



Sachstand

Verarbeitung personenbezogener Daten durch die Polizei Rechtsgrundlage in den deutschen Nachbarländern

Verarbeitung personenbezogener Daten durch die Polizei
Rechtsgrundlage in den deutschen Nachbarländern

Aktenzeichen: WD 3 - 3000 - 162/21
Abschluss der Arbeit: 22.10.2021
Fachbereich: WD 3: Verfassung und Verwaltung

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

1. Fragestellung

Der Sachstand gibt einen Überblick über das für die Datenverarbeitung durch die Polizei einschlägige Recht in Deutschland, den Niederlanden, Belgien, Luxemburg, Frankreich, Österreich, Tschechien und Polen in Bezug auf die Datenverarbeitung durch die Polizei.

Das Datenschutzrecht ist auf europäischer Ebene durch die Datenschutz-Grundverordnung (DSGVO)¹ und die Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zweck der Strafverfolgung und Strafvollstreckung (JI-Richtlinie)² geregelt. Die Verordnung und die Richtlinie sind inhaltlich aufeinander abgestimmt und wurden gemeinsam verabschiedet. Die DSGVO gilt dabei grundsätzlich für alle Arten von Datenverarbeitung, soweit ihre Anwendbarkeit nicht nach Art. 2 Abs. 2 bis 4 DGSVO ausgeschlossen ist. Der Anwendungsbereich der JI-Richtlinie entspricht der Ausnahme des Art. 2 Abs. 2 d) DGSVO, welcher die Verarbeitung durch die zuständigen Behörden 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 umfasst.

2. Deutschland

Vorrangig richtet sich der Datenschutz in Deutschland nach den europäischen Vorschriften. Die JI-Richtlinie wurde durch **Teil 3 des neuen Bundesdatenschutzgesetzes (BDSG)³ von 2017** umgesetzt.

Unter den Anwendungsbereich des BDSG fallen nach § 1 BDSG die **Polizeibehörden des Bundes**, der Generalbundesanwalt beim Bundesgerichtshof sowie die Zollfahndung, soweit sie die Daten zu den genannten Zwecken verarbeiten. Die **Polizeibehörden der Länder**, die Staatsanwaltschaften an den Landgerichten, die Generalstaatsanwaltschaften bei den Oberlandesgerichten und die Steuerfahndung an den Finanzbehörden der Länder, verarbeiten zwar auch personenbezogene Daten zu den in § 45 BDSG genannten Zwecken und führen zum Teil auch Bundesrecht aus. Als öffentliche Stellen der Länder gelten für sie aber nach § 1 Abs. 1 UAbs. 1 Nr. 2 BDSG die **Datenschutzgesetze der Länder**.

Erheben Polizei- und Justizbehörden personenbezogene Daten zu den genannten Zwecken beziehungsweise verarbeiten oder nutzen sie diese, sind zudem die jeweiligen spezialgesetzlichen Vorschriften zu beachten. Dazu zählen die Vorschriften in den **Polizeigesetzen der Länder** und **des Bundes** sowie der **Strafprozessordnung**, die vielfach von den Landesdatenschutzgesetzen bezie-

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

2 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

3 Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das durch Artikel 10 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist.

ungsweise dem Bundesdatenschutzgesetz abweichen. Neben Generalklauseln zur Erhebung personenbezogener Daten regeln die Polizeigesetze und die Strafprozessordnung spezielle Maßnahmen der Datenerhebung, -verarbeitung und -nutzung. Diese müssen eine bereichsspezifische und normenklare Bestimmung des Anlasses und des Verwendungszwecks enthalten, um verfassungsmäßig zu sein.

§ 45 BDSG bestimmt den **Anwendungsbereich** von Teil 3. Danach muss eine **Verarbeitung personenbezogener Daten** durch die für die **Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen**, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten, erfolgen. Unter Verarbeitung fällt gemäß § 46 Nr. 2 BDSG jeder Datenumgang mit personenbezogenen Daten unabhängig vom Medium oder der Speicherart. Dazu gehören neben automatisierten und computergestützten Verfahren auch analoge und sonstige Verfahren, unabhängig davon, ob die Speicherung in einem Datei- oder Ablagesystem erfolgt oder erfolgen soll.

3. Belgien

In Belgien wurde die JI-Richtlinie in nationales Recht umgesetzt durch Titel 2 des **Gesetzes vom 30. Juli 2018 über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten**.⁴ Art. 27 definiert den Anwendungsbereich als die Verarbeitungen personenbezogener 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. In Abs. 7 des Art. 26 werden die zuständigen Behörden abschließend aufgelistet, Abs. 2 definiert den Begriff „Verarbeitung persönlicher Daten“ sehr weit. Die Datenverarbeitung muss dabei den Grundsätzen aus Art. 5 DSGVO genügen.

Art. 71 des Gesetzes hat zudem eine unabhängige Kontrollstelle für polizeiliche Informationen eingesetzt, die die Verarbeitung von Informationen und persönlichen Daten überwacht und dem Repräsentantenhaus berichten soll.

Eine Verarbeitung und Speicherung persönlicher Daten durch die Polizei erfolgt zudem aufgrund des **Gesetzes über das Polizeiamt vom 5. August 1992**. Dieses regelt insbesondere die Führung von polizeilichen Datenbanken. Einschlägig sind ferner das **Gesetz zur integrierten Polizei vom 7. Dezember 1998** sowie das Strafprozessrecht einschließlich damit in Zusammenhang stehender weitere Gesetze.

4. Dänemark

In Dänemark wurde die JI-Richtlinie durch das **Strafverfolgungsgesetz von 2017** in nationales Recht umgesetzt. Eine Verarbeitung personenbezogener Daten, die über die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung hinausgeht, fällt unter die **DSGVO** beziehungsweise das **Dänische Datenschutzgesetz**.

4 Die inoffizielle Koordinierung in deutscher Sprache des Gesetzes vom 30. Juli 2018 über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten ist abrufbar unter http://www.ejus-tice.just.fgov.be/mopdf/2021/03/30_1.pdf#Page9.

5. Frankreich

Das wichtigste Gesetz in Frankreich bezüglich des Umgangs der Polizei mit Daten ist das Gesetz Nummer 78-17 vom 6. Januar 1978 zu Datenverarbeitung, Akten und Freiheiten, auch bekannt als „Informations- und Freiheitsgesetz“. Diesem Gesetz entsprechend wurde eine nationale Datenschutzbehörde aufgebaut, die „Commission Nationale Informatique et Libertés“. Deren Aufgabe ist es, der Regierung öffentliche Stellungnahmen zu Gesetzesentwürfen mit Bezug zu elektronischen Akten bereitzustellen. So soll sichergestellt werden, dass der Schutz öffentlicher Freiheiten mit der Erreichung eines legitimen Ziels wie der Bekämpfung von Terrorismus oder Drogenhandel in Ausgleich gebracht wird.

Das Gesetz Nummer 78-17 vom 6. Januar 1978 wurde geändert, um die DSGVO und die JI-Richtlinie umzusetzen. Artikel 97 bis 103 beinhalten die Pflichten der zuständigen Behörden und der für die Verarbeitung zuständigen Stellen, Artikel 104 bis 111 bezeichnen die Rechte der Person, deren Daten verarbeitet werden.

6. Luxemburg

Die Umsetzung der JI-Richtlinie erfolgte durch das Gesetz vom 1. August 2018 zum Schutz natürlicher Personen bezüglich der Verarbeitung ihrer persönlichen Daten in Strafsachen sowie im Bereich der nationalen Sicherheit. Daneben gilt die DSGVO.

Ein nationales Gesetzesvorhaben mit der Kennung PL 7741, das auf eine bessere Regulierung des Umgangs mit Polizeiakten abzielt, wurde im Dezember 2020 vorgestellt und soll im Jahr 2022 abgestimmt werden.

7. Österreich

Das durch das Datenschutz-Anpassungsgesetz novellierte **Datenschutzgesetz in der Form vom 25. Mai 2018 (DSG)** ist die umfangreichste nationale Rechtsgrundlage und stellt die Umsetzung der JI-Richtlinie dar. Für die Polizei sind die §§ 36-61 DSG (= 3. Hauptstück) hervorzuheben, da dieses die Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs regeln.

Es gibt darüber hinaus auf nationaler Ebene weitere Gesetze und Verordnungen mit einer Vielzahl einzelner Bestimmungen zum Datenschutz, welche von der Polizei beachtet werden müssen, zum Beispiel §§ 13a, 53 und 58c des Sicherheitspolizeigesetzes.

8. Polen

Auch Polen hat die JI-Richtlinie umgesetzt durch das Gesetz vom 14. Dezember 2018 zum Schutz persönlicher Daten bei Verarbeitung zum Zweck der Strafprävention und Strafverfolgung und dadurch das Polizeigesetz vom 6. April 1990 geändert. Nach dessen Art. 20 Abs. 1 darf die Polizei Daten, auch personenbezogene Daten, unter den Beschränkungen des Art. 19 verarbeiten. Danach können persönliche Daten, die im Rahmen einer operativen Maßnahme gesammelt werden, nur mit Erlaubnis des für die anfragende Polizeibehörde zuständigen Amtsgerichts gespeichert und verarbeitet werden. Ist Gefahr im Verzug, kann ein solches Vorgehen auch vom Polizeipräsidenten,

vom Leiter der zentralen Anti-Korruptionsbehörde, dem Leiter der Behörde für Innere Angelegenheiten der Polizei oder dem örtlichen Polizeichef angeordnet werden, vorausgesetzt der zuständige Staatsanwalt hat schriftlich zugestimmt und eine Entscheidung beim zuständigen Amtsgericht wurde gleichzeitig beantragt.

Operative Maßnahmen können eingesetzt werden bei Verbrechen gegen das Leben und die Gesundheit, sexuelle Freiheit und Sittlichkeit, wenn das Opfer minderjährig ist, bei Wirtschaftskriminalität und anderen Straftaten mit hoher Strafandrohung, die im Gesetz ausdrücklich aufgeführt werden.

Zu den Maßnahmen gehören das Verschaffen und Aufnehmen des Inhalts von Unterhaltungen, die mit technischen Mitteln geführt werden inklusive Telekommunikationsnetzwerken, von Bildern oder Audioaufnahmen von Personen auf Grundstücken, in Verkehrsmitteln oder an anderen nicht-öffentlichen Orten, des Inhalts von Schriftverkehr inklusive elektronischer Kommunikation, von Daten auf Computerdatenträgern, Telekommunikationsendgeräten, IT- und ITC-Systemen sowie das Erhalten von Zugang zu und der Kontrolle vom Inhalt von Post.

Die Vorschriften des Polizeigesetzes verweisen darauf, dass der Austausch und die Verarbeitung von Informationen persönliche Daten, auf die sich Artikel 14 Abs. 1 des Gesetzes vom 14. Dezember 2018 bezieht, betreffen kann. Daten bezüglich des Ergebnisses einer DNA-Analyse hingegen beinhalten lediglich Informationen über den nicht codierenden Teil der DNA.

Artikel 20 Abs. 1c bestimmt, dass die Polizei Informationen inklusive persönlicher Daten zum Zweck der Erfüllung der ihr gesetzlich übertragenen Aufgaben, zur Erfüllung anderer öffentlicher Pflichten und im Rahmen ihrer Beteiligung an Verwaltungsverfahren verarbeiten darf.

Die Polizei darf darüber hinaus unter den Voraussetzungen der Strafprozessordnung vom 6. Juni 1997 und des Strafgesetzes persönliche Daten aufnehmen.

9. Tschechien

Die Umsetzung der JI-Richtlinie in tschechisches Recht erfolgte hauptsächlich durch das **Gesetz über den Strafprozess (Gesetzblatt Nr. 141/1861)** und das **Gesetz über die Polizei der Tschechischen Republik (Gesetzblatt Nr. 273/2008)**, insbesondere dessen §§ 79 bis 88b. Eine Datenverarbeitung darf danach nur zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung erfolgen.

Eine Datenverarbeitung durch die Staatspolizei aus den in Art. 6 Abs. 1 lit. c und e DSGVO aufgeführten Gründen wird durch § 2 und § 60 des Gesetzes über die Polizei der Tschechischen Republik (Gesetzblatt Nr. 273/2008) geregelt, ferner durch das Aufenthaltsgesetz der Tschechischen Republik (Gesetzblatt Nr. 326/1999), das Asylgesetz (Gesetzblatt Nr. 325/1999) und das Waffen- und Munitionsgesetz (Gesetzblatt Nr. 119/2002). Die Datenverarbeitung soll die Aufgabenerfüllung der Verwaltung ermöglichen, insbesondere im Bereich der Waffen und Munition, der Einreise und des Aufenthalts von Ausländern auf dem Gebiet der Tschechischen Republik oder des Asylverfahrens. Auch die Gemeindepolizei darf personenbezogene Daten auf Grundlage der DGSVO sowie nach dem Gesetz über die Gemeindepolizei (Gesetzblatt Nr. 553/1991) verarbeiten.
