zur Verfügung stehen; eine Auskunft über solche Daten ist überhaupt nicht mehr möglich.

Die Auskunft ist gebührenfrei. In dem Antrag soll der Auskunftssuchende die Art der Daten näher bezeichnen, Abs. 1 S. 2 (z.B. durch den Zeitpunkt und den Anlass der Erhebung). Fehlt es an einer solchen näheren Bezeichnung, so besteht dennoch der Auskunftsanspruch; die Behörde muss dann im Rahmen ihrer technischen Möglichkeiten die in Dateien gespeicherten Daten nach solchen Informationen absuchen, die den Auskunftssuchenden betreffen. Bei einem Antrag auf Auskunft aus Akten kann vom Auskunftssuchenden verlangt werden, dass er weitere Angaben macht, so dass die Daten mit einem angemessenen Aufwand gefunden werden können (Abs. 1 S. 3). Kommt der Auskunftssuchende diesem Verlangen nicht nach, so liegt es im pflichtgemäßen Ermessen der Behörde, den Antrag abzulehnen (Abs. 1 S. 4).

Ist inzwischen ein Strafverfahren anhängig, in das die Daten eingeführt sind, so muss vor Erteilung der Auskunft die Zustimmung der Staatsanwaltschaft eingeholt werden (Abs. 5).

Die Erteilung der Auskunft ist nach wohl h.M. als Verwaltungsakt anzusehen, so dass sie vor Gericht mit Hilfe einer Verpflichtungsklage begehrt werden kann.

B. Verweigerung der Auskunft (Abs. 2, 3)

Nach Abs. 2 besteht der Auskunftsanspruch ausnahmsweise nicht, soweit eine Abwägung ergibt, dass die schutzwürdigen Belange des Betroffenen, also seine aus dem Persönlichkeitsrecht fließenden Rechte (insbesondere das Recht auf informationelle Selbstbestimmung) hinter dem öffentlichen Geheimhaltungsinteresse oder dem Geheimhaltungsinteresse eines Dritten (auch eines Privaten und einer juristischen Person des Privatrechts) zurücktreten müssen.

Ein öffentliches Geheimhaltungsinteresse besteht insbesondere dann, wenn die Gefahr der Ausforschung polizeilicher Tätigkeit besteht oder wenn Strafverfolgungsmaßnahmen vereitelt werden könnten. Ein privates Geheimhaltungsinteresse besteht z.B. dann, wenn ein Informant der Polizei vor Racheakten geschützt werden soll. Diese Interessen sind jeweils mit dem Recht des Betroffenen auf informationelle Selbstbestimmung abzuwägen. Es handelt sich dabei um eine gerichtlich voll überprüfbare Entscheidung; die Polizei hat bei dieser Entscheidung (anders als bei der Entscheidung nach Abs. 1 S. 4) kein Ermessen und kann daher keine Zweckmäßigkeitserwägungen anstellen.

Die Auskunft kann nur verweigert werden, „soweit“ die Interessen des Betroffenen zurücktreten müssen. Das bedeutet, dass die Auskunft nur bezüglich derjenigen Daten verweigert werden kann, deren Bekanntgabe an den Betroffenen die genannten Geheimhaltungsinteressen zu sehr beeinträchtigen würde. Im Übrigen bleibt der Auskunftsanspruch bestehen.

Eine Entscheidung, durch die die Auskunft gem. Abs. 2 abgelehnt wird, stellt i.d.R. einen schriftlichen Verwaltungsakt dar und ist daher gem. § 39 I VwVfG zu begründen. Dabei sind

die wesentlichen tatsächlichen und rechtlichen Gründe mitzuteilen (§ 39 I 2 VwVfG). Einer solchen Begründung bedarf es allerdings gem. der Spezialregelung des § 50 III ASOG insofern nicht, als durch diese Begründung der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Beispiel: Ist ein Informant der Polizei zu schützen, so würde möglicherweise schon die Bekanntgabe des Verweigerungsgrundes (nämlich dass ein Informant zu schützen ist) den Betroffenen davon in Kenntnis setzen, dass jemand ihn „verraten“ hat; schon dadurch könnte der Informant in Gefahr geraten.

C. Hinweis auf Anrufung des Datenschutzbeauftragten (Abs. 4)

Wird die Auskunft gem. Abs. 2 nicht gewährt (nicht aber bei einer Auskunftsverweigerung nach Abs. 1 S. 4), so ist der Auskunftssuchende auf die Möglichkeit hinzuweisen, sich an den Berliner Datenschutzbeauftragten zu wenden. Dem Datenschutzbeauftragten wiederum müssen die Gründe der Auskunftsverweigerung mitgeteilt werden; dieser darf sie aber ohne Zustimmung der speichernden Stelle nicht an den Betroffenen weitergeben, wenn daraus auf den Erkenntnisstand der speichernden Stelle geschlossen werden kann.

D. Akteneinsicht (Abs. 6)

Sind die Daten in Akten gespeichert, so kann gem. Abs. 6 statt der Auskunft auch Akteneinsicht gewährt werden. Bei der auch hier stattfindenden Abwägung gem. Abs. 2 muss berücksichtigt werden, dass die Gefahr der Verletzung von Geheimhaltungsinteressen Dritter besonders groß ist, wenn der Auskunftssuchende die gesamte Akte zu sehen bekommt. Daher wird i.d.R. die Auskunft über den Akteninhalt vorzugswürdig (wenn auch aufwändiger) sein.

E. Bezüge zu anderen Vorschriften

- §§ 147, 385 III, 397 I, 406e, 433, 475 ff., 491 StPO: Akteneinsicht bei Kriminalakten. Diese Vorschriften der StPO haben Vorrang gegenüber § 50 ASOG. Insbesondere zu beachten § 147 StPO: Akteneinsicht nur durch den Verteidiger, nicht durch den Beschuldigten; dem Beschuldigten werden nur Auskünfte und Abschriften erteilt.
- § 29 VwVfG: Akteneinsicht durch Beteiligte am Verwaltungsverfahren. Diese Vorschrift tritt zurück gegenüber dem spezielleren § 50 ASOG.