Fachbereich WD 3

Rechtliche Voraussetzungen und Grenzen des behördlichen Ankaufs von personenbezogenen Daten aus Werbedatenbanken

Rechtliche Voraussetzungen und Grenzen des behördlichen Ankaufs von personenbezogenen Daten aus Werbedatenbanken

Aktenzeichen:	WD 3 - 3000 - 065/25
Abschluss der Arbeit:	27. November 2025
Fachbereich:	WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Einleitung

Diese Ausarbeitung untersucht die rechtlichen Voraussetzungen und Grenzen des **Ankaufs personenbezogener Daten aus kommerziellen Werbedatenbanken durch deutsche Behörden**. Im Anschluss an eine einleitende Darstellung des Datenhandels wird zunächst auf den insoweit für die **Nachrichtendienste des Bundes** geltenden Rechtsrahmen eingegangen (siehe 2.). Sodann wird auf die maßgeblichen Regelungen im Bereich der **Verfolgung und Verhütung von Straftaten** sowie der **Gefahrenabwehr** eingegangen (siehe 3.). Abschließend werden die Bedingungen skizziert, unter denen **andere Behörden** Daten aus kommerziellen Datenbanken ankaufen können (siehe 4.).

Der Ankauf personenbezogener Daten aus kommerziellen Werbedatenbanken durch staatliche Stellen hat in den vergangenen Jahren zunehmend Beachtung gefunden. Ursprünglich beschränkte sich der Handel mit solchen Datensätzen auf die Privatwirtschaft, insbesondere auf Werbe- und Analyseunternehmen, die große Mengen an Verbraucherinformationen erfassen und auswerten. Zu den aggregierten Daten gehören **Informationen aus Kundenbindungsprogrammen, sozialen Netzwerken, App-Nutzungsstatistiken, Geolokalisierungsdiensten sowie öffentlichen Registern**.[1] Solche Datensammlungen enthalten häufig **personenbezogene Angaben** zu **Wohnsitz, Alter, Geschlecht, Konsumverhalten, Interessen, der sexuellen Orientierung, politischen Ansichten, Religionszugehörigkeit, Kommunikationskanälen oder Bewegungsprofilen** und werden in standardisierten Formaten angeboten.[2]

Zur tatsächlichen **Häufigkeit** und zum **Umfang** der Ankäufe solcher Daten durch **deutsche staatliche Stellen** liegen bislang **keine gesicherten Informationen** vor.[3] Gleichwohl gibt es Indizien, die nahelegen, dass die Praxis kein Ausnahmephänomen darstellt, sondern zunehmend Teil des behördlichen Informationsmanagements wird. So wird in der **Begründung des Gesetzentwurfs zur BND-Novelle** aus dem Jahr 2023 explizit auf die Nutzung und den Erwerb von Daten aus Werbedatenbanken durch den Bundesnachrichtendienst verwiesen.[4] **Konkrete Beispiele** für den Ankauf personenbezogener Daten aus kommerziellen Datenbanken betreffen vor allem **US-Behörden** wie die Defense Intelligence Agency (DIA) und die National Security Agency (NSA) sowie den **militärischen Nachrichtendienst Norwegens** und die **niederländischen Nachrichtendienste**.[5]

Diese Ausarbeitung untersucht nur die rechtlichen Voraussetzungen und Grenzen eines Datenkaufs durch deutsche Behörden und somit ausschließlich den Verarbeitungsschritt der

---

1 Vgl. Brunner/Ciesielski/Wurscher/Zierer, Datenhandel außer Kontrolle, tagesschau.de vom 15.01.2025.

2 Ruckerbauer/Wetzling, Informationsbeschaffung mit der Kreditkarte – Wie nachrichtendienstliche Datenkäufe verfassungsrechtliche Mindeststandards unterlaufen, 01.05.2024, Punkt 2.2.

3 Sosna, „Fundgrube Internet“ – vom tatsächlich möglichen und rechtlich zulässigen Sammeln der Nachrichtendienste im Netz, GSZ 2024, 53 (53 f.).

4 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Änderung des BND-Gesetzes, BT-Drs. 20/8627 vom 02.10.2023, S. 43.

5 Ruckerbauer/Wetzling, Informationsbeschaffung mit der Kreditkarte – Wie nachrichtendienstliche Datenkäufe verfassungsrechtliche Mindeststandards unterlaufen, 01.05.2024, Punkt 2.4.

Datenerhebung, nicht die anschließende Verwendung in Gestalt der Speicherung, Auswertung und weiteren Verknüpfung.

2. Datenankauf durch Nachrichtendienste des Bundes

Um die rechtlichen Voraussetzungen und Grenzen eines Datenankaufs durch die Nachrichtendienste des Bundes, also das **Bundesamt für Verfassungsschutz (BfV), den Bundesnachrichtendienst (BND) und den Militärischen Abschirmdienst (MAD)**, bewerten zu können, muss zunächst der einschlägige Prüfungsrahmen ermittelt werden.

2.1. Prüfungsmaßstab

Die Zulässigkeit der Verarbeitung personenbezogener Daten richtet sich grundsätzlich nach der unionsrechtlichen **Datenschutz-Grundverordnung (DS-GVO)**[6]. Die Verordnung gilt gemäß Art. 2 Abs. 1 DS-GVO für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Für die Tätigkeit der Nachrichtendienste greift jedoch eine **Bereichsausnahme**. Gemäß **Art. 2 Abs. 2 Buchst. a DS-GVO** findet die Verordnung **keine Anwendung** auf die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen. Zu diesen Tätigkeiten gehört unter anderem der **Schutz der nationalen Sicherheit**, der gemäß Art. 4 Abs. 2 Satz 3 des Vertrages über die Europäische Union (EUV)[7] in der alleinigen Verantwortung der Mitgliedstaaten und somit außerhalb des Anwendungsbereichs des Unionsrechts liegt. Auch Erwägungsgrund 16 zur DS-GVO stellt klar, dass die Verordnung auf Tätigkeiten, die die nationale Sicherheit betreffen, nicht anzuwenden ist. Dieser Ausnahme unterfällt auch die Arbeit der Nachrichtendienste, so dass die DS-GVO für die Verarbeitung personenbezogener Daten durch diese Behörden nicht gilt.[8] Nachrichtendienstliche Maßnahmen sind daher am **Grundgesetz (GG)**[9] und den einschlägigen **Fachgesetzen** zu messen.

2.2. Schutzbereich

Der Ankauf von personenbezogenen Daten aus Werbedatenbanken durch Nachrichtendienste kann je nach Art der betroffenen Daten unterschiedliche Grundrechtspositionen tangieren. In

---

6 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DS-GVO), ABl. L 119 vom 04.05.2016, S. 1-88.

7 Vertrag über die Europäische Union (EU-Vertrag – EUV), konsolidierte Fassung, ABl. EG Nr. C 115 vom 09.05.2008, S. 13, zuletzt geändert durch die Akte über die Bedingungen des Beitritts der Republik Kroatien und die Anpassungen des Vertrags über die Europäische Union, des Vertrags über die Arbeitsweise der Europäischen Union und des Vertrags zur Gründung der Europäischen Atomgemeinschaft, ABl. EU L 112/21 vom 24.04.2012 m.W.v. 01.07.2013.

8 BVerwG, Urteil vom 18.09.2019 - 6 A 7/18 (= NVwZ 2020, 305 (Rn. 43)).

9 Grundgesetz für die Bundesrepublik Deutschland (GG) in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 1 des Gesetzes vom 22.05.2025 (BGBl. 2025 I Nr. 94).

Betracht kommen zum einen das **Telekommunikationsgeheimnis aus Art. 10 Abs. 1 GG**, zum anderen das **Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG**.

2.2.1. Telekommunikationsgeheimnis, Art. 10 Abs. 1 GG

Das Telekommunikationsgeheimnis schützt die **unkörperliche Übermittlung von Informationen mit Hilfe des Telekommunikationsverkehrs** vor einer **Kenntnisnahme** durch die **öffentliche Gewalt**.[10] Dies gilt allerdings nicht für Übermittlungen an die Öffentlichkeit, sondern ausschließlich für **Übermittlungen an individuelle Empfänger**.[11] Die Veröffentlichung von an jedermann adressierten Inhalten im Internet (z.B. auf einer nicht zugangsgesicherten Webseite oder einem allgemein zugänglichen Profil in einem sozialen Netzwerk) erfährt daher keinen Schutz durch Art. 10 Abs. 1 GG.[12] Entscheidend für die Eröffnung des Schutzbereichs ist vielmehr die **individuelle Adressierung** der Kommunikation.[13] Dabei reicht die Beteiligung *eines* menschlichen Kommunikationspartners, wie etwa im Fall des empfängergesteuerten Abrufs von Webseiten, aus.[14] Neben den **Inhalten der Kommunikation** erfasst der Schutzbereich auch die **näheren Umstände des Kommunikationsvorgangs**, also ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist.[15] Diese Angaben unterfallen ebenso wie alle weiteren **Verkehrsdaten**, die Aufschluss über die an einer Kommunikation beteiligten Personen und die Umstände der Kommunikation geben, dem Schutzbereich von Art. 10 Abs. 1 GG.[16] Erfasst sind auch die personenbezogenen Daten, die beim **Surfen im Internet**, also dem individuell verantworteten Aufruf von Webseiten, von den nutzenden Personen übermittelt werden, beispielsweise ihre (dynamische) IP-Adresse.[17]

Kaufen Nachrichtendienste Daten dieser Art an, so ist folglich der Schutzbereich von Art. 10 Abs. 1 GG eröffnet. Dabei **geht** das **Telekommunikationsgeheimnis anderen Datenschutzgrundrechten vor**, so dass auf diese nur dann zurückgegriffen werden kann, soweit Art. 10 Abs. 1 GG nicht einschlägig ist.[18]

---

10 BVerfG, Beschluss vom 24.01.2012 - 1 BvR 1299/05 (= BVerfGE 130, 151 (179)).

11 BVerfG, a.a.O.

12 Schenke, in: Stern/Becker, Grundrechte-Kommentar, 4. Aufl. 2024, Art. 10 Rn. 43.

13 Jarass, in: Jarass/Pieroth, GG, 18. Aufl. 2024, Art. 10 Rn. 6.

14 BVerfG, Beschluss vom 06.07.2016 - 2 BvR 1454/13 (= NJW 2016, 3508 (Rn. 38)).

15 BVerfG, a.a.O.

16 Durner, in: Dürig/Herzog/Scholz, GG, Werkstand: 107. EL März 2025, Art 10 Rn. 112, m.w.N.

17 BVerfG, Beschluss vom 06.07.2016 - 2 BvR 1454/13 (= BVerfG, ZD 2017, 132 (Rn. 38)); Wischmeyer, in: Dreier, GG, 4. Aufl. 2023, Art. 10 Rn. 65.

18 BVerfG, Urteil vom 02.03.2010 - 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 (= BVerfGE 125, 260 (310)); BVerfG, Beschluss vom 13.06.2007 - 1 BvR 1550/03, 1 BvR 2357/04, 1 BvR 603/05 (= BVerfGE 118, 168 (184)); BVerfG, Urteil vom 02.03.2006 - 2 BvR 2099/04 (= BVerfGE 115, 166 (189)).

2.2.2. Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG)

Das von der Rechtsprechung als Ausprägung des allgemeinen Persönlichkeitsrechts aus **Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG** anerkannte **Recht auf informationelle Selbstbestimmung** verleiht dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.[19] Das Grundrecht schützt also vor dem staatlichen Zugriff **auf jegliche Angaben über die persönlichen und sachlichen Verhältnisse einer Person**.[20] Die Eröffnung des Schutzbereichs ist dabei unabhängig von der Sensibilität der Daten für die Persönlichkeit der Betroffenen und wird auch nicht dadurch ausgeschlossen, dass die Daten bereits öffentlich zugänglich sind.[21] Kaufen Nachrichtendienste demnach personenbezogene Daten an, die nicht bereits durch Art. 10 Abs. 1 GG geschützt sind, ist das Grundrecht auf informationelle Selbstbestimmung einschlägig.

2.3. Eingriff

Der Ankauf personenbezogener Daten aus Werbedatenbanken dürfte auch einen Eingriff in die jeweils betroffenen Grundrechte darstellen.

2.3.1. Telekommunikationsgeheimnis, Art. 10 Abs. 1 GG

Ein Eingriff in das Telekommunikationsgeheimnis ist grundsätzlich **jede Kenntnisnahme, Aufzeichnung und Verwertung der geschützten kommunikativen Daten** durch eine staatliche Stelle.[22] Folglich stellen die behördliche **Erfassung** von Telekommunikationsdaten, ihre **Speicherung**, ihr **Abgleich** mit anderen Daten, ihre **Auswertung**, ihre **Selektierung** zur weiteren Verwendung und ihre **Übermittlung an Dritte** jeweils eigene Eingriffe in das Telekommunikationsgeheimnis dar.[23] Werden umgekehrt **Dritte** durch eine Behörde **zur Herausgabe** von durch Art. 10 Abs. 1 GG geschützten Daten **verpflichtet**, wie beispielsweise im Fall der Beschlagnahme von Verkehrsdaten, so stellt bereits diese Verpflichtung einen Eingriff in das Telekommunikationsgeheimnis dar.[24]

Andererseits ist ein **Eingriff** in Art. 10 Abs. 1 GG zu **verneinen**, wenn eine staatliche Stelle auf dem **technisch vorgesehenen Weg** einen **Kommunikationsvorgang erfasst** und **mindestens eine** der an der Kommunikation **beteiligten Personen** der staatlichen Stelle den Zugriff **freiwillig**

---

19 Eichberger, in: Huber/Voßkuhle, GG, 8. Aufl. 2024, Art. 2 Rn 274.

20 Eichberger, in: Huber/Voßkuhle, GG, 8. Aufl. 2024, Art. 2 Rn 284.

21 Eichberger, in: Huber/Voßkuhle, GG, 8. Aufl. 2024, Art. 2 Rn 285.

22 Ogorek, in: Epping/Hillgruber, GG, 63. Edition Stand 15.09.2025, Art. 10 Rn. 50 (m.w.N.).

23 BVerfG, Urteil vom 14.07.1999 - 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 (= BVerfGE 100, 313 (366)).

24 BVerfG, Beschluss vom 15.08.2014 - 2 BvR 969/14 (= NJW 2014, 3085, Rn. 46)); BVerfG, Urteil vom 02.03.2010 - 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 (= BVerfGE 125, 260 (310)).

ermöglicht hat.[25] Ein Eingriff in das Telekommunikationsgeheimnis scheidet ferner aus, wenn eine Behörde **allgemein zugängliche Inhalte** erhebt, etwa indem sie offene Diskussionsforen oder nicht zugangsgesicherte Webseiten einsieht.[26]

Ob eine **Erhebung im Wege des Ankaufs** personenbezogener (Kommunikations-)Daten aus Werbedatenbanken als **Eingriff** in die Telekommunikationsfreiheit zu werten ist, hat die **Rechtsprechung bislang nicht entschieden**. Die **Eingriffsqualität** könnte in Anbetracht der vorstehend dargelegten Kriterien mit dem Argument **bezweifelt** werden, dass der Datenkauf grundsätzlich für jedermann möglich ist und die **Datenbanken** insoweit **allgemein zugänglich** sind. Bei einem Ankauf **ermöglicht** der **Datenbroker** dem Käufer den **Zugriff** auf die Daten zudem **freiwillig**. Diese Betrachtungsweise berücksichtigt jedoch nicht den Umstand, dass die in kommerziellen Datenbanken gespeicherten Daten – wie in der Einleitung dargelegt – aus **zahlreichen unterschiedlichen Quellen**, von denen viele gerade **nicht allgemein zugänglich** sind, stammen (z.B. Kundenbindungsprogramme, Geolokalisierungsdienste, Apps oder Social Media). Zudem werden diese Daten in den Datenbanken **systematisch zu Profilen zusammengeführt**. Der Zugriff auf diese Daten ist daher **nicht vergleichbar** mit der Beobachtung eines **offenen Diskussionsforums** oder dem Besuch einer **nicht zugangsgesicherten Webseite**. Darüber hinaus macht es aus Sicht der Betroffenen **keinen Unterschied**, ob Dritte von Art. 10 Abs. 1 GG geschützte Daten aufgrund einer **Herausgabeanordnung** oder aufgrund eines **Kaufvertrages** an die Nachrichtendienste übermitteln, da die Vertraulichkeit des Kommunikationsvorgänge, denen die Daten entstammen, in beiden Fällen in gleicher Weise kompromittiert werden. Dass die **Betreiber** von Werbedatenbanken die Daten **freiwillig** verkaufen und herausgeben, spricht im Übrigen auch deshalb nicht gegen die Eingriffsqualität des Ankaufs, da sie **selbst nicht Beteiligte** des Kommunikationsvorgangs waren, dem die gehandelten Daten entstammen.

2.3.2. Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG

Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt grundsätzlich bei **jeder staatlichen Erhebung, Sammlung, Speicherung, Verwendung und Weitergabe personenbezogener Daten** vor.[27] Insbesondere dann, wenn die Entfaltung der Persönlichkeit dadurch gefährdet wird, dass personenbezogene Informationen von Behörden in einer Art und Weise genutzt und verknüpft werden, die Betroffene **weder überschauen noch beherrschen** können, wird der Schutzbereich des Grundrechts verkürzt.[28]

Demgegenüber ist ein Eingriff zu **verneinen**, wenn eine staatliche Stelle im Internet verfügbare **Kommunikationsinhalte** erhebt, die sich an **jedermann** oder zumindest an einen **nicht weiter abgegrenzten Personenkreis** richten, so beispielsweise dann, wenn die Behörde eine **allgemein**

---

25 BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07 (= NJW 2008, 822 (835)); a.A. noch BVerfG, Beschluss vom 25.04.1992 - 1 BvR 1430/88 (= BVerfGE 85, 386 (399)); ebenso Wischmeyer, in: Dreier, GG, 4. Aufl. 2023, Art. 10 Rn. 92 (m.w.N.).

26 BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07 (= NJW 2008, 822 (835)).

27 Eichberger, in: Huber/Voßkuhle, GG, 8. Aufl. 2024, Art. 2 Rn. 289; Jarass, in: Jarass/Pieroth, GG, 18. Aufl. 2024, Art. 2 Rn. 59.

28 BVerfG, Beschluss vom 10.11.2020 - 1 BvR 3214/15 (= BVerfGE 156, 11 (Rn. 71)).

zugängliche Webseite aufruft, eine jedem Interessierten offenstehende **Mailingliste** abonniert oder einen **offenen Chat** beobachtet.[29] Ein **Eingriff** ist jedoch **anzunehmen**, wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, **gezielt zusammengetragen, gespeichert** und gegebenenfalls unter Hinzuziehung weiterer Daten **ausgewertet** werden und sich daraus eine **besondere Gefahrenlage für die Persönlichkeit** der Betroffenen ergibt.[30]

Auch im Hinblick auf das Recht auf informationelle Selbstbestimmung hat die Rechtsprechung bislang nicht entschieden, ob der behördliche Ankauf von Daten aus Werbedatenbanken als Eingriff zu werten ist, jedoch sprechen die soeben dargelegten Kriterien dafür, einen Eingriff anzunehmen. Der Ankauf personenbezogener Daten aus Werbedatenbanken steht zwar grundsätzlich jedem Interessierten offen, jedoch liegt der besondere Wert der dort verfügbaren Daten aus Sicht der Nachrichtendienste gerade in dem Umstand, dass die Daten aus vielen verschiedenen Quellen aggregiert wurden und deshalb besonders umfangreiche Informationen über die Betroffenen enthalten. Betroffene können in aller Regel weder überschauen noch beherrschen, welche Daten aus welchen Quellen in Werbedatenbanken gespeichert und miteinander verknüpft werden. Die spezifische Gefahrenlage für die Persönlichkeit Betroffener ist beim behördlichen Ankauf solcher Daten somit im Wesentlichen vergleichbar mit einer Konstellation, in der die Behörde die einzelnen Daten selbst sammelt und zusammenführt.

2.4. Verfassungsrechtliche Rechtfertigung

Die mit dem Ankauf von personenbezogenen Daten aus Werbedatenbanken verbundenen Grundrechtseingriffe sind verfassungsrechtlich gerechtfertigt, wenn die Grundrechte Schranken unterliegen, die in verfassungsgemäßer Weise konkretisiert werden, die Konkretisierung den Datenankauf abdeckt und ihre Anwendung im Einzelfall verfassungskonform ist.

2.4.1. Grundrechtsschranken

Das **Telekommunikationsgeheimnis** aus Art. 10 Abs. 1 GG unterliegt gemäß Art. 10 Abs. 2 Satz 1 GG einem **einfachen Gesetzesvorbehalt**, so dass es durch ein **Parlamentsgesetz** oder durch eine **Rechtsverordnung oder Satzung**, die auf einem solchen Gesetz beruhen, eingeschränkt werden kann.[31]

Für die Rechtfertigung von Eingriffen in das **Recht auf informationelle Selbstbestimmung** aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG gilt die sog. **Schrankentrias** in Art. 2 Abs. 1 GG.[32] Danach findet das Grundrecht seine Grenze in den **Rechten anderer**, der **verfassungsmäßigen Ordnung** und dem **Sittengesetz**. Die Schrankentrias kommt im Ergebnis einem **einfachen Gesetzesvorbehalt** gleich, da das Grundrecht durch ein **Parlamentsgesetz** oder aufgrund einer formell-

29 BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07 (= NJW 2008, 822 (836)).

30 BVerfG, a.a.O.

31 Gusy, in: Huber/Voßkuhle, GG, 8. Aufl. 2024, Art. 10 Rn. 68.

32 Jarass, in: Jarass/Pieroth, GG, 18. Aufl. 2024, Art. 2 Rn. 65.

gesetzlichen Ermächtigung auch durch eine **Rechtsverordnung oder Satzung** eingeschränkt werden kann.[33]

Demnach bedarf es für Eingriffe in beide Grundrechte einer **einfachgesetzlichen Ermächtigungsgrundlage**.

2.4.2. Schrankenkonkretisierung

Als Konkretisierung der grundrechtlichen Vorbehalte muss eine gesetzliche Vorschrift vorliegen, die den Ankauf personenbezogener Daten durch die Nachrichtendienste abdeckt.

2.4.2.1. Übermittlungsvorschriften im Recht der Nachrichtendienste

Als Ermächtigungsgrundlagen kommen zunächst verschiedene, im Wesentlichen gleichlautende gesetzliche Vorschriften über die **Übermittlung bestimmter Informationen durch die Nachrichtendienste** in Betracht. So darf der **BND** gemäß **§ 10a Abs. 1 des Gesetzes über den Bundesnachrichtendienst (BNDG)**[34] personenbezogene Daten, die er aus allgemein zugänglichen Quellen **erhoben** hat, einer anderen Stelle übermitteln, wenn dies zur Erfüllung seiner Aufgaben oder zur Erfüllung der Aufgaben der empfangenden Stelle erforderlich ist. Dies gilt gemäß § 10a Abs. 2 Satz 1 BNDG nicht für personenbezogene Daten, die aus allgemein zugänglichen Quellen systematisch erhoben oder zusammengeführt wurden. In diesen Fällen richtet sich die Übermittlung gemäß § 10a Abs. 2 Satz 2 BNDG nach spezielleren Vorschriften. **§ 25d Bundesverfassungsschutzgesetz (BVerfSchG)**[35] enthält eine gleichlautende Regelung für das **BfV**. Diese gesetzliche Bestimmung gilt gemäß **§ 11 Satz 1 des Gesetzes über den Militärischen Abschirmdienst (MADG)**[36] für die Tätigkeit des **MAD** entsprechend.

In der Begründung des Gesetzentwurfs zu § 10a BNDG wird der Ankauf personenbezogener Daten aus kommerziellen Datenbanken ausdrücklich als Datenerhebung aus allgemein zugänglichen Quellen eingeordnet.[37] Gleichwohl dürfte die Vorschrift, so wie auch die parallelen Regelungen für das BfV und den MAD, keine taugliche Ermächtigungsgrundlage für den Ankauf personenbezogener Daten darstellen, da sie dem BND ihrem Wortlaut nach **lediglich die Befugnis zur Übermittlung** zuvor erhobener personenbezogener Daten an andere Stellen einräumt, nicht aber die Befugnis, die Daten selbst – etwa durch Ankauf – zu erheben.

---

33 Jarass, in: Jarass/Pieroth, GG, 18. Aufl. 2024, Art. 2 Rn. 16.

34 BND-Gesetz (BNDG) vom 20.12.1990 (BGBl. I S. 2954, 2979), zuletzt geändert durch Artikel 4 des Gesetzes vom 06.05.2024 (BGBl. 2024 I Nr. 149).

35 Bundesverfassungsschutzgesetz (BVerfSchG) vom 20.12.1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Artikel 1 des Gesetzes vom 25.10.2024 (BGBl. 2024 I Nr. 332).

36 MAD-Gesetz (MADG) vom 20.12.1990 (BGBl. I S. 2954, 2977), zuletzt geändert durch Artikel 3 des Gesetzes vom 06.05.2024 (BGBl. 2024 I Nr. 149).

37 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Änderung des BND-Gesetzes, BT-Drs. 20/8627 vom 02.10.2023, S. 42 f.

2.4.2.2. Überwachung der Telekommunikation, § 1 Abs. 1 Nr. 1 Artikel 10-Gesetz (G10)[38]

Als Ermächtigungsgrundlage für den Ankauf personenbezogener Daten, die dem Schutzbereich von Art. 10 Abs. 1 GG unterfallen, kommt ferner **§ 1 Abs. 1 Nr. 1 G10** in Betracht. Danach sind BfV, BND und MAD zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages berechtigt, die Telekommunikation zu überwachen und aufzuzeichnen. Mit „überwachen" ist das Mithören der Kommunikation des Betroffenen in Echtzeit gemeint, mit „aufzeichnen" das Speichern zuvor erfasster Kommunikation.[39]

§ 1 Abs. 1 Nr. 1 G10 könnte dann eine taugliche Ermächtigungsgrundlage für den Ankauf personenbezogener (Telekommunikations-)Daten darstellen, wenn der **Ankauf als wesensgleiches Minus zum Überwachen** verstanden werden könnte. Dies wäre der Fall, wenn durch den Ankauf im Vergleich zur nachrichtendienstlichen Überwachung keine spezifischen oder weitergehenden Gefahren für das Telekommunikationsgeheimnis entstehen könnten. Führen die Nachrichtendienste selbst eine Überwachung i.S.d. § 1 Abs. 1 Nr. 1 G10 durch, so müssen sie dabei die den §§ 3 ff. G10 geregelten materiellen Voraussetzungen und Vorgaben beachten und die vorgeschriebenen Verfahrensschritte gem. §§ 9 ff. G10 einhalten. Zudem unterliegt die nachrichtendienstliche Überwachung der Kontrolle durch das Parlamentarische Kontrollgremium (vgl. §§ 14 ff. G10). Diese Vorschriften gelten dagegen nicht für die Betreiber kommerzieller Datenbanken. Unter welchen Umständen und mit welchen Methoden die Daten erhoben und in die Datenbank eingepflegt wurden, ist daher völlig offen und für den ankaufenden Nachrichtendienst auch kaum mit hinreichender Sicherheit überprüfbar. Es erscheint daher möglich, dass Nachrichtendienste durch den Ankauf an Daten gelangen könnten, die sie im Wege einer Überwachung nicht selbst erheben dürften. Der Ankauf personenbezogener Telekommunikationsdaten birgt daher im Vergleich zu einer behördlichen Überwachung ein spezifisches Gefährdungspotenzial für das Telekommunikationsgeheimnis und kann daher nicht als wesensgleiches Minus aufgefasst werden. § 1 Abs. 1 Nr. 1 G10 scheidet daher als Ermächtigungsgrundlage für den Datenankauf aus.

2.4.2.3. Anwendung nachrichtendienstlicher Mittel, §§ 8 Abs. 2, 9 Abs. 1 BVerfSchG

Als Ermächtigungsgrundlage für den Ankauf von personenbezogenen Daten könnten jedoch die Befugnisse zur Anwendung nachrichtendienstlicher Mittel dienen. Das BfV darf gemäß **§§ 8 Abs. 2, 9 BVerfSchG** unter bestimmten Voraussetzungen Methoden, Gegenstände und Instrumente zur **heimlichen Informationsbeschaffung** anwenden. Eine entsprechende Befugnis zur Informationsbeschaffung mit nachrichtendienstlichen Mitteln steht gemäß **§ 5 BNDG** auch dem BND und gemäß **§ 4 Abs. 1, 5 MADG** auch dem MAD zu.

Der Ankauf personenbezogener Daten müsste also als Methode zur heimlichen Informationsbeschaffung zu qualifizieren sein. **Heimliche Maßnahmen** sind dadurch gekennzeichnet, dass sie

---

38 Artikel 10-Gesetz (G10) vom 26.06.2001 (BGBl. I S. 1254, 2298; 2017 I S. 154), zuletzt geändert durch Artikel 4 des Gesetzes vom 22.12.2023 (BGBl. 2023 I Nr. 413).

39 Roggan, in: Roggan, G10, 2. Online-Aufl. 2018, § 1 Rn. 19.

insbesondere vom Betroffenen nicht bemerkt werden.[40] Dies dürfte bei Datenkäufen durch Nachrichtendienste regelmäßig der Fall sein. Die Aufzählung **nachrichtendienstlicher Mittel** in § 8 Abs. 2 BVerfSchG wie u.a. Observation oder Tarnpapiere ist nur **beispielhaft** und nicht abschließend aufzufassen[41], so dass die fehlende Nennung des Ankaufs personenbezogener Daten nicht zum Ausschluss der §§ 8 Abs. 2, 9 BVerfSchG als Ermächtigungsgrundlage führt. **Nachrichtendienstliche Mittel** unterscheiden sich von den allgemeinen Befugnissen zur Erhebung von Informationen (vgl. § 8 Abs. 1 BVerfSchG, § 2 Abs. 1 BNDG) durch ihre **höhere Eingriffsintensität**.[42] Dies verdeutlicht auch § 9 Abs. 1 Satz 2 BVerfSchG, der den Rückgriff auf nachrichtendienstliche Mittel verbietet, wenn die Erforschung des Sachverhalts durch für die Betroffenen weniger beeinträchtigende Maßnahmen wie das Erheben der Information aus allgemein zugänglichen Quellen möglich ist. Wie oben unter Punkt 2.3.2. dargestellt, wertet die Rechtsprechung den **Rückgriff auf allgemein zugängliche Quellen** im Internet grundsätzlich nicht als Eingriff in das Recht auf informationelle Selbstbestimmung. Werden jedoch Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, **gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet**, so entsteht eine **besondere Gefahrenlage** für die Persönlichkeit der Betroffenen, durch die die Eingriffsschwelle überschritten wird. Zwar steht der Ankauf von Daten aus kommerziellen Werbedatenbanken grundsätzlich jedermann offen und ist insofern allgemein zugänglich; der Umstand, dass dort eine Vielzahl von Daten über natürliche Personen aus einer Vielzahl von Quellen systematisch zusammengeführt und zu Profilen verknüpft werden, verleiht dem nachrichtendienstlichen Zugriff auf diese Datenbestände aus Sicht der Betroffenen jedoch besonderes Gewicht.

Es ist daher **grundsätzlich denkbar**, dass nachrichtendienstliche Mittel zur heimlichen Informationsbeschaffung i.S.d. **§§ 8 Abs. 2, 9 Abs. 1 BVerfSchG, § 5 BNDG, §§ 4 Abs. 1, 5 MADG** auch den **Datenankauf** umfassen. Als **gesetzliche Ermächtigungsgrundlagen** für einen Datenkauf könnten diese Befugnisnormen jedoch nur dann herangezogen werden, wenn sie **in dieser Lesart** auch verfassungsmäßig wären.

2.4.3. Verfassungsmäßigkeit der Schrankenkonkretisierung

§§ 8 Abs. 2, 9 Abs. 1 BVerfSchG, § 5 BNDG, §§ 4 Abs. 1, 5 MADG müssten als Ermächtigungsgrundlagen für einen Datenkauf also **formell und materiell verfassungsgemäß** sein.

2.4.3.1. Formelle Verfassungsmäßigkeit

An der **formellen Verfassungsmäßigkeit** von §§ 8 Abs. 2, 9 Abs. 1 BVerfSchG, § 5 BNDG, §§ 4 Abs. 1, 5 MADG bestehen keine Zweifel. Dem Bund stehen ausschließliche Gesetzgebungskompetenzen für das BVerfSchG (Art. 71, 73 Abs. 1 Nr. 10 GG) sowie für das BNDG und das MADG (Art. 71, 73 Abs. 1 Nr. 1 GG (auswärtige Angelegenheiten und Verteidigung)) zu.

---

40 Gusy, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 5 BNDG Rn. 8.

41 Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 8 BVerfSchG Rn. 24.

42 Gusy, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 5 BNDG Rn. 13.

2.4.3.2. Materielle Verfassungsmäßigkeit

Die gesetzlichen Regelungen müssen überdies den Anforderungen an die **materielle Verfassungsmäßigkeit** genügen.

2.4.3.2.1. Zitiergebot

Dem **Zitiergebot aus Art. 19 Abs. 2 Satz 2 GG**, wonach ein Gesetz, das ein Grundrecht einschränkt, das Grundrecht unter Angabe des Artikels nennen muss, tragen § 22 BVerfSchG, § 68 BNDG und § 16 MADG Rechnung, indem sie darauf hinweisen, dass die jeweiligen Gesetze jeweils das Grundrecht aus Art. 10 Abs. 1 GG einschränken. Zwar wird eine Einschränkung des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG dort nicht genannt, dies ist jedoch unschädlich, da das Zitiergebot für dieses Grundrecht nicht gilt.[43]

2.4.3.2.2. Bestimmtheitsgebot

Die gesetzlichen Ermächtigungsgrundlagen müssen zudem die Anforderungen des **Bestimmtheitsgebots** erfüllen. Einschränkende Gesetze müssen die Voraussetzungen und den Umfang der Einschränkungen **hinreichend bereichsspezifisch, präzise und normenklar** umschreiben, wobei sich der Umfang nach Art und Schwere des Grundrechtseingriffs richtet.[44] Bei Eingriffen in das Recht auf informationelle Selbstbestimmung verlangt das Bestimmtheitsgebot, dass sowohl der **Anlass** der Maßnahme als auch der **Verwendungszweck** der betroffenen Informationen klar **umgrenzt** werden.[45] Das Bestimmtheitsgebot dient der **Vorhersehbarkeit von Eingriffen** für die Bürgerinnen und Bürger, einer **wirksamen Begrenzung der Befugnisse** der Verwaltung sowie der **Ermöglichung einer effektiven Kontrolle** durch die Gerichte, wobei an **heimliche Datenerhebungen** wegen ihres besonderen Gewichts für die Privatsphäre der Betroffenen **besonders strenge Anforderungen** zu stellen sind.[46] Da § 5 BNDG und §§ 4 Abs. 1, 5 MADG im Wesentlichen auf die Befugnisse im BVerfSchG verweisen, beschränken sich die folgenden Ausführungen auf die Regelungen des BVerfSchG.

§ 9 Abs. 1 BVerfSchG lautet:

> „Das Bundesamt für Verfassungsschutz darf Informationen, insbesondere personenbezogene Daten, mit den Mitteln gemäß § 8 Abs. 2 erheben, wenn Tatsachen die Annahme rechtfertigen, daß

---

43 BVerwG, Urteil vom 10.03.2022 - 3 C 1.21 (= BeckRS 2022, 14268 (Rn. 50)) (m.w.N.).

44 BVerfG, Urteil vom 15.12.1983 - 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 (= BVerfGE 65, 1 (46)); BVerfG, Urteil vom 11.03.2008 - 1 BvR 2074/05, 1 BvR 1254/07 (= BVerfGE 120, 378 (408)).

45 BVerfG, Urteil vom 11.03.2008 - 1 BvR 2074/05, 1 BvR 1254/07 (= BVerfGE 120, 378 (408)) (m.w.N.).

46 BVerfG, Urteil vom 20.04.2016 - 1 BvR 966/09, 1 BvR 1140/09 (= BVerfGE 141, 220 (Rn. 94)).

1. auf diese Weise Erkenntnisse über Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 oder die zur Erforschung solcher Erkenntnisse erforderlichen Quellen gewonnen werden können oder

2. dies zum Schutz der Mitarbeiter, Einrichtungen, Gegenstände und Quellen des Bundesamtes für Verfassungsschutz gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erforderlich ist.

Die Erhebung nach Satz 1 ist unzulässig, wenn die Erforschung des Sachverhalts auf andere, den Betroffenen weniger beeinträchtigende Weise möglich ist; eine geringere Beeinträchtigung ist in der Regel anzunehmen, wenn die Information aus allgemein zugänglichen Quellen oder durch eine Auskunft nach § 18 Abs. 3 gewonnen werden kann. Die Anwendung eines Mittels gemäß § 8 Abs. 2 darf nicht erkennbar außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhaltes stehen. Die Maßnahme ist unverzüglich zu beenden, wenn ihr Zweck erreicht ist oder sich Anhaltspunkte dafür ergeben, daß er nicht oder nicht auf diese Weise erreicht werden kann."

Die Vorschrift benennt zunächst hinreichend klar und präzise, welche Behörde unter welchen Voraussetzungen befugt ist, mit den in § 8 Abs. 2 BVerfSchG genannten Mitteln Informationen, insbesondere personenbezogene Daten, zu erheben. Anlass und Zweck der Maßnahmen werden damit klar umgrenzt. Zudem enthält § 9 Abs. 1 Satz 2 BVerfSchG eine besondere Ausprägung des Verhältnismäßigkeitsgrundsatzes. Dort wird ausdrücklich benannt, in welchen Fällen solche Maßnahmen unzulässig sind und unter welchen Voraussetzungen sie unverzüglich beendet werden müssen. Damit begrenzt die Norm die Befugnisse der Verwaltung und erleichtert es Bürgerinnen und Bürgern zugleich vorherzusehen, in welchen Fällen sie mit Maßnahmen rechnen müssen und in welchen nicht.

Zu den Mitteln, derer sich die Behörde unter den Voraussetzungen von § 9 Abs. 1 BVerfSchG bedienen kann, heißt es in § 8 Abs. 2 BVerfSchG:

„Das Bundesamt für Verfassungsschutz darf Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung, wie den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen anwenden. In Individualrechte darf nur nach Maßgabe besonderer Befugnisse eingegriffen werden. Im Übrigen darf die Anwendung eines Mittels gemäß Satz 1 keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht. Die Mittel nach Satz 1 sind in einer Dienstvorschrift zu benennen, die auch die Zuständigkeit für die Anordnung solcher Informationsbeschaffungen und das Nähere zu Satz 3 regelt. Die Dienstvorschrift bedarf der Zustimmung des Bundesministeriums des Innern, für Bau und Heimat, das das Parlamentarische Kontrollgremium unterrichtet."

Zunächst wird also klargestellt, dass die **Mittel** („Methoden, Gegenstände und Instrumente") der **heimlichen Informationsbeschaffung** dienen, allerdings werden sie danach nur **beispielhaft** („wie") aufgezählt. Der **Ankauf von Daten** aus Werbedatenbanken wird dort **nicht erwähnt**. Welche Mittel im Einzelnen für die heimliche Informationsbeschaffung zur Verfügung stehen, ist gemäß § 8 Abs. 2 Satz 4 BVerfSchG in einer **Dienstvorschrift** zu benennen, die auch die Zuständigkeit für die Anordnung solcher Informationsbeschaffungen und das Nähere zur

Verhältnismäßigkeit der Mittel regelt. Bei der Dienstvorschrift handelt es sich um **Innenrecht der Verwaltung**,[47] das **nicht allgemein zugänglich** ist.[48]

Ob die Behörde überhaupt Daten aus Werbedatenbanken ankaufen darf, ist für Bürgerinnen und Bürger daher ebenso wenig transparent wie die Voraussetzungen, unter denen ein Ankauf aus Sicht der Behörde als verhältnismäßig anzusehen wäre. Dies spricht dafür, dass die §§ 8 Abs. 2, 9 Abs. 1 BVerfSchG nicht als Ermächtigungsgrundlage für den Ankauf von Daten herangezogen werden können, weil anderenfalls gegen das Bestimmtheitsgebot verstoßen würde. Andererseits könnte argumentiert werden, dass die Einzelheiten nachrichtendienstlicher Methoden naturgemäß der Geheimhaltung unterliegen.[49] Wie ein Blick auf das Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)[50] zeigt, ist es der Rechtsordnung zudem keineswegs fremd, aufgrund der verfassungsrechtlichen Legitimation der nachrichtendienstlichen Aufgaben (vgl. Art. 45d, 73 Abs. 1 Nr. 10 Buchst. b, 87 Abs. 1, 109 Abs. 3, 115 Abs. 2 GG) generell Besonderheiten bei der normativen Zuweisung von Aufträgen und Befugnissen sowie bei der parlamentarischen und gerichtlichen Überprüfung zuzulassen.[51] In diesem Sinne wird durch das Erfordernis der Zustimmung des Bundesministeriums des Innern (BMI) und der Unterrichtung des Parlamentarischen Kontrollgremiums in § 8 Abs. 2 Satz 5 BVerfSchG eine ministerielle Aufsicht sowie eine parlamentarische Kontrolle gewährleistet.[52] Vor diesem Hintergrund könnte die Beeinträchtigung der Funktion des Bestimmtheitsgebots, die mit der Regelung von Einzelheiten über die Mittel zur heimlichen Informationserhebung in einer nicht allgemein zugänglichen Dienstvorschrift einhergeht, als notwendige Folge des gesetzgeberischen Versuchs, legitime staatliche Geheimhaltungsinteressen mit rechtsstaatlichen Anforderungen in Einklang zu bringen, aufgefasst werden.

Es ist demnach **offen**, ob **§§ 8 Abs. 2, 9 Abs. 1 BVerfSchG**, soweit man sie als **Ermächtigungsgrundlage** für den nachrichtendienstlichen Ankauf von Daten aus Werbedatenbanken ansieht, **hinreichend bestimmt** wären. Damit ist auch unklar, ob diese Vorschriften nach verfassungskonformer Auslegung einen solchen Ankauf grundsätzlich erlauben würden oder nicht.

---

47 Lindner/Barczak, in: Möstl/Schwabenbauer, Polizei und Sicherheitsrecht, 26. Edition, Stand: 15.10.2024, Art. 8 BayVSG Rn. 28.

48 Bergemann, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Abschnitt H Rn. 89.

49 Lampe, Die Schwierigkeiten mit der Rechtfertigung nachrichtendienstlicher Tätigkeiten, NStZ 2015, 361 (366).

50 Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG) vom 29.07.2009 (BGBl. I S. 2346), zuletzt geändert durch Artikel 10 des Gesetzes vom 19.04.2021 (BGBl. I S. 771).

51 Lampe, Die Schwierigkeiten mit der Rechtfertigung nachrichtendienstlicher Tätigkeiten, NStZ 2015, 361 (367).

52 Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 8 BVerfSchG Rn. 44.

2.4.3.2.3. Verhältnismäßigkeit

Im Übrigen müssten die gesetzlichen Vorschriften dem Grundsatz der Verhältnismäßigkeit genügen, also **zur Erreichung eines legitimen Ziels geeignet, erforderlich und angemessen** sein.[53]

Grundsätzlich bestehen an der Verhältnismäßigkeit von §§ 8 Abs. 2, 9 Abs. 1 BVerfSchG keine Zweifel, da diese Bestimmungen das Ergreifen von Maßnahmen zur heimlichen Informationserhebung in das **Ermessen der Behörde** stellen und daher stets eine verfassungskonforme Anwendung im Einzelfall möglich ist. Zudem betont **§ 9 Abs. 1 Satz 2 - 4 BVerfSchG** selbst die Bedeutung des Verhältnismäßigkeitsgrundsatzes und schreibt vor, nachrichtendienstliche Eingriffe in die Privatsphäre von Bürgerinnen und Bürgern **auf das unerlässliche Minimum zu beschränken**.

Bei gesetzlichen Befugnissen, die mit einem erhöhten Risiko von Eingriffen in den **Kernbereich privater Lebensgestaltung** einhergehen, verlangt das BVerfG jedoch zudem **ausdrückliche gesetzliche Schutzvorkehrungen**.[54] In den zugrundeliegenden Entscheidungen ging es u.a. um die Telekommunikationsüberwachung[55] und die Online-Durchsuchung[56], mithin um heimliche Maßnahmen, mit denen staatliche Stellen auf Informationen zugreifen, die auch über kommerzielle Werbedatenbanken gehandelt werden. Daher besteht auch beim **Ankauf von Daten** aus Werbedatenbanken eine **besondere Gefahr von Eingriffen in den Kernbereich privater Lebensgestaltung**, so dass das vom BVerfG postulierte Erfordernis ausdrücklicher gesetzlicher Schutzvorkehrungen auch in diesem Fall greifen dürfte. Zwar wird die besondere Bedeutung des Verhältnismäßigkeitsgrundsatzes in § 9 Abs. 1 Satz 2 - 4 BVerfSchG ausdrücklich hervorgehoben, spezifische Anforderungen im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung ergeben sich daraus jedoch nicht. Zwar könnte eine solche Regelung in der (nicht gesetzlichen) Dienstvorschrift i.S.d. § 8 Abs. 2 Satz 4 BVerfSchG untergebracht werden, jedoch ist unklar, ob dies den Anforderungen des BVerfG an den ausdrücklichen Kernbereichsschutz genügen würde.

Daher ist auch insoweit **offen**, ob der nachrichtendienstliche Datenankauf unter die Befugnisse nach **§§ 8 Abs. 2, 9 Abs. 1 BVerfSchG** in verfassungskonformer Auslegung subsumiert werden könnte.

2.4.3.3. Verfassungsmäßigkeit der Einzelmaßnahme

Die mit dem Ankauf verbundenen Grundrechtseingriffe sind nur dann verfassungsrechtlich gerechtfertigt, wenn die Ermächtigungsgrundlagen auch **im Einzelfall verfassungskonform angewandt** werden. Dazu muss unter anderem die Anwendung im Einzelfall dem **Grundsatz der Verhältnismäßigkeit** entsprechen, also zur Erreichung eines legitimen Zwecks geeignet, erforderlich

---

53 Grzeszick, in: Dürig/Herzog/Scholz, GG, Werkstand: 107. EL März 2025, Art. 20 Rn. 109.

54 BVerfG, Urteil vom 20.04.2016 - 1 BvR 966/09, 1 BvR 1140/09 (= NJW 2016, 1781 (1786 ff.)); BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07 (= BVerfGE 120, 274 (335)); BVerfG, Urteil vom 27.07.2005 - 1 BvR 668/04 (= BVerfGE 113, 348 (392)); BVerfG, Urteil vom 03.03.2004 - 1 BvR 2378/98, 1 BvR 1084/99 (= BVerfG 109, 279 (331)).

55 BVerfG, Urteil vom 27.07.2005 - 1 BvR 668/04 (= BVerfGE 113, 348 (392)).

56 BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07 (= BVerfGE 120, 274 (335)).

und angemessen sein. Beim Ankauf von Daten könnte vor allem die Angemessenheit problematisch sein. Eine Maßnahme ist angemessen, wenn die belastenden Auswirkungen, die sie für die Betroffenen hat, nicht außer Verhältnis zu dem mit der Maßnahme verfolgten Ziel stehen.[57]

Im Hinblick auf die Schwere der Belastung, die ein nachrichtendienstlicher Datenankauf für die Betroffenen hat, dürften neben der **Heimlichkeit der Maßnahme**[58] vor allem die **Authentizität** und die **Legalität der Daten** von Bedeutung sein. So ist zum einen unklar, inwieweit die von kommerziellen Händlern angebotenen Daten überhaupt **inhaltlich korrekt** sind. Beispielsweise können einzelne Daten fälschlich einer bestimmten Person zugeordnet worden sein.[59]

Des Weiteren besteht auch die Möglichkeit, dass die Daten **rechtswidrig erhoben** und in die Werbedatenbank eingestellt wurden. Das Recht der Nachrichtendienste enthält keine Vorschrift, die den Behörden die Verwendung von Informationen, die Dritte rechtswidrig erhoben haben, ausdrücklich verbietet. Ebenso sind die Nachrichtendienste nicht gesetzlich verpflichtet, die Rechtmäßigkeit der Informationen, die sie von Dritten erhalten, zu überprüfen.[60] Das BVerfG hat sich bislang nicht dazu geäußert, ob die rechtswidrige Erhebung von Daten durch Dritte ein Verwendungsverbot für die Nachrichtendienste zur Folge hat. In der Nichtannahmeentscheidung der Verfassungsbeschwerde zur Verwertbarkeit illegal erlangter Steuerdaten aus Liechtenstein hat es jedoch darauf hingewiesen, dass es von Verfassungs wegen keinen Rechtssatz des Inhalts, dass im Fall einer rechtsfehlerhaften Beweiserhebung die Verwertung der gewonnenen Beweise stets unzulässig wäre, gebe.[61] Auch wenn daher anzunehmen ist, dass den Nachrichtendiensten die Verwendung von Daten, die Dritte rechtswidrig erhoben haben, nicht a priori verboten ist, so kann diese Rechtswidrigkeit ebenso wie die inhaltliche Unrichtigkeit gleichwohl die Intensität des mit einem nachrichtendienstlichen Datenankauf verbundenen Eingriffs in die Grundrechte der Betroffenen deutlich erhöhen.

Diesen Gesichtspunkten muss bei der Entscheidung über einen Datenankauf im Einzelfall hinreichend Rechnung getragen werden. Ihnen könnte in der **Abwägung mit dem verfolgten Ziel** ein so großes Gewicht zukommen, dass die belastenden Auswirkungen des Datenankaufs außer Verhältnis zu dem damit verfolgten Ziel (vgl. § 9 Abs. 1 Nr. 1 und 2 BVerfSchG) stehen könnten, so dass der Ankauf in diesem Fall nicht angemessen und somit unzulässig wäre.

---

57 Grzeszick, in: Dürig/Herzog/Scholz, GG, Werkstand: 107. EL März 2025, Art. 20 Rn. 119.

58 Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Abschnitt G Rn. 127.

59 Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Abschnitt G Rn. 128.

60 Sosna, „Fundgrube Internet“ – vom tatsächlich möglichen und rechtlich zulässigen Sammeln der Nachrichtendienste im Netz, GSZ 2024, 53 (57).

61 BVerfG, Beschluss vom 09.11.2010 - 2 BvR 2101/09 (= NStZ 2011, 103 (Rn. 43)).

3. Datenankauf durch Behörden für Zwecke der Strafverfolgung und der Gefahrenabwehr

Auch im Fall von behördlichen Datenankäufen für Zwecke der Verfolgung und Verhütung von Straftaten und der Gefahrenabwehr muss zunächst der einschlägige Prüfungsmaßstab bestimmt werden.

3.1. Prüfungsmaßstab

Wie im Fall der Nachrichtendienste (siehe oben 2.1.) greift auch für die Verarbeitung personenbezogener Daten im Bereich der **Strafverfolgung** und der **Gefahrenabwehr** im Hinblick auf die Anwendbarkeit der DS-GVO eine **Bereichsausnahme**. Gemäß **Art. 2 Abs. 2 Buchst. d) DS-GVO** findet die Verordnung keine Anwendung, wenn Behörden personenbezogene Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, verarbeiten. Für den Datenschutz im Zusammenhang mit diesen Tätigkeiten gilt, wie in Erwägungsgrund 19 zur DS-GVO bekräftigt wird, stattdessen die **Richtlinie (EU) 2016/680** des Europäischen Parlaments und des Rates (JI-RL)[62].

Obwohl dem Unionsrecht im Verhältnis zum **nationalen Recht grundsätzlich ein umfassender Anwendungsvorrang zukommt, ist unionsrechtlich nicht vollständig determiniertes innerstaatliches Recht primär am Maßstab** der Grundrechte des GG zu überprüfen, auch wenn das innerstaatliche Recht der Durchführung des Unionsrechts dient.[63] Anders als eine unionsrechtliche Verordnung, die gemäß Art. 288 Abs. 2 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV)[64] allgemeine Geltung besitzt und in allen ihren Teilen verbindlich und in jedem Mitgliedstaat unmittelbar gültig ist, erstreckt sich die Verbindlichkeit einer Richtlinie gemäß Art. 288 Abs. 3 AEUV allein auf das zu erreichende Ziel, während die Wahl der Form und der Mittel innerstaatlichen Stellen überlassen bleibt. Die JI-RL macht den Mitgliedstaaten Vorgaben für die Datenverarbeitung im Bereich der Strafverfolgung und Gefahrenabwehr, lässt den Mitgliedstaaten aber Regelungsspielräume bei der Umsetzung in nationales Recht.[65] Dieser Bereich ist folglich nicht vollständig unionsrechtlich determiniert, so dass die **Grundrechte des Grundgesetzes anwendbar** bleiben und somit als Prüfungsmaßstab herangezogen werden können.

---

62 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2000/383/JI des Rates, ABl. L 119 vom 04.05.2016, S. 89 - 131.

63 BVerfG, Beschluss vom 06.11.2019 - 1 BvR 16/13 (= NJW 2020, 300 (Rn. 41 ff.)).

64 Vertrag über die Arbeitsweise der Europäischen Union (AEUV), Fassung aufgrund des am 01.12.2009 in Kraft getretenen Vertrages von Lissabon (Konsolidierte Fassung bekanntgemacht im ABl. EG Nr. C 115 vom 09.05.2008, S. 47), zuletzt geändert durch die Akte über die Bedingungen des Beitritts der Republik Kroatien und die Anpassungen des Vertrags über die Europäische Union, des Vertrags über die Arbeitsweise der Europäischen Union und des Vertrags zur Gründung der Europäischen Atomgemeinschaft (ABl. EU L 112/21 vom 24.4.2012) m.W.v. 01.07.2013.

65 Herbst, in: Möllers/Heid, Wörterbuch Polizei- und Sicherheitsrecht, 4. Aufl. 2025, Eintrag „Recht auf informationelle Selbstbestimmung“.

3.2. Schutzbereich und Eingriff

Im Hinblick auf die Schutzbereiche der einschlägigen Grundrechte und die Frage, ob der behördliche Datenankauf in diese Schutzbereiche eingreift, gilt das **oben unter 2.2. und 2.3.** Ausgeführte entsprechend.

3.3. Verfassungsmäßige Rechtfertigung

Die Eingriffe sind verfassungsmäßig gerechtfertigt, wenn der Datenkauf durch gesetzliche Ermächtigungsgrundlagen, die die Grundrechtsschranken in verfassungsmäßiger Weise ausfüllen, gedeckt ist, und diese Grundlagen im Einzelfall verfassungskonform angewandt werden.

3.3.1. Grundrechtsschranken

Zu den Grundrechtsschranken gilt das oben unter 2.4.1. Gesagte.

3.3.2. Schrankenkonkretisierung

Als Schrankenkonkretisierungen kommen im Bereich der Verfolgung und Verhütung von Straftaten und der Gefahrenabwehr, je nach handelnder Behörde, **auf Bundesebene** insbesondere Vorschriften aus der **Strafprozessordnung (StPO)**[66], dem **Bundeskriminalamtgesetz (BKAG)**[67] und dem **Bundespolizeigesetz (BPolG)**[68] in Betracht. Für Datenankäufe durch Landesbehörden muss insoweit auf entsprechende **landesrechtliche Regelungen**, beispielsweise in den **Polizeigesetzen der Länder**, zurückgegriffen werden. Diese Regelungen sind jedoch nicht Gegenstand dieser Ausarbeitung.

3.3.2.1. Staatsanwaltschaft

Die StPO verleiht der Staatsanwaltschaft (StA) zahlreiche Befugnisse zur Erhebung solcher Daten, die typischerweise auch in Werbedatenbanken zusammengeführt und angeboten werden. Die Befugnisse der StA stehen gemäß § 399 Abgabenordnung (AO)[69] auch den **Finanzbehörden** zu, wenn sie in Steuerstrafverfahren ermitteln. Zu diesen Befugnissen gehören die **Telekommunikationsüberwachung (§ 100a StPO) sowie die Erhebung von Verkehrs- (§ 100g StPO), Standort- (§ 100i StPO) und Nutzungsdaten (§ 100k StPO)**. Diese Befugnisse erlauben der StA allerdings **nicht** den **Ankauf von Daten**, sondern allein die **Erhebung durch eigene Ermittlungsmittel** oder durch **Anordnungen** an **dezidierte Dritte**, zu denen **nicht** die **Betreiber von Werbedatenbanken** gehören. So ist bei der Telekommunikationsüberwachung gemäß **§ 100a Abs. 4 StPO** „jeder, der

---

66 Strafprozeßordnung (StPO) in der Fassung der Bekanntmachung vom 07.04.1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Artikel 2 des Gesetzes vom 17.07.2025 (BGBl. 2025 I Nr. 163).

67 Bundeskriminalamtgesetz (BKAG) vom 01.06.2017 (BGBl. I S. 1354; 2019 I S. 400), zuletzt geändert durch Artikel 1 des Gesetzes vom 17.07.2025 (BGBl. 2025 I Nr. 172).

68 Bundespolizeigesetz (BPolG) vom 19.10.1994 (BGBl. I S. 2978, 2979), zuletzt geändert durch Artikel 5 des Gesetzes vom 06.05.2024 (BGBl. 2024 I Nr. 149).

69 Abgabenordnung (AO) in der Fassung der Bekanntmachung vom 01.10.2002 (BGBl. I S. 3866, ber. 2003 S. 61), zuletzt geändert durch Gesetz vom 02.12.2024 (BGBl. I S. 387).

Telekommunikationsdienstleistungen erbringt oder daran mitwirkt“ gegenüber den Behörden zur Auskunft verpflichtet. Für die Erhebung von Verkehrsdaten stellt **§ 100g Abs. 5 StPO** ausdrücklich klar, dass § 100g StPO nur auf diejenigen Fälle anwendbar ist, in denen die Daten beim Erbringer von Telekommunikationsdienstleistungen erhoben werden, und im Übrigen auf die allgemeinen Vorschriften zurückzugreifen ist. Eine parallele Regelung findet sich für die Erhebung von Nutzungsdaten in **§ 100k Abs. 5 StPO**. **§ 100i Abs. 1 StPO** erlaubt den Behörden die Erhebung von Standortdaten nur „durch technische Mittel“.

In Ermangelung spezieller Eingriffsbefugnisse könnte als gesetzliche Grundlage für Datenkäufe die **allgemeine Ermittlungsbefugnis der StA** aus **§ 161 Abs. 1 Satz 1 StPO** in Betracht kommen. Danach ist die StA befugt, **Ermittlungen jeder Art** entweder selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen. Als einschlägige Ermittlungsmaßnahmen „kommen sämtliche, gerade auch freibeweisliche Informationsbeschaffungen in Betracht, die zur Aufklärung des Sachverhalts erforderlich sind, wegen **minderer Eingriffstiefe** keiner eigenen spezialgesetzlichen Ermächtigungsgrundlage bedürfen und darüber hinaus auch im engeren Sinne **verhältnismäßig** sind“[70]. Auch ein Ankauf von Beweismitteln ist danach nicht von vornherein ausgeschlossen.[71] Dies gilt insbesondere auch für den Ankauf von durch Privatpersonen zuvor beschafften Daten – selbst dann, wenn diese Beschaffung rechtswidrig erfolgte.[72]

Allerdings könnte je nach Sachverhaltskonstellation im Einzelfall fraglich erscheinen, ob auch der Ankauf umfangreicher und potenziell tief in das Privatleben betroffener Personen hineinreichender Informationen, wie sie in Werbedatenbanken enthalten sein können, tatsächlich noch als **Maßnahme mit nur geringer Eingriffsintensität** im Sinne von § 161 Abs. 1 StPO angesehen werden könnte. Nach **Ansicht des BVerfG** kann die StA zwar – gestützt auf § 161 Abs. 1 StPO – Kreditkarteninstitute darum ersuchen, die Daten über Kunden, die innerhalb eines bestimmten Zeitraums eine Zahlung in bestimmter Höhe an einen bestimmten Empfänger geleistet haben, herauszugeben.[73] Denn auch wenn das Ersuchen aus Sicht der betroffenen Kunden heimlich erfolgt sei und sich auf Daten bezogen habe, die nicht für den staatlichen Zugriff bestimmt gewesen seien, weise ein solches Ersuchen nur eine **geringe Eingriffsintensität** auf, da von ihm nur ein eng begrenzter und präzise beschriebener Personenkreis, der nach dem damaligen Ermittlungsstand durch sein Verhalten den Tatverdacht begründet hatte, betroffen gewesen sei.[74]

Die dieser Entscheidung **zugrundeliegende Konstellation dürfte sich vom Datenankauf** aus kommerziellen Datenbanken jedoch maßgeblich dadurch **unterscheiden**, dass das Ersuchen dort

---

70 Weingarten, in: Karlsruher Kommentar zur Strafprozessordnung, 9. Aufl. 2023, § 161 StPO Rn. 14 m.w.N. (Hervorhebung nicht im Original).

71 Vgl. Kaiser, Zulässigkeit des Ankaufs deliktisch erlangter Steuerdaten, NStZ 2011, 383 (385); Wissenschaftliche Dienste des Deutschen Bundestages, Der Ankauf von Beweismitteln durch die Staatsanwaltschaft, Ausarbeitung WD 7-3000-062/08, 15.04.2008, S. 7.

72 Vgl. LG Düsseldorf, Beschluss vom 11.10.2010 - 4 Qs 50/10 (= NStZ-RR 2011, 84); Verfassungsgerichtshof Rheinland-Pfalz, Urteil vom 24.02.2014 - VGH B 26/13 (= NZWiSt 2014, 421); Kaiser, Zulässigkeit des Ankaufs deliktisch erlangter Steuerdaten, NStZ 2011, 383 (385 f.).

73 BVerfG, Beschluss vom 17.02.2009 - 2 BvR 1372, 1745/07 (= NJW 2009, 1405 (1406 f.)).

74 BVerfG, Beschluss vom 17.02.2009 - 2 BvR 1372, 1745/07 (= NJW 2009, 1405 (1407)).

ausschließlich ganz bestimmte Angaben über eine Zahlung betraf, während kommerzielle Datenbanken **umfangreiche Informationen** über **Wohnsitz, Alter, Geschlecht, Konsumverhalten, Interessen, Kommunikationskanäle oder Bewegungsprofile** enthalten können und somit gegebenenfalls einen deutlich tieferen Einblick in die Persönlichkeit und das Privatleben Betroffener erlauben als die Information über eine einzelne Kontobewegung.[75] Die unterschiedlichen Datentypen können in den Datenbanken zudem **systematisch zusammengetragen** und **miteinander verknüpft** sein, so dass ein staatlicher Zugriff auf diese Daten potenziell den **Kernbereich der persönlichen Lebensgestaltung** betroffener Personen tangiert. Hinzu kommt, dass die StPO für viele der Datentypen, die in kommerzielle Datenbanken einfließen (Telekommunikations-, Verkehrs-, Standort- und Nutzungsdaten) gerade aufgrund der Sensibilität und Höchstpersönlichkeit der betroffenen Bereiche wie oben dargelegt **Spezialbefugnisse** enthält. Es erscheint insofern fraglich, ob es mit dieser gesetzgeberischen Wertung zu vereinbaren wäre, wenn die entsprechenden Datentypen aufgrund von § 161 Abs. 1 Satz 1 StPO durch das Mittel des Ankaufs erlangt und im Nachgang ausgewertet werden könnten, ohne dass die hierfür in der StPO spezifisch vorgesehenen, die Rechtsgüterabwägung gesetzgeberisch konkretisierenden Sicherungsmechanismen Anwendung fänden.

Insofern dürfte sich die Zulässigkeit des Ankaufs und der Auswertung von Daten nicht pauschalabstrakt feststellen lassen, sondern von der Fallkonstellation im jeweiligen Einzelfall abhängen – insbesondere davon, **welche Daten** konkret erfasst sind, **wie** sie ursprünglich **erlangt** wurden und von welcher **Schwere** die **Straftat** ist, auf die sich das Ermittlungsverfahren bezieht.

3.3.2.2. Bundespolizei

Die **Bundespolizei (BPol)** kann gemäß **§ 21 Abs. 1 BPolG** personenbezogene Daten erheben, soweit dies zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist. Grundsätzlich muss die Datenerhebung gemäß § 21 Abs. 3 Satz 1 BPolG **offen und beim Betroffenen selbst erfolgen**. Sie kann jedoch gemäß § 21 Abs. 3 Satz 2 BPolG **ausnahmsweise** dann **bei anderen nicht-öffentlichen Stellen** erfolgen, wenn die Erhebung beim Betroffenen nicht möglich ist oder durch sie die Erfüllung der der Bundespolizei obliegenden Aufgaben gefährdet oder erheblich erschwert würde. Als nicht-öffentliche Stellen sind dabei neben natürlichen Personen auch **alle privatrechtlich organisierten Unternehmungen und Vereinigungen** zu verstehen, solange sie nicht wegen der Wahrnehmung öffentlicher Aufgaben dem öffentlichen Bereich zugerechnet werden.[76] Dies spricht dafür, dass die Bundespolizei personenbezogene Daten in Ausnahmefällen auch von kommerziellen Datenbanken ankaufen könnte. Allerdings berechtigen verdeckte Datenerhebungen i.S.d. § 21 Abs. 3 BPolG **nicht** zu **Maßnahmen**, die in ihrer **Eingriffsintensität** den in § 28 Abs. 2 BPolG geregelten **besonderen Mitteln der Datenerhebung vergleichbar** sind.[77] § 28 Abs. 2 BPolG nennt die **längerfristige Observation**, den **verdeckten Einsatz technischer Mittel** zur Anfertigung von **Bild- und Tonaufzeichnungen** sowie zum **Abhören** des **nichtöffentlich gesprochenen Wortes**, den Einsatz von **Vertrauenspersonen** (V-Leute) und **verdeckten Ermittlern**. Gemein ist diesen Maßnahmen, dass sie der BPol Zugriff auf sehr detaillierte Informationen über die

---

75 Differenzierend etwa auch Verfassungsgerichtshof Rheinland-Pfalz, Urteil vom 24.02.2014 - VGH B 26/13 (= NZWiSt 2014, 421 (427 f.)).

76 Graulich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 21 BPolG Rn. 12.

77 Graulich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 21 BPolG Rn. 14.

Persönlichkeit und das Privatleben Betroffener verschaffen. Die in kommerziellen Datenbanken enthaltenen Daten ermöglichen nicht zuletzt aufgrund ihrer systematischen Zusammenführung und Verknüpfung **ähnlich tiefe Einblicke**. Ein behördlicher Zugriff auf diese Daten würde also mit **vergleichbarer Intensität** in die Grundrechte Betroffener eingreifen wie die besonderen Mittel der Datenerhebung nach § 28 Abs. 2 BPolG. Dies gilt umso mehr, wenn die Erhebung ohne das Wissen der betroffenen Personen erfolgt.

Somit dürfte § 21 Abs. 1, 3 BPolG **als Ermächtigungsgrundlage** für einen Datenankauf durch die BPol **ausscheiden**.

3.3.2.3. Bundeskriminalamt

Dem Bundeskriminalamt (BKA) stehen, ähnlich wie der StA, umfangreiche Befugnisse zur **Erhebung** von **Telekommunikationsdaten (§ 51 BKAG), Verkehrs- und Nutzungsdaten (§ 52 BKAG)** sowie **Standortdaten (§ 53 BKAG)** zu. Allerdings berechtigen auch diese Vorschriften nur zu eigenen Überwachungsmaßnahmen der Behörde (vgl. § 51 Abs. 1, 2 BKAG) oder zur **Verpflichtung ganz bestimmter Stellen**, zu denen **nicht** die **Betreiber kommerzieller Datenbanken** gehören, Auskunft zu erteilen oder Daten herauszugeben (vgl. § 52 Abs. 2, 53 Abs. 4 BKAG). Somit scheiden diese Vorschriften als Ermächtigungsgrundlage für einen Datenankauf aus.

Das BKA kann ferner gemäß **§ 39 Abs. 1 BKAG** personenbezogene Daten erheben, soweit die zur Erfüllung seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus (vgl. § 5 Abs. 1 Satz 1 BKAG) erforderlich ist. Zudem erlaubt **§ 39 Abs. 2 BKAG** die Erhebung von Daten unter bestimmten Voraussetzungen auch zur Verhütung von Straftaten, die in § 129a Abs. 1 und Abs. 2 Strafgesetzbuch (StGB)[78] bezeichnet sind (vgl. § 5 Abs. 1 Satz 2 BKAG). Dabei gelten gemäß § 39 Abs. 3 BKAG die in **§ 9 Abs. 2 und 3 BKAG** enthaltenen Regelungen entsprechend. Gemäß **§ 9 Abs. 2 Satz 2 BKAG** sind personenbezogene Daten **offen und bei der betroffenen Person** zu erheben. Sie können gemäß **§ 9 Abs. 2 Satz 3 BKAG** auch bei **nichtöffentlichen Stellen** erhoben werden, wenn die Erhebung bei der betroffenen Person nicht möglich ist oder durch sie die Erfüllung der dem Bundeskriminalamt obliegenden Aufgaben gefährdet oder erheblich erschwert würde. Diese **Regelungen entsprechen** im Wesentlichen dem oben erläuterten **§ 21 Abs. 3 BPolG**. Dies legt nahe, dass auch im Rahmen des BKAG **verdeckte Erhebungen bei nichtöffentlichen Stellen** jedenfalls dann **nicht** auf die allgemeinen Befugnisse zur Datenerhebung in **§ 39 Abs. 1, 2 BKAG** gestützt werden können, wenn diese Maßnahmen in ihrer **Eingriffsintensität besonderen Mitteln der Datenerhebung gleichkommen**. Dem BKA stehen gemäß § 45 Abs. 2 BKAG die gleichen besonderen Mittel zu wie der BPol gemäß § 28 Abs. 2 BPolG. Entsprechend dem oben zu den Befugnissen der BPol Gesagten würde ein verdeckter Zugriff des BKA auf die in Werbedatenbanken enthaltenen personenbezogenen Daten eine ähnlich hohe Eingriffsintensität aufweisen wie die besonderen Mittel der Datenerhebung nach § 45 Abs. 2 BKAG.

Somit dürften **§ 39 Abs. 1 und 2 BKAG keine Ermächtigungsgrundlagen** für den Ankauf personenbezogener Daten aus kommerziellen Datenbanken darstellen.

---

78 Strafgesetzbuch (StGB) in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 07.11.2024 (BGBl. I S. 351).

4. Datenankauf durch Behörden für andere Zwecke

Kaufen Behörden Daten aus kommerziellen Datenbanken zu **anderen als den vorstehend erörterten Zwecken** an, so muss wiederum zunächst der einschlägige Prüfungsmaßstab bestimmt werden.

4.1. Prüfungsmaßstab

Anders als für die Tätigkeit der Nachrichtendienste sowie für die Bereiche der Verfolgung und Verhütung von Straftaten und der Gefahrenabwehr enthält die DS-GVO **keine dezidierte Bereichsausnahme** für andere behördliche Aufgabenbereiche. Soweit Behörden in diesen Aufgabenbereichen **personenbezogene Daten ganz oder teilweise automatisiert verarbeiten** oder personenbezogene Daten im Fall der **nichtautomatisierten Verarbeitung** in einem **Dateisystem speichern** oder **speichern wollen**, gilt dafür die DS-GVO (vgl. Art. 2 Abs. 1 DS-GVO). Als Verarbeitung gilt gemäß Art. 4 Nr. 2 DS-GVO auch das Erheben und Erfassen personenbezogener Daten. Der behördliche Ankauf personenbezogener Daten aus Werbedatenbanken dient der Erhebung und Erfassung dieser Daten, so dass die **DS-GVO** in diesen Fällen **anwendbar** ist.

Als **unionsrechtliche Verordnung** ist die DS-GVO gemäß **Art. 288 Abs. 2 AEUV** in allen ihren Teilen **verbindlich** und hat in jedem Mitgliedstaat **unmittelbare Geltung**. Bei der Anwendung solcher unionsrechtlich vollständig vereinheitlichter Regelungen sind grundsätzlich **nicht die deutschen Grundrechte**, sondern **allein die Unionsgrundrechte** maßgeblich, da das Unionsrecht in diesen Fällen gegenüber den Grundrechten des Grundgesetzes Anwendungsvorrang genießt.[79] Dies gilt jedenfalls unter dem Vorbehalt, dass auf Unionsebene ein dem Grundgesetz im Wesentlichen vergleichbarer Grundrechtsschutz gegeben ist.[80] Dies ist nach dem derzeitigen Stand des Unionsrechts der Fall.[81] Soweit die Grundrechte des Grundgesetzes durch den Anwendungsvorrang des Unionsrechts verdrängt werden, kontrolliert das BVerfG dessen Anwendung durch deutsche Stellen am **Maßstab der Unionsgrundrechte**. Soweit den Mitgliedstaaten ein Umsetzungsspielraum bei der Ausgestaltung der jeweiligen fachgesetzlichen Eingriffsbefugnisse verbleibt, sind weiterhin die Grundrechte des GG einschlägig (insoweit vgl. oben 2.2. - 2.4.).

4.2. Schutzbereich und Eingriff/Beeinträchtigung

Soweit die Unionsgrundrechte als Maßstab einschlägig sind, kommen insbesondere das Grundrecht auf den Schutz personenbezogener Daten aus **Art. 8 der Grundrechte-Charta (GRCh)**[82] und das Recht auf Achtung des Privatlebens und der Kommunikation aus **Art. 7 GRCh** in Betracht. Während sich der Schutz von Art. 8 GRCh allgemein auf **personenbezogene Daten** erstreckt[83],

---

79 BVerfG, Beschluss vom 06.11.2019 -1 BvR 276/17 (= NJW 2020, 314 (Rn. 42)).

80 BVerfG, Beschluss vom 06.11.2019 - 1 BvR 276/17 (= NJW 2020, 314 (Rn. 47)).

81 BVerfG, Beschluss vom 06.11.2019 - 1 BvR 276/17 (= NJW 2020, 314 (Rn. 48)).

82 Charta der Grundrechte der Europäischen Union (GRCh), ABl. C 326 vom 26.10.2012, S. 391.

83 Kingreen, in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. 2022, Art. 8 GRCh Rn. 10.

schützt Art. 7 GRCh mit dem Begriff „Kommunikation“ insbesondere das **Brief-, Post- und Telekommunikationsgeheimnis**, also den kommunikativen Übermittlungsvorgang.[84]

Den obigen Ausführungen unter 2.2. und 2.3. entsprechend stellt ein behördlicher Ankauf personenbezogener Daten **je nach Datentyp** eine **Beeinträchtigung** in das Recht auf Achtung des Privatlebens und der Kommunikation aus Art. 7 GRCh (**Telekommunikations- und Verkehrsdaten**) oder einen **Eingriff** in das Recht auf Schutz personenbezogener Daten aus Art. 8 GRCh (**sonstige personenbezogene Daten**) dar.

4.3. Rechtfertigung

Eingriffe in das Grundrecht aus Art. 8 Abs. 1 GRCh bedürfen gemäß **Art. 8 Abs. 2 Satz 1 GRCh** einer **gesetzlich geregelten legitimen Grundlage**. Damit konkretisiert Art. 8 Abs. 2 Satz 1 GRCh den allgemeinen Gesetzesvorbehalt des Art. 52 Abs. 1 Satz 1 GRCh.[85] Darüber hinaus muss die Datenerhebung den **Wesensgehalt des Grundrechts** achten, einen **legitimen Zweck** verfolgen und **verhältnismäßig** sein (vgl. **Art. 52 Abs. 1 Satz 2 GRCh**).[86]

Beeinträchtigungen des Grundrechts aus Art. 7 GRCh unterliegen dem allgemeinen Gesetzesvorbehalt für Eingriffe in Unionsgrundrechte in **Art. 52 Abs. 1 GRCh**.[87] Danach muss jede Einschränkung der Ausübung der Grundrechte **gesetzlich vorgesehen** sein, den **Wesensgehalt** dieser Rechte **achten** und den **Grundsatz der Verhältnismäßigkeit** wahren.

4.4. Konkretisierung

Als Konkretisierung beider Vorbehalte kommt **Art. 6 Abs. 1 Buchst. e, Abs. 2-4 DS-GVO** in Betracht. Danach ist die Verarbeitung personenbezogener Daten zulässig, wenn die Verarbeitung für die **Wahrnehmung einer Aufgabe** erforderlich ist, die im **öffentlichen Interesse** liegt, oder **in Ausübung öffentlicher Gewalt** erfolgt, die dem Verantwortlichen übertragen wurde. Die Vorschrift betrifft Datenverarbeitungen der öffentlichen Hand.[88] Sie stellt jedoch **keinen eigenständigen Erlaubnistatbestand** für eine Verarbeitung dar, so dass es dafür einer **Rechtsgrundlage im Unionsrecht** oder im **Recht der Mitgliedstaaten** bedarf.[89] Diese muss den **Anforderungen von Art. 6 Abs. 3 DS-GVO** genügen.[90] Die konkrete Rechtsgrundlage richtet sich nach der im Einzelfall handelnden Behörde und dem einschlägigen Fachrecht. Wegen der Vielzahl der insoweit

---

84 Kingreen, in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. 2022, Art. 7 GRCh Rn. 10.

85 Kingreen, in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. 2022, Art. 8 GRCh Rn. 15.

86 Kingreen, a.a.O.

87 Kingreen, in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. 2022, Art. 7 GRCh Rn. 14.

88 Schulz, in: Gola/Heckmann, DS-GVO/BDSG, 3. Aufl. 2022, Art. 6 DS-GVO Rn. 51.

89 Schulz, a.a.O.

90 Schulz, a.a.O.

grundsätzlich in Betracht kommenden Vorschriften würde eine nähere Betrachtung über den Rahmen dieser Ausarbeitung hinausgehen.

Art. 6 Abs. 3 Satz 1 DS-GVO verlangt, dass der **Zweck der Verarbeitung** in der Rechtsgrundlage festgelegt oder für die Erfüllung der in Art. 6 Abs. 1 Buchst. e DS-GVO genannten Aufgabe erforderlich sein muss. Diese Rechtsgrundlage kann gemäß **Art. 6 Abs. 3 Satz 2 DS-GVO** spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften der DS-GVO enthalten, unter anderem Bestimmungen darüber, welche **allgemeinen Bedingungen** für die Regelung der **Rechtmäßigkeit der Verarbeitung** durch den Verantwortlichen gelten, welche **Arten von Daten** verarbeitet werden, welche **Personen betroffen** sind, an **welche Einrichtungen** und für **welche Zwecke** die personenbezogenen Daten **offengelegt** werden dürfen, welcher **Zweckbindung** sie unterliegen, **wie lange** sie **gespeichert** werden dürfen und welche **Verarbeitungsvorgänge und -verfahren** angewandt werden dürfen, einschließlich Maßnahmen zur **Gewährleistung** einer **rechtmäßig** und nach **Treu und Glauben** erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX der DS-GVO. Die Rechtsgrundlage muss gemäß **Art. 6 Abs. 3 Satz 3 DS-GVO** ferner ein **im öffentlichen Interesse liegendes Ziel** verfolgen und in einem **angemessenen Verhältnis** zu dem verfolgten legitimen Zweck stehen.

Erfüllt die jeweilige Rechtsgrundlage diese Voraussetzungen, so muss sie darüber hinaus den Ankauf von personenbezogenen Daten aus kommerziellen Datenbanken abdecken und **im Einzelfall recht- und verhältnismäßig angewandt** worden sein.

***