Sachstand

Extremistendateien in Deutschland

Aktualisierung des Sachstands WD 3 - 3000 - 149/17

Extremistendateien in Deutschland
Aktualisierung des Sachstands WD 3 - 3000 - 149/17

Aktenzeichen: WD 3 - 3000 - 070/22
Abschluss der Arbeit: 23.05.2022
Fachbereich: WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Einleitung

Erbeten wurde eine Aktualisierung des Sachstands WD 3 - 3000 - 149/17 aus dem Jahr 2017. Der Sachstand gibt einen Überblick über die Regelungen zu den in Deutschland geführten Extremistendateien bei Polizei- und Verfassungsschutzbehörden. Es werden die einzelnen Dateien, die Art der gespeicherten Daten, die Löschung der Daten sowie die Zuständigkeit der Kontrollorgane dargestellt.

Der Sachstand wurde im Wesentlichen um die Rechtsgrundlagen ergänzt, die Art der gespeicherten Daten konkretisiert und die datenschutzrechtliche Kontrolle in Bezug auf das „nachrichtendienstliche Informationssystem und Wissensnetz“ klargestellt.

2. Antiterrordatei

Die **Antiterrordatei (ATD)** vernetzt Erkenntnisse von Polizeien und Nachrichtendiensten des Bundes und der Länder aus dem Bereich des internationalen Terrorismus. Sie wird beim Bundeskriminalamt (BKA) geführt und ermöglicht den beteiligten Behörden einen schnellen Informationsüberblick.[1]

Die **Rechtsgrundlage** für die Errichtung der Antiterrordatei findet sich im Antiterrordateigesetz (ATDG).[2]

Zugriff auf die Antiterrordatei haben neben dem BKA die Bundespolizeidirektion, die Landeskriminalämter, die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst und das Zollkriminalamt, § 1 Abs. 1 ATDG. Auf Ersuchen der Länder kann der Bundesminister des Innern unter den Voraussetzungen von § 1 Abs. 2 ATDG durch Rechtsverordnung auch den Zugriff von Landespolizeivollzugsbehörden zulassen.

Das ATDG unterscheidet bei einer **Speicherung** von Daten zwischen „Grunddaten“ und „erweiterten Grunddaten“, § 3 Abs. 1 Nr. 1 ATDG. Grunddaten werden direkt angezeigt und liefern auf den ersten Blick die erforderlichen Informationen, um eine gesuchte Person zu identifizieren, z. B. Namen, Aliaspersonalien, abweichende Namensschreibweisen, Geschlecht, Geburtsdatum, Lichtbilder. Außerdem wird angezeigt, welche anderen Behörden ebenfalls über Informationen zu dieser Person verfügen. Erweiterte Grunddaten sind z. B. die genutzten Telekommunikationsanschlüsse, E-Mail-Adressen, Bankverbindungen, Schließfächer. Sie sind nur sichtbar, wenn die Behörde sie freischaltet, die die Daten in der ATD gespeichert hat. Daten können ausnahmsweise auch beschränkt oder verdeckt gespeichert werden, wenn besondere Geheimhaltungsinteressen oder besonders schutzwürdige Interessen des Betroffenen dies erfordern, § 4 ATDG. Unter welchen Voraussetzungen die o.g. Behörden berechtigt und sogar verpflichtet sind, erhobene Daten in der ATD zu speichern, ist in § 2 ATDG geregelt.

---

1 Bundeskriminalamt, Datenbestand und Nutzung der Antiterrordatei (ATD) und der Rechtsextremismus-Datei (RED), abrufbar unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Antiterrordatei-Rechtsextremismusdatei/antiterrordateiRechtsextremismusdatei_node.html.

2 Antiterrordateigesetz vom 22. Dezember 2006 (BGBl. I S. 3409), zuletzt geändert durch Artikel 2 Absatz 1 des Gesetzes vom 30. März 2021 (BGBl. I S. 402).

Personenbezogene Daten sind durch die Behörde, die die Daten eingegeben hat, zu **löschen**, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die Aufklärung oder Bekämpfung des internationalen Terrorismus nicht mehr erforderlich ist, § 11 Abs. 2, 4 ATDG.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) und die Landesdatenschutzbeauftragten sind für die **datenschutzrechtliche Kontrolle** der ATD zuständig, § 10 Abs. 1 ATDG.

3. Rechtsextremismus-Datei

Die **Rechtsextremismusdatei (RED)** ist beim BKA installiert und schafft eine Vernetzung deutscher Sicherheitsbehörden im Kampf gegen den gewaltbezogenen Rechtsextremismus. Neben dem BKA arbeiten das Bundesamt für Verfassungsschutz, der Militärische Abschirmdienst, die Bundespolizei sowie die Landeskriminalämter und Landesbehörden für Verfassungsschutz mit der RED.[3]

Die **Rechtsgrundlage** für die Rechtsextremismusdatei findet sich im Rechtsextremismus-Datei-Gesetz (RED-G).[4]

Ähnlich wie bei der ATD wird bei der **Speicherung** zwischen „Grunddaten“ und „erweiterten Grunddaten“ unterschieden. Hierzu werden von Personen mit rechtsextremistischem Hintergrund z. B. Namen, Aliaspersonalien, abweichende Namensschreibweisen, Geschlecht, Geburtsdatum und Geburtsort als Grunddaten erfasst, § 3 Abs. 1 Nr. 1 lit. a RED-G. Als erweiterte Grunddaten werden z. B. genutzte Telekommunikationsanschlüsse, E-Mail-Adressen, Bankverbindungen, Schließfächer, Familienstand und besondere Kenntnisse und Fertigkeiten in der Herstellung oder im Umgang mit Sprengstoffen oder Waffen gespeichert, § 3 Abs. 1 Nr. 1 lit. b RED-G. Daten können aus Geheimhaltungsgründen ausnahmsweise auch beschränkt oder verdeckt gespeichert werden, § 4 Abs. 1 RED-G. Unter welchen Voraussetzungen die Sicherheitsbehörden verpflichtet sind, erhobene Daten in der RED zu speichern, regelt § 2 RED-G.

Personenbezogene Daten sind durch die Behörde, die die Daten eingegeben hat, zu **löschen**, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus, insbesondere zur Verhinderung und Verfolgung von Straftaten mit derartigem Hintergrund, nicht mehr erforderlich ist, § 12 Abs. 2, 4 RED-G.

Für die **datenschutzrechtliche Kontrolle** der RED ist der BfDI zuständig, § 11 Abs. 1 Satz 1 RED-G. Soweit die Länder für eigegebene Datensätze verantwortlich sind, können diese auch durch die Landesdatenschutzbeauftragten kontrolliert werden, § 11 Abs. 1 Satz 2 RED-G. Die Landesdatenschutzbeauftragten und der BfDI arbeiten insoweit zusammen, § 11 Abs. 1 Satz 3 RED-G.

---

3 Bundeskriminalamt, Datenbestand und Nutzung der Antiterrordatei (ATD) und der Rechtsextremismus-Datei (RED), abrufbar unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/AntiterrordateiRechtsextremismusdatei/antiterrordateiRechtsextremismusdatei_node.html.

4 Rechtsextremismus-Datei-Gesetz vom 20. August 2012 (BGBl. I S. 1798), zuletzt geändert durch Artikel 2 Absatz 2 des Gesetzes vom 30. März 2021 (BGBl. I S. 402).

4. INPOL

Bei INPOL handelt es sich um das beim BKA angesiedelte **elektronische Informationssystem der Polizei (INPOL)**. Zugriff auf INPOL haben neben dem BKA die Landespolizeidienststellen, die Bundespolizei und die Zollbehörden.[5]

INPOL ist eine auf **Grundlage** von § 13 i.V.m. §§ 29, 30 Bundeskriminalamtgesetz (BKAG)[6] errichtete Verbunddatei des einheitlichen polizeilichen Informationsverbunds. Das BKA ist gemäß § 2 Abs. 3 BKAG Zentralstelle des Informationsverbundes und führt sog. Zentralstellendateien.[7] Diese können als Verbund- oder Zentraldateien den Verbundteilnehmern von INPOL zur Verfügung gestellt werden. Das BKA entscheidet, ob eine Datei in INPOL eingebunden wird. Eingebundene Verbund- und Zentraldateien unterscheiden sich durch die Zugriffsberechtigung. Während in Verbunddateien die Daten unmittelbar von den Verbundteilnehmern eingegeben und im automatisierten Verfahren abgerufen werden können, können Daten aus Zentraldateien nur im automatisierten Abrufverfahren abgerufen werden. Bei INPOL befinden sich u. a. die Verbunddateien „Gewalttäter rechts“ und „Gewalttäter links“ sowie „Gewalttäter politisch motivierte Kriminalität – religiöse Ideologie“, „Gewalttäter politisch motivierte Kriminalität – ausländische Ideologie“ und „Gewalttäter politisch motivierte Kriminalität – nicht zuzuordnen“.[8] Die an INPOL teilnehmenden Stellen geben Daten in eigener Verantwortlichkeit in die Verbunddateien ein.[9]

Eine **Speicherung** von personenbezogenen Daten und Kenntnissen kann gemäß § 18 Abs. 1 BKAG erfolgen über

– Verurteilte,

– Beschuldigte,

– Personen, die einer Straftat verdächtig sind, sofern die Weiterverarbeitung der Daten erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind, und

---

5 BKA, Das elektronische Informationssystem der Polizei (INPOL), abrufbar unter: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/ElektronischeFahndungsInformationssysteme/polizeilicheInformationssysteme_node.html.

6 Bundeskriminalamtgesetz vom 1. Juni 2017 (BGBl. I S. 1354; 2019 I S. 400), zuletzt geändert durch Artikel 2 des Gesetzes vom 25. Juni 2021 (BGBl. I S. 2099).

7 Laut der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. zum Stand der Umsetzung des Programms „Polizei 2020“, BT-Drs. 19/15346 (siehe https://dserver.bundestag.de/btd/19/153/1915346.pdf), S. 3 führt das BKA innerhalb der Abteilung Schwere und Organisierte Kriminalität derzeit 116 Zentral- und 32 Verbunddateien.

8 Vgl. BT-Drs. 19/15346 (https://dserver.bundestag.de/btd/19/153/1915346.pdf), S. 3 und dazu Anlage 1 S. 14 f.

9 Graulich, in: Schenke/Graulich/Ruthig, 2. Auflage 2019, BKAG, § 29 Rn. 2.

– Personen, bei denen Anlass zur Weiterverarbeitung der Daten besteht, weil tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffenen Personen in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden (Anlasspersonen).

§ 18 Abs. 2 BKAG legt die Art der Daten fest, die verarbeitet werden dürfen. Danach können zu allen genannten Personen die Grunddaten und, soweit erforderlich, andere zur Identifizierung geeignete Merkmale, die kriminalaktenführende Polizeidienststelle und die Kriminalaktennummer, die Tatzeiten und Tatorte sowie die Tatvorwürfe gespeichert werden, § 18 Abs. 2 Nr. 1 BKAG. § 18 Abs. 2 Nr. 2 und Nr. 3 BKAG bestimmen, unter welchen Voraussetzungen weitere personenbezogene Daten gespeichert werden dürfen. Die BKADV[10] regelt nähere Einzelheiten zu Art und Umfang der nach § 18 Abs. 2 BKAG zu speichernden Daten. So umfassen die „Grunddaten" u. a. Namen, Geschlecht, Geburtsdatum, Geburtsort, Staatsangehörigkeit und Anschrift, § 18 Abs. 1, § 20 Satz 2 Nr. 1 BKAG i.V.m. § 1 Abs. 1 BKADV.

Die Voraussetzungen, unter denen eine Verarbeitung der genannten Daten durch das BKA in INPOL zulässig ist, ergeben sich aus § 16 BKAG. In INPOL dürfen zudem nur personenbezogene Daten verarbeitet werden, die eine sog. Verbundrelevanz aufweisen, § 30 Abs. 1 BKAG.

Gemäß § 77 Abs. 1 Satz 1 BKAG ist bei der Einzelfallbearbeitung und nach festgesetzten Fristen zu prüfen, ob gespeicherte personenbezogene Daten zu berichtigen oder zu **löschen** sind. Die festgelegten Aussonderungsprüffristen dürfen bei Erwachsenen zehn Jahre, bei Jugendlichen fünf Jahre und bei Kindern zwei Jahre nicht überschreiten, wobei nach Zweck der Speicherung sowie Art und Schwere des Sachverhalts zu unterscheiden ist, § 77 Abs. 1 Satz 2 BKAG. Bei Personen, die bei einer künftigen Strafverfolgung als Zeugen oder als Opfer einer künftigen Straftat in Betracht kommen, die mit Verurteilten, Beschuldigten, Tatverdächtigen und sonstigen Anlasspersonen nicht nur flüchtig oder in zufälligem Kontakt stehen oder bei denen es sich um Hinweisgeber und sonstige Auskunftspersonen handelt, dürfen die Aussonderungsprüffristen bei Erwachsenen fünf Jahre und bei Jugendlichen drei Jahre nicht überschreiten, § 77 Abs. 2 Satz 1 Alternative 1 i.V.m. § 19 Abs. 1 BKAG. Bei einer Verfolgung von Straftaten nach den §§ 6 bis 13 des Völkerstrafgesetzbuches dürfen die Aussonderungsprüf-fristen bei Erwachsenen zehn Jahre und bei Jugendlichen fünf Jahre nicht überschreiten, § 77 Abs. 2 Satz 1 Alternative 2 BKAG. Die Behörde, die personenbezogene Daten zu einer Person eingegeben hat, teilt dem BKA die zu löschenden personenbezogenen Daten mit, § 77 Abs. 4 Satz 1 BKAG. Die Löschung unterbleibt, wenn Anhaltspunkte dafür bestehen, dass die Daten für die Aufgabenerfüllung des BKA als Zentralstelle, namentlich bei Vorliegen weitergehender Erkenntnisse, erforderlich sind, es sei denn, auch das BKA wäre zur Löschung verpflichtet, § 77 Abs. 4 Satz 3 BKAG.

Für die **datenschutzrechtliche Kontrolle** von INPOL sind gemäß § 31 Abs. 3 BKAG der BfDI und, soweit die Länder für die eigegebenen Daten verantwortlich sind, auch die Landesdatenschutzbeauftragten zuständig.

---

10 Verordnung über die Art der Daten, die nach den §§ 8 und 9 des Bundeskriminalamtgesetzes gespeichert werden dürfen (BKA-Daten-Verordnung - BKADV) vom 4. Juni 2010 (BGBl. I S. 716), zuletzt geändert durch Art. 6 Abs. 12 G zur Reform der strafrechtlichen Vermögensabschöpfung vom 13. April 2017 (BGBl. I S. 872).

5. NADIS WN

Das **„nachrichtendienstliche Informationssystem und Wissensnetz“** (NADIS WN) ist das zentrale Hinweis- und Verbundsystem der Verfassungsschutzbehörden des Bundes und der Länder für Personen und Objekte.[11]

Die **Rechtsgrundlage** für die Errichtung von NADIS WN findet sich in § 6 Abs. 2 Bundesverfassungsschutzgesetz (BVerfSchG).[12]

Neben den Verfassungsschutzbehörden des Bundes und der Länder ist auch der Militärische Abschirmdienst berechtigt, auf die in NADIS WN verfügbaren Daten zuzugreifen, § 6 Abs. 2 Satz 2 BVerfSchG i.V.m. § 3 Abs. 3 des Gesetzes über den Militärischen Abschirmdienst (MADG)[13]. Das Bundesamt für Verfassungsschutz (BfV) stellt NADIS WN im Rahmen seiner Zentralstellenfunktion bereit, § 5 Abs. 4 Nr. 1 BVerfSchG.

In NADIS WN übermitteln sich die Verfassungsschutzbehörden alle Informationen, die für die Erfüllung ihrer Aufgaben *relevant* sind, einschließlich der Erkenntnisse ihrer Auswertungen, § 6 Abs. 1 BVerfSchG. Der Militärische Abschirmdienst und die Verfassungsschutzbehörden unterrichten einander mittels NADIS WN über alle Angelegenheiten, deren Kenntnis für die Erfüllung ihrer Aufgaben *erforderlich* ist, § 3 Abs. 3 Satz 1 MADG. Die Art der in NADIS WN **gespeicherten** personenbezogenen Daten ist im BVerfSchG nicht weiter eingegrenzt. Gespeichert werden sowohl Freitexte als auch sonstige Daten wie etwa Bilder und Videodateien. Es handelt sich mithin nicht um eine bloße Hinweisdatei zum Auffinden von Akten oder zur Identifizierung von Personen.[14]

Die jeweiligen Verfassungsschutzbehörden tragen für die von ihnen eingegebenen Daten die Verantwortung; nur sie dürfen diese Daten verändern, die Verarbeitung einschränken oder **löschen**, § 6 Abs. 2 Satz 5 BVerfSchG. So hat das BfV die von ihm in NADIS WN gespeicherten personenbezogenen Daten zu löschen, wenn ihre Speicherung unzulässig war oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist, § 12 Abs. 2 Satz 2 BVerfSchG. Spätestens nach fünf Jahren muss das BfV überprüfen, ob gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind, § 12 Abs. 3 Satz 1 BVerfSchG. Das Speichern von Daten oder Informationen über das Verhalten von Minderjährigen vor Vollendung des 14. Lebensjahres in Dateien ist nicht zulässig, § 11 Abs. 1 Satz 2 BVerfSchG. Die Überprüfung der gespeicherten Daten über Minderjährige nach Vollendung des 14. Lebensjahres unterliegt kürzeren Fristen, § 11 Abs. 2 BVerfSchG.

---

11 BT-Drs. 18/5659 S. 12; siehe auch Bundesamt für Verfassungsschutz, Die Zentralstelle, abrufbar unter: https://www.verfassungsschutz.de/DE/verfassungsschutz/verfassungsschutzverbund/zentralstelle/zentralstelle_artikel.html.

12 Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Artikel 1 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2274).

13 Gesetz über den Militärischen Abschirmdienst vom 20. Dezember 1990 (BGBl. I S. 2954), zuletzt geändert durch Art. 2 Gesetz zur Anpassung des Verfassungsschutzrechts vom 5. Juli 2021 (BGBl. I S. 2274).

14 Bergemann, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Auflage 2021, Kap. H. Rn. 118.

Da gemäß § 6 Abs. 2 Satz 5 BVerfSchG jede Verfassungsschutzbehörde für die von ihr eingegebenen Daten die datenschutzrechtliche Verantwortung trägt, richtet sich die **datenschutzrechtliche Kontrolle** nach den für die jeweilige Bundes- oder Landesbehörde maßgeblichen Regelungen.

§ 28 Abs. 2 BVerfSchG regelt die datenschutzrechtlichen Kontrolle für die Datenverarbeitung durch das BfV:

> *Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert beim Bundesamt für Verfassungsschutz die Einhaltung der Vorschriften über den Datenschutz. Soweit die Einhaltung von Vorschriften der Kontrolle durch die G 10-Kommission unterliegt, unterliegt sie nicht der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, es sei denn, die G 10-Kommission ersucht die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.*

Die Komplexität der Vorschrift ist dadurch bedingt, dass das BfV (u. a. in NADIS WN) auch personenbezogene Daten verarbeitet, die durch Überwachung der Telekommunikation oder des Brief- und Postverkehrs nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses[15] (G 10) gewonnen wurden. Die Datenerhebung und -verarbeitung nach dem G 10 unterliegt gemäß § 15 Abs. 5 Satz 1 und 2 G 10 der Kontrollbefugnis der G 10-Kommission. Gemäß § 15 Abs. 5 Satz 5 G 10 kann sie den BfDI jedoch in Fragen des Datenschutzes Gelegenheit zur Stellungnahme geben. Daran knüpft § 28 Abs. 2 Satz 2 BVerfSchG an. Außerhalb der Prüfkompetenz der G 10-Kommission verleiht § 28 Abs. 2 Satz 1 BVerfSchG dem BfDI eine eigene Zuständigkeit zur Kontrolle der Einhaltung der Vorschriften des Datenschutzes.[16]

* * *

15 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) vom 26. Juni 2001 (BGBl. I S. 1254, 2298; 2017 I S. 154), zuletzt geändert durch Artikel 6 Absatz 4 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2274).

16 Entgegen dem Eindruck, den der Sachstand WD 3 - 3000 - 149/17, S. 6 erzeugt, war dies auch bereits 2017 nach dem damals gültigen § 24 BDSG a.F. materielle Rechtslage. Diese wurde sprachlich bei der Übernahme der Regelung in § 26a BVerfSchG a.F. nur klargestellt, vgl. BT-Drs. 18/11325 (abrufbar unter: https://dserver.bundestag.de/btd/18/113/1811325.pdf) S. 122 und Siems, in: Schenke/Graulich/Ruthig, 2. Auflage 2019, BVerfSchG, § 26a Rn. 6. Der derzeit geltende § 28 BVerfSchG ist identisch mit der Vorgängernorm § 26a BVerfSchG a.F.