

Nutzung von kommerziell erhältlichen personenbezogenen Daten und daraus gewonnenen Informationen durch die Bundesregierung

BT-Drucksache 21/2855

Vorbemerkung der Fragesteller:

Data Broker sammeln personenbezogene Daten an mit dem Ziel, diese in nativer oder aufbereiteter Form an Kunden zu veräußern, die an Betrugserkennung, Bonitätsbewertung, dem Einsatz von personalisierter Werbung oder anderen Motiven der Profilbildung interessiert sind (<https://www.avenga.com/magazine/what-is-a-data-broker/>). Die globale Marktgröße wird auf knapp 300 Mrd. US-Dollar geschätzt, wobei der Anteil Nordamerikas daran mehr als 40 Prozent beträgt (<https://www.grandviewresearch.com/industry-analysis/data-broker-market-report>). Informationsquellen der Data Broker sind nicht nur öffentlich zugängliche Informationen, sondern insbesondere persönliche Daten und Verhaltensmuster aus Apps und Diensten, bei denen die Nutzenden in die Weitergabe der Daten beispielsweise zum Zweck des Marketings vermeintlich eingewilligt haben. Der Datenabfluss erfolgt dann häufig über Softwarepakete Dritter (SDKs), aber auch beim Ausspielen personalisierter Onlinewerbung selbst können personenbezogene Daten während des „Real Time Bidding“ massenhaft in die Hände von Werbetreibenden oder auch von Data Brokern gelangen (<https://netzpolitik.org/2025/databroker-files-im-dschungel-der-datenhaendler/>). Wie groß das Ausmaß dieses Datenhandels weitgehend abseits der öffentlichen Wahrnehmung ist, zeigten Recherchen unter anderem von Netzpolitik.org in den vergangenen Jahren: Allein die Angebotsliste des Datenmarktplatzes Xandr enthielt im Jahr 2021 die Zuordnung einer unbekannten Anzahl einzelner Personen in mehr als 650.000 Kategorien persönlicher Eigenschaften. 3,6 Milliarden Standortdaten von 11 Millionen Handys aus Deutschland aus einem Zeitraum von nur 2 Monaten erhielten BR/ARD und Netzpolitik.org während einer gemeinsamen Recherche als Preview von einem Datenhändler, vermittelt über Datarade im Jahr 2024. Datarade sieht sich selbst nicht als datenverarbeitender Datenhändler, sondern als Datenmarktplatz, der lediglich als Vermittlungsplattform zwischen Data Brokern und Interessenten operiert. Das Unternehmen erhielt unter anderem Mittel vom Bundeswirtschaftsministerium im Rahmen des High-Tech Gründerfonds (<https://fragden-staat.de/anfrage/antwort-des-staatssekretaers-sven-giegold-auf-eine-frage-der-abgeordneten-martina-renner-zur-foerderung-des-unternehmens-datarade/960450/anhang/10-390-renner-anlageeinstufungaufgehoben.pdf>).

Nach Ansicht der Fragestellenden mehrten sich bereits seit den Enthüllungen Edward Snowdens im Jahr 2013 Hinweise darauf, dass Sicherheitsbehörden einen nachfrageseitigen Faktor beim kommerziellen Handel mit personenbezogenen Daten darstellen.

2017 wurde von Forschenden der Begriff „advertising-based intelligence“ (ADINT) geschaffen, um das Phänomen zu beschreiben (<https://adint.cs.washington.edu>), dass Anbieter von Überwachungs-Dienstleistungen für Sicherheitsbehörden tätig sind und Material von Data Brokers für diese Zwecke aufbereiten und analysieren. Ein direkter Erwerb der Rohdaten durch die Interessenten ist somit nicht unbedingt erforderlich. Aus den USA ist bekannt, dass staatliche Stellen in erheblichem Umfang auf Angebote von Datenhändlern und Dienste von ADINT-Firmen zurückgreifen. Mindestens seit 2020 nutzen US-amerikanische Behörden für Einwanderung und Grenzschutz Handy-Standortdaten der Werbeindustrie, bereitgestellt über den Dienstleister Venntel (<https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>). Einem Medienbericht zufolge geschieht dies auch in den Niederlanden (<https://www.bnr.nl/nieuws/technologie/10537256/nederlandse-telefoons-online-stiekem-te-volgen-extreem-veiligheidsrisico>). Konkret in Deutschland geht aus der Gesetzesbegründung zu §10a im Entwurf des BND-Gesetzes (Bundestagsdrucksache 20/8627) hervor, dass die Bundesregierung den Ankauf von Werbedaten zumindest hinsichtlich des Bundesnachrichtendienstes als ein mögliches Szenario erwähnt.

Indes stellt der Datenhandel gleichzeitig ein Sicherheitsrisiko für die Staaten selbst dar. So gelang es BR/ARD und Netzpolitik.org allein anhand der über Datarade vermittelten Vorschau-Daten, Bewegungsprofile einem hohen Beamten mit Sicherheitsaufgaben sowie einem Mitarbeiter eines deutschen Geheimdienstes zuzuordnen und diese zu identifizieren (<https://netzpolitik.org/2024/databroker-files-wie-datenhaendler-deutschlands-sicherheit-gefaehrden/>). Auch für Militäreinrichtungen (<https://www.tagesschau.de/investigativ/br-recherche/militaereinrichtungen-standortdaten-sicherheitsrisiko-100.html>) und kritische Infrastruktur geht ein erhebliches Risiko von Data Brokers aus.

Vorbemerkung der Bundesregierung:

Die Bundesregierung ist nach sorgfältiger Abwägung der grundsätzlichen verfassungsrechtlichen Pflicht, Informationsansprüche des Deutschen Bundestages zu erfüllen, zu der Auffassung gelangt, dass die Fragen 5-8 aus Gründen des Staatswohls nicht für das Bundeskriminalamt, die Bundespolizei und die Zentrale Stelle für Informationstechnik im Sicherheitsbereich - auch nicht in eingestufte Form - beantwortet werden können.

Durch die Beantwortung der Fragen zu konkreten Maßnahmen, Kontakten oder Beschaffungen würden Einblicke auf zur Verfügung stehende (kriminal)polizeiliche und sonstige technische Vorgehensweisen zur Gefahrenabwehr oder zur Verhinderung und Aufklärung von Straftaten offengelegt oder Rückschlüsse darauf ermöglicht und damit die Arbeitsfähigkeit und Aufgabenerfüllung der Sicherheits- und Strafverfolgungsbehörden gefährdet. Täter oder potentielle Zielpersonen könnten ihr Verhalten anpassen und künftige Maßnahmen dadurch erschweren oder gar vereiteln. Eine Preisgabe dieser sensiblen Informationen würde sich auf die staatliche Aufgabenwahrnehmung im Gefahrenabwehrbereich wie auch auf die Durch-

setzung des Strafverfolgungsanspruchs und die (kriminal-)polizeiliche Informationsbeschaffung außerordentlich nachteilig auswirken, da unter anderem eine eindeutige Zuordnung zu etwaigen Vorgehensweisen möglich wäre.

Neben der Preisgabe bezüglich der generellen Nutzung von entsprechenden Angeboten können andererseits insbesondere durch Informationen zu konkret genutzten Unternehmen und den genutzten Zeiträumen Rückschlüsse auf den Kenntnisstand der oben genannten Behörden sowie deren aktuellen Bearbeitungsschwerpunkte gezogen werden. Eine Beantwortung könnte auch fremde staatliche Akteure dazu verleiten, entsprechende Dienste anzugreifen, um die jeweiligen Datenbestände im eigenen Sinne zu manipulieren. Die erbetenen Informationen zielen im Kern auf die Offenlegung bestimmter Arbeitsmethoden und Vorgehensweisen im Bereich der technischen Ressourcen ab. Solche durch die Kooperation mit Unternehmen nachvollziehbaren Arbeitsmethoden sind im Hinblick auf die künftige Erfüllung des jeweiligen (gesetzlichen) Auftrags jedoch besonders schutzwürdig. Die besondere Schutzwürdigkeit spezifischer technischer Fähigkeiten, wie sie der Einsatz bzw. Nicht-Einsatz derartiger Angebote von Datenhändlern und konkreten Anbietern nahelegt, dient der Aufrechterhaltung effektiver Arbeitsfähigkeit. Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages kommt angesichts ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der technischen Aufklärung für die Aufgabenerfüllung nicht in Betracht. Auch ein geringfügiges Risiko des Bekanntwerdens derart sensibler Informationen kann unter keinen Umständen hingenommen werden. Es würde dabei die Gefahr entstehen, dass bestehende oder in der Entwicklung befindliche operative Fähigkeiten und Methoden aufgeklärt würden und damit der Einsatzerfolg gefährdet würde. Auch könnten entsprechende Abwehrstrategien feindlicher Mächte entwickelt werden. Auch dies könnte einen erheblichen Nachteil für die wirksame Aufgabenerfüllung und damit für die (Sicherheits)Interessen der Bundesrepublik Deutschland bedeuten. In der Abwägung des parlamentarischen Informationsrechts der Abgeordneten einerseits und der staatswohlbegründeten Geheimhaltungsinteressen andererseits muss das parlamentarische Informationsrecht daher ausnahmsweise zurückstehen.

Aufgrund entsprechender Formulierung der Fragestellenden beziehen sich Fragen 5-8 darüber hinaus ausdrücklich nicht auf die Nachrichtendienste.

1. *Hält es die Bundesregierung grundsätzlich zur Erfüllung ihrer Aufgaben für angemessen, kommerziell erwerbliche Handy-Standortdaten oder andere personenbezogene Daten von Datenhändlern oder anderen Anbietern zu beziehen (bitte aufgeschlüsselt nach Ressorts einschließlich Bundeskanzleramt und nachgeordneter Behörden inklusive Geheimdienste beantworten)?*

Zu 1. Die Bundesregierung schließt nicht aus, dass der Bezug von personenbezogenen Daten von Datenhändlern im Einzelfall zur Erfüllung ihrer Aufgaben angemessen sein

kann. Dies muss im jeweiligen Einzelfall unter Berücksichtigung der jeweiligen Rechtslage individuell geprüft werden.

2. *Wird systematisch erfasst und für interne Analysen aufbereitet, wie oft und in welchem Kontext die Bundesregierung derartige Quellen gegebenenfalls für ihre Arbeit nutzt und wenn ja, welche Ergebnisse aus der Erfassung kann die Bundesregierung öffentlich bekanntgeben?*

Zu 2. Innerhalb der Bundesregierung erfolgt keine derartige systematische Erfassung.

3. *Wie begründet die Bundesregierung, dass laut Gesetzesbegründung zu §10a im Entwurf des BND-Gesetzes (Bundestagsdrucksache 20/8627) kommerziell gehandelte personenbezogene Daten, zum Beispiel der umfängliche Ankauf solcher Daten aus Webdatenbanken, als Informationen aus allgemein zugänglichen Quellen einzustufen seien, und sollte sich die Bundesregierung dieser Gesetzesbegründung nicht anschließen, aus welchen Gründen nicht?*

Zu 3. Zur Begründung, warum aus Sicht der Bundesregierung kommerziell gehandelte personenbezogenen Daten als Informationen aus allgemein zugänglichen Quellen einzustufen sind, verweist die Bundesregierung auf die Gesetzesbegründung zu § 10 a des Entwurfs eines Gesetzes zur Änderung des Gesetzes über den Bundesnachrichtendienst (BT-Drucksache 20/8627, dort Seite 42).

4. *Wie prüft die Bundesregierung bei der Nutzung personenbezogener Daten aus kommerziellen Quellen die Rechtmäßigkeit der Erhebung dieser Daten (bitte gegebenenfalls auf behördenspezifische Unterschiede eingehen)?*

Zu 4. Die Beurteilung der Rechtmäßigkeit der Datenverarbeitung durch die verantwortlichen Stellen, obliegt den unabhängigen Datenschutzaufsichtsbehörden, auf deren Einschätzung die Bundesregierung keinen Einfluss hat. Darüber hinaus unterliegt die Nutzung personenbezogener Daten durch öffentliche Stellen den allgemeinen oder besonderen (datenschutz)rechtlichen Vorgaben, ungeachtet der Frage, ob diese von einem kommerziellen Anbieter erhoben wurden oder nicht. Hier sind neben der Datenschutz-Grundverordnung auch speziellere Vorgaben (z. B. solche des Bundesdatenschutzgesetzes bzw. der Strafprozessordnung) maßgeblich.

5. *Bezieht oder bezog die Bundesregierung Handy-Standortdaten oder andere personenbezogene Daten von den Unternehmen Datarade, Datastream Group, Datasys, Gravy Analytics, Unacast, Irys, Huq Industries, GapMaps, Azira, Start.io, Sovereign Intelligence, PREDIK, Quadrant, Veraset oder anderen Unternehmen der Online-Werbeindustrie und Datenhändlern und wenn ja, welche Behörden*
- a) *beziehen oder bezogen Daten welcher Unternehmen,*
 - b) *bezogen Daten in welchem Zeitraum,*
 - c) *nutzten die Daten in welchem Zeitraum und*
 - d) *wendeten welche Geldbeträge für den Bezug der Daten auf (bitte aufgeschlüsselt nach Ressorts einschließlich Bundeskanzleramt und nachgeordneter Behörden exklusive der Geheimdienste beantworten)?*

Zu 5. Die Fragen 5a bis 5d werden im Sachzusammenhang beantwortet. Der unter d) umfasste Zeitraum wird auf 2021 bis 2025 festgelegt. Auf die Vorbemerkung der Bundesregierung wird verwiesen.

Ressort	Behörde	a)	b)	c)	d)
BMI	BKG	infas360 GmbH,data analytics institute AG, Content Intelligence Services UG (haftungsbeschränkt), ArztData AG	2020-2025 (vo-raussichtlich bis 2028)	Nutzung der Daten seit 2020	2021: 30.780 € 2022: 29.980 € 2023: 28.980 € 2024: 28.980 € 2025: 24.950 €

6. *Nutzt oder nutzte die Bundesregierung Angebote zur Aufbereitung von Handy-Standortdaten oder anderen personenbezogenen Daten, insbesondere Tangles (Penlink / Cobwebs),*

Webloc (Penlink / Cobwebs), Sherlock (Insanet), Locate X (Babel Street), Cognyte (Bsightful), Echo (Rayzone), AdHoc (Intelos), Havoc (Intelos), Horizon Investigate (ShadowDragon) oder von anderen Unternehmen und wenn ja, welche Behörden

- a) *nutzen oder nutzen derartige Angebote welcher Unternehmen,*
- b) *nutzen Angebote in welchem Zeitraum,*
- c) *wendeten welche Geldbeträge für Nutzung der aufbereiteten Daten auf (bitte aufgeschlüsselt nach Ressorts einschließlich Bundeskanzleramt und nachgeordneter Behörden exklusive der Geheimdienste beantworten)?*

Zu 6. Die Fragen 6a bis 6c werden im Sachzusammenhang beantwortet. Der unter c) umfasste Zeitraum wurde auf 2021 bis 2025 festgelegt. Auf die Vorbemerkung der Bundesregierung wird hingewiesen. Es erfolgt keine Nutzung von Angeboten zur Aufbereitung von Handy-Standortdaten oder anderen personenbezogenen Daten durch dort nicht genannte Behörden.

7. *Nimmt oder nahm die Bundesregierung Dienste von Unternehmen in Anspruch, die die Nutzung von Handy-Standortdaten oder anderen personenbezogenen Daten ermöglichen, insbesondere von Penlink, Cobwebs, Babel Street, ShadowDragon, Insanet, Intelos, Rayzone, Bsightful, Anomaly 6, Venntel, X-Mode oder von anderen Unternehmen und wenn ja, welche Behörden*

- a) *nutzen oder nutzen derartige Dienste welcher Unternehmen,*
- b) *nutzen diese Dienste in welchem Zeitraum,*
- c) *haben sich über Angebote welcher dieser Dienste informiert,*
- d) *wendeten welche Geldbeträge für Nutzung dieser Dienste auf (bitte aufgeschlüsselt nach Ressorts einschließlich Bundeskanzleramt und nachgeordneter Behörden exklusive der Geheimdienste beantworten)?*

Zu 7.

Ressort	Behörde	a)	b)	c)	d)
BMI	BBK	Google und Apple	Seit 2016	Siehe a	keine

8. *Welche Kontakte hatte die Bundesregierung (bitte aufgeschlüsselt nach Ressorts einschließlich Bundeskanzleramt und nachgeordneter Behörden exklusive der Geheimdienste beantworten) zu jeweils welchem Zeitpunkt seit der 20. Wahlperiode mit Unternehmen, die Handy-Standortdaten oder andere personenbezogene Daten kommerziell anbieten (bitte*

den Anlass des Kontaktes danach sortierten, ob es um Interesse der Bundesregierung an Angeboten dieser Unternehmen ging, oder ob es Kontakte ohne derartige Absichten waren)?

- Zu 8. Die Bundesregierung versteht die Fragestellung dahingehend, dass nach Gesprächen/Kontakten der Leitungsebene der Ministerien und der Geschäftsbereichsbehörden gefragt ist. Die Mitglieder der Bundesregierung, Parlamentarische Staatssekretärinnen und Parlamentarische Staatssekretäre bzw. Staatsministerinnen und Staatsminister sowie Staatssekretärinnen und Staatssekretäre pflegen in jeder Wahlperiode im Rahmen der Aufgabenwahrnehmung Kontakte mit einer Vielzahl von Akteuren aller gesellschaftlichen Gruppen. Unter diesen ständigen Austausch fallen Gespräche und auch Kommunikation in anderen Formen (schriftlich, elektronisch, telefonisch). Es ist weder rechtlich geboten noch im Sinne einer effizienten und ressourcenschonenden öffentlichen Verwaltung leistbar, entsprechende Informationen und Daten (z. B. sämtliche Veranstaltungen, Sitzungen und Termine nebst Teilnehmerinnen und Teilnehmern) vollständig zu erfassen oder entsprechende Dokumentationen darüber zu erstellen oder zu pflegen. Da insbesondere eine Gesamtübersicht nicht durch eine einfache technische Auswertung zusammengestellt werden kann und die durchgeführte händische Ressort- und Behördenweite Recherche zur Beantwortung stets nur mit Blick auf einen zumutbaren Zeitaufwand und anhand der verfügbaren Quellen erfolgen kann, wurde bei der Recherche das Besondere – aber nicht abschließende – Interesse der Fragestellenden nach Kontakten zu den unter Frage 6 und 7 genannten Unternehmen angenommen.

Unter Beachtung dieser Maßgaben hatte die Bundesregierung keine Kontakte im Sinne der Frage.

9. *Ist nach Auffassung der Bundesregierung der Handel mit personenbezogenen Daten zum Selbstzweck, also deren Nutzung als Handelsware, mit dem Datenschutzrecht unvereinbar, so wie es das Bundesministerium für Umwelt und Verbraucherschutz im Juli 2024 gegenüber Netzpolitik.org äußerte (<https://netzpolitik.org/2024/databroker-files-us-senator-schaltet-pentagon-ein-bundesministerium-fordert-eu-gesetze/>)?*
10. *Welche Maßnahmen plant die Bundesregierung, um die Wahrung der informationellen Selbstbestimmung hinsichtlich des Handels personenbezogener Daten zu Werbezwecken zu verbessern?*

Zu 9 und 10: Die Frage 9 und 10 werden im Sachzusammenhang beantwortet. Die Bundesregierung verweist auf ihre Antwort zur Schriftlichen Frage des Abgeordneten Dr. Konstantin von Notz auf Bundestagsdrucksache 21/1709, Nr. 36. Ergänzend wird hinsichtlich Frage 9

darauf hingewiesen, dass sich die Äußerung des damaligen Bundesministeriums für Umwelt und Verbraucherschutz im Juli 2024 auf die Gemeinsame Stellungnahme 02/2022 des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten bezog: Nach deren Rz. 15 würde eine Behandlung von personenbezogenen Daten lediglich als handelbare Ware „nicht nur den eigentlichen Begriff der Menschenwürde und den von der EU in ihrer Datenstrategie verfolgten Ansatz, der den Menschen in den Mittelpunkt stellt, untergraben, sondern auch Gefahr laufen, die Grundrechte auf Rechte auf Schutz der Privatsphäre und auf Datenschutz zu untergraben“. Darüber hinaus weist die Bundesregierung auf die Mitteilung der Europäischen Kommission an das Europäische Parlament und den Rat vom 19. November 2025 zur Strategie für eine Datenunion und zur Verfügbarkeit von Daten für künstliche Intelligenz hin (COM[2025] 835 final) hin. Darin stellt die Kommission fest, dass der Handel mit Daten zunehmend Anlass zur Sorge gibt, da einige Unternehmen personenbezogene Daten ohne Wissen, ausdrückliche Einwilligung oder Kontrolle der Betroffenen sammeln, zusammenführen und damit handeln. Solche intransparenten Praktiken untergraben grundlegende Prinzipien des Datenschutzrechts und der Privatsphäre, verzerren den Wettbewerb und zerstören das Vertrauen der Öffentlichkeit in digitale Märkte. Insofern hält die Kommission im Hinblick auf intransparente Praktiken des Datenhandels eine verstärkte Durchsetzung der bestehenden Vorschriften für erforderlich und kündigt an, zu prüfen, ob zusätzliche Schutzmaßnahmen notwendig sind, um diese Praktiken einzudämmen, die Transparenz im Datenhandel zu erhöhen und sicherzustellen, dass Einzelpersonen und Unternehmen darauf vertrauen können, wie Daten in der Union abgerufen und ausgetauscht werden.

11. Welche Maßnahmen ergriff oder gedenkt die Bundesregierung zu ergreifen seit Bekanntwerden der eingangs beschriebenen Recherchen von BR/ARD und Netzpolitik.org, um einer möglichen Gefährdung der nationalen Sicherheit durch Data Broker entgegenzuwirken?

Zu 11: Der Erwerb von durch Data Broker gehandelte personenbezogene Daten wie Standortdaten, die individuelle Bewegungsprofile nachzeichnen und hierüber die Identifizierung konkreter Personen zulassen, kann als eine Möglichkeit gesehen werden, wie ausländische Nachrichtendienste Aufklärung betreiben. Dieses Aufklärungsinteresse ausländischer Nachrichtendienste richtet sich hierbei auch gegen Berufsgruppen, die in sicherheitsrelevanten oder politisch herausgehobenen Bereichen arbeiten.

Eine Beeinträchtigung der nationalen Sicherheit kann in Abhängigkeit des individuellen Falls hierbei nicht vollständig ausgeschlossen werden. Allerdings ist darauf hinzuweisen, dass ausländischen Nachrichtendiensten die Ermittlung von Aufenthalts- und Wohnorten relevanter Personen auch mit klassischen, analogen Mitteln, z. B. durch Nachverfolgung, schon immer möglich ist.

Die Bundesregierung ist sich dem umfänglichen Aufklärungsinteresse ausländischer Nachrichtendienste, das alle Möglichkeiten der Informationsbeschaffung umfasst, bewusst.

Die Bundesregierung sensibilisiert die Beschäftigten relevanter Behörden und Einrichtungen zu den Risiken, die mit den von Data Brokern gesammelten personenbezogenen Daten einhergehen und gibt Tipps zur Konfigurierung privater und dienstlicher IT. Weiter wird auf die Antwort der Bundesregierung zur Schriftlichen Frage des Abgeordneten Dr. Konstantin von Notz auf Bundestagsdrucksache 21/1709, Nr. 36 verwiesen.