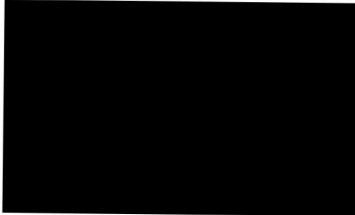




Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Postfach 1468, 53004 Bonn



HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-2204
TELEFAX (0228) 997799-5550
E-MAIL referat15@bdi.bund.de

BEARBEITET VON [REDACTED]
INTERNET www.informationsfreiheit.bund.de

DATUM Bonn, 21.05.2019
GESCHÄFTSZ. 22-642 II#1285

Bitte geben Sie das vorstehende Geschäftszeichen bei
allen Antwortschreiben unbedingt an.

BETREFF **Prüfung einer Datei mit Daten aus Funkzellenabfragen beim BKA**
BEZUG Mein Bescheid vom 25. September 2017
ANLAGEN Kontrollbericht zur Zentraldatei ST 15 vom 12. September 2017

Sehr geehrter [REDACTED]

in Abänderung meines Bescheides vom 25. September 2017 ergeht auf Ihren Antrag nach dem Informationsfreiheitsgesetz vom 17. Juli 2017 folgender

BESCHIED

1. Ihrem Antrag auf Übersendung der Unterlagen zu der beim Bundeskriminalamt durchgeführten Kontrolle zur Funkzellenabfrage wird insoweit stattgegeben, als der Prüfbericht des BfDI vom 12. September 2017 mit Teilschwärzungen zur Verfügung gestellt wird.
2. Darüber hinausgehende Unterlagen können aufgrund ihrer Verschlussachen-Einstufung nicht überlassen werden.

43866/2019

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße



3. Es werden keine Gebühren erhoben.

Begründung:

Mit E-Mail vom 17. Juli 2017 baten Sie nach § 1 Abs. 1 Informationsfreiheitsgesetz (IFG) um Zusendung aller Informationen (inklusive Memos, Vermerken, Gesprächsprotokollen, Entwürfen, Notizen, Eingaben, Schriftwechseln, Gutachten, Berichten und Zwischenständen) zur datenschutzrechtlichen Kontrolle der Datei mit Daten aus Funkzellenabfragen im BKA, insbesondere im Zusammenhang mit der Vor-Ort-Prüfung.

Mit Bescheid vom 25. September 2017 wurde der Antrag zunächst unter Hinweis auf § 4 Abs. 1 IFG abgelehnt, da der Kontroll- und Prüfvorgang zu diesem Zeitpunkt noch nicht abgeschlossen war.

Gleichzeitig wurde mitgeteilt, dass der Antrag nach Abschluss des Verfahrens nochmals aufgenommen würde.

Vorsorglich wurde aber bereits darauf hingewiesen, dass eine Herausgabe auch nach Abschluss des Kontrollverfahrens nur eingeschränkt zulässig sein würde, da wesentliche Bestandteile nach der Verschlussanweisung (VSA) eingestuft sind und für diese Schriftstücke gem. § 3 Nr. 4 IFG kein Informationszugang besteht.

Nachdem der Kontrollvorgang zwischenzeitlich abgeschlossen ist und die Voraussetzungen des § 4 Abs. 1 IFG nicht mehr vorliegen, habe ich geprüft, inwieweit die von Ihnen beantragte Herausgabe jetzt möglich ist.

Gem. § 3 Nummer 4 Informationsfreiheitsgesetz (IFG) besteht kein Informationsanspruch, wenn die verlangte Information u. a. der durch die Allgemeine Verwaltungs-



SEITE 3 VON 3

vorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen ge-
regelten Geheimhaltungs- oder Vertraulichkeitspflicht unterliegt.

Im vorliegenden Fall sind die Unterlagen, die im Zusammenhang mit der Datei mit
Daten aus Funkzellenabfragen stehen, vom Bundeskriminalamt als „VS-NfD“ einge-
stuft worden. In Folge dessen unterliegen auch die meisten der hiesigen Vermerke,
die mit der Kontrollmaßnahme in Verbindung stehen –und nicht zuletzt natürlich auch
der Kontrollbericht selbst- der Verschlusssacheneinstufung VS-NfD (Nur für den
Dienstgebrauch).

Nach Rücksprache mit dem BKA kann daher nur der beigefügte Kontrollbericht mit
Teilschwärzungen herausgegeben werden.

Rechtsmittelbelehrung:

Gegen diesen Bescheid kann innerhalb eines Monats nach Bekanntgabe Wider-
spruch bei dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
in Bonn erhoben werden.

Mit freundlichen Grüßen

Im Auftrag

VS – Nur für den Dienstgebrauch



Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Andrea Voßhoff

Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

POSTANSCHRIFT Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Postfach 1468, 53004 Bonn

Bundesministerium des Innern
Frau Staatssekretärin
Dr. Emily Haber
Alt-Moabit 140
10557 Berlin

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-100
TELEFAX (0228) 997799-550
E-MAIL arbeitsgruppe22a@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 12.09.2017

nachrichtlich:
Präsident des Bundeskriminalamtes
Herrn Holger Münch
Thaerstraße 11
65193 Wiesbaden

██████████, bDSB
Thaerstraße 11
65193 Wiesbaden

BETREFF

**Datenschutz beim Bundeskriminalamt -
Beanstandung der Zentraldatei ST 15**

HIER Funkzellendatenabgleich ██████████,
Beratungs- und Kontrollbesuch am 31.01.2017

Sehr geehrte Frau Dr. Haber,

am 31.01.2017 haben meine Mitarbeiter Herr Bergemann, Frau Waldhaus und Herr Richter beim Bundeskriminalamt am Dienstsitz Meckenheim eine datenschutzrechtliche Kontrolle durchgeführt. Gegenstand der Kontrolle war die Zentraldatei „ST15-Funkzellendatenabgleich ██████████“.

Ich danke für die Unterstützung meiner Mitarbeiter im Rahmen der Kontrolle. Von Seiten des BKA waren vor allem Mitarbeiter der Organisationseinheit St 15 und des Datenschutzreferats beteiligt.

A. Übersicht

Die Speicherung der personenbezogenen Daten in der „Zentraldatei ST 15 Funkzellendatenabgleich ██████████“ und den auf Grundlage dieser Daten durchgeführten Datenabgleich

17317/2017

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße



beanstande ich gemäß § 25 Abs. 1 BDSG.

Es fehlt an einer Rechtsgrundlage. § 7 Abs. 1 BKAG trägt die Maßnahme nicht, weil diese inhaltlich eine Rasterfahndung darstellt oder einer solchen zumindest gleichkommt. Auch § 98a StPO kommt als Rechtsgrundlage schon deshalb nicht in Betracht, weil die Maßnahme nicht als Rasterfahndung in einem konkreten Strafverfahren angeordnet wurde.

B. Feststellungen

Die Datei dient dem zentralen bundesweiten Abgleich von Funkzellendaten, die in Ermittlungsverfahren [REDACTED]. Zweck ist es, [REDACTED] und die Länder darüber zu unterrichten.

I. Zielsetzung der Datei

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Wenn dieser Zweck erreicht ist, soll die Maßnahme nach dem Vorschlag von ST15 auslaufen. Ein konkretes Datum steht dafür nicht fest.

[REDACTED], dies stellt jedoch nur ein Zwischenergebnis dar: [REDACTED]
[REDACTED]

II. Vorgehensweise beim Datenabgleich

1. Speicherort

Zentraler Speicherort der Datei ST15 ist das Vorgangsbearbeitungssystem (VBS) des BKA. Hier ist für ST15 ein abgeschirmter Bereich eingerichtet. Auf ihn hat nur eine Mitarbeiterin lesenden und schreibenden Zugriff. Zwei Mitarbeiterinnen haben lesenden Zugriff, um die Daten auswerten zu können.



SEITE 3 VON 12 Die Datei ist in zwei Bereiche unterteilt:

- für administrative Zwecke, ohne Speicherung personenbezogener Daten,
- unterteilt nach Ländern zur Abspeicherung der eingehenden Rohdaten, [REDACTED]

Es wird nach folgenden Merkmalen unterschieden:

- [REDACTED]

2. Anlieferung der Daten

Die Länder legen die Tatorte und Dauer des Erfassungszeitraums der Funkzellenabfrage fest, die ausgewertet werden sollen.

[REDACTED] Diese werden in unterschiedlichen Formaten (je nach Anbieter) angeliefert, z.B. als .xls, .txt oder .csv.

Die Daten werden an eine speziell dafür eingerichtete E-Mail-Adresse im BKA übermittelt. Auf dieses Postfach kann nur die Mitarbeiterin zugreifen, die lesenden und schreibenden Zugriff auf ST15 hat. Sie überführt die Daten aus dem E-Mail-Postfach in die Datei ST15.

[REDACTED]

Die angelieferten Rohdaten enthalten eine hohe Anzahl an nicht validen Daten, z.B. abgebrochene Anwahlversuche, Daten mit ersichtlich falschen Telefonnummern wie z.B. „00000000“, Servicrufnummern und ähnliches.

[REDACTED]



SEITE 4 VON 12 Diese Daten enthalten jedoch noch Redundanzen z.B. durch die unterschiedliche Übermittlung der Vorwahlen (Beispiel: 0 – 49) und müssen daher nach der Mitteilung an die Länder durch diese nochmals überprüft werden.

3. Verarbeitung der Daten

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Die Datenübertragung per USB-Stick erfolgt [REDACTED]. Der USB-Stick befindet sich grundsätzlich verschlossen in einem Schrank und kann nur von den beiden berechtigten Mitarbeitern benutzt werden und bleibt immer auf dem Gelände des BKA. Es wird derzeit an einer anderen Lösung gearbeitet, die den Datentransport per USB-Stick ablösen soll.

4. Ausgabe, Unterrichtung der Länder

Nach der Analyse werden die [REDACTED] den Ländern mitgeteilt, wobei jedes Land gesondert angeschrieben wird und nur Mitteilung über die Treffer in seinem Zuständigkeitsbereich erhält.

5. Protokollierung

Die Protokollierung der Datei ST15 erfolgt über die Protokollierung des VBS. Hier erfolgt eine Vollprotokollierung. Die berechtigten Mitarbeiter müssen sich mit Kennung und Passwort in die Datei einwählen. Im Analysesystem erfolgt außer der Authentifizierung der berechtigten Mitarbeiter keine Protokollierung.

6. Aufbewahrungsfristen/ Löschungen

Entsprechend der Errichtungsanordnung werden die Rohdaten [REDACTED] aufbewahrt. Da der erste Abgleich im [REDACTED] stattgefunden hat, gibt es derzeit noch keine Daten, die automatisch durch Fristablauf gelöscht wurden.

Manuelle Löschungen haben hingegen stattgefunden. So hat NRW einen „Tatort“ zurückgenommen. In dem Fall wurde der Beschluss der STA im VBS gespeichert, die Daten wurden gelöscht, so dass der Speicherplatz für den Tatort im VBS leer ist. Bei der nächsten Erstellung der [REDACTED] sind diese Daten dann nicht mehr enthalten, da zur Erstellung der [REDACTED] immer alle vorhandenen Rohdaten herangezogen werden.



SEITE 6 VON 12 Weiter erfolgte eine Rücknahme von Daten, deren Speicherung nicht durch die Errichtungsanordnung gedeckt war.

Die Lösungsbestätigung wird jeweils im VBS abgelegt.

C. Begründung der Beanstandung

In der Datei gleicht das Bundeskriminalamt personenbezogene Daten ab, die die Strafverfolgungsbehörden in Bund und Ländern mit Funkzellenabfragen gemäß § 100g Abs. 1 und 3 StPO erhoben haben. Das Vorgehen ist in dieser Form nicht durch die in der Errichtungsanordnung genannte Rechtsgrundlage des § 7 Abs. 1 BKAG gedeckt. Zwar kann ich den polizeilichen Ansatz nachvollziehen, Zusammenhänge zwischen den betreffenden Straftaten zu erkennen. Dies ändert jedoch an der rechtlichen Beurteilung nichts.

Auf der einen Seite wiegt das erhebliche Strafverfolgungsinteresse [REDACTED] [REDACTED] schwer. Ebenfalls liegt auf der Hand, dass hier – ggf. [REDACTED] – Zusammenhänge zwischen den Straftaten aufgedeckt werden sollen.

Auf der anderen Seite entsteht bereits auf der Grundlage nur einer einzelnen Funkzellenabfrage eine große Menge personenbezogener Daten, die jeweils im Millionenbereich liegen kann. Diese betreffen weit überwiegend unbeteiligte Personen, die selbst keinen Anlass für einen Grundrechtseingriff gegeben haben. Die vorliegende Datei beschränkt sich nicht auf ein bestimmtes Strafverfahren, sondern soll die Funkzellendaten aus einer Vielzahl von Strafverfahren speichern [REDACTED]. Das steigert die Eingriffsintensität nochmals maßgeblich. Dies bestätigt auch der nunmehr festgestellte Umfang der Datei. Mit steigender Datenmenge erhöht sich auch das Risiko, dass letztlich unschuldige Personen in der Treffermenge enthalten sind.

Als Grundlage einer solchen Maßnahme ist eine hinreichend bestimmte bereichsspezifische gesetzliche Befugnis notwendig.

Diese bietet § 7 Abs. 1 BKAG als Generalklausel aber nicht. Zudem dürfen speziellere Vorschriften nicht umgangen werden. Inhaltlich **entspricht** der in dem daten-



schutzrechtlichen Beratungs- und Kontrollbesuch festgestellte Datenabgleich einer Rasterfahndung bzw. steht dieser in der Eingriffsintensität gleich.

I. Rechtsgrundlage

Für den mit der Datei und dem Verfahren durchgeführten Datenabgleich besteht keine hinreichende Rechtsgrundlage. § 7 Abs. 1 i.V.m. § 28 BKAG rechtfertigt diesen Grundrechtseingriff nicht. Die Vorschrift kommt als Rechtsgrundlage nur in Betracht, wenn keine spezielleren Vorschriften eingreifen bzw. umgangen werden und zudem der Eingriff keine solche Eingriffsintensität erreicht, dass bei verfassungskonformer Auslegung eine spezifische Rechtsgrundlage erforderlich wäre (1.). Des Weiteren liegen die Voraussetzungen des § 98a StPO nicht vor (2.).

1. § 7 BKAG

Zum Anwendungsbereich des § 7 Abs. 1 BKAG habe ich in der jüngeren Vergangenheit mehrfach Stellung genommen, vgl. etwa meine Stellungnahme vom 19.11.2015, V-642-3/001#1175 VS-NfD (Ihr Zeichen: OeSI3-20108/1#75-VS-NfD). An meiner grundsätzlichen Bewertung zur Auslegung dieser Vorschrift halte ich fest.

§ 7 Abs. 1 BKAG rechtfertigt die Speicherung von personenbezogenen Dateien als Zentralstellengeneralklausel nur insoweit, als nicht vorrangig speziellere Vorschriften eingreifen. Die Regelung darf weder die Vorgaben der §§ 8, 9 BKAG noch die der Strafprozessordnung umgehen. Dasselbe gilt für Datenabgleiche gemäß § 28 BKAG, wenn diese auf der Grundlage der nach § 7 Abs. 1 BKAG gespeicherten Daten durchgeführt werden. § 28 Abs. 1 BKAG ist ebenfalls als Generalklausel ohne nähere spezifische Eingrenzungen formuliert.

Das Bundesverfassungsgericht fordert für eingriffsintensive Maßnahmen eine normklare und verhältnismäßige Regelung. Je größer der Grundrechtseingriff, desto genauer muss der Gesetzgeber die Voraussetzungen und Eingriffsschwellen regeln. Welche verfassungsrechtlichen Anforderungen an die tatbestandliche Eingrenzung der jeweiligen Eingriffsbefugnis zu stellen sind, richtet sich vor allem nach Art und Schwere des Grundrechtseingriffs. Dafür sind insbesondere Eingriffsintensität und Streubreite maßgeblich, die im Verhältnis dazu an bestimmte Einschreitschwellen geknüpft sein müssen; dafür kommt es insbesondere darauf an, ob die Betroffenen selbst einen Anlass für den Eingriff gegeben haben (BVerfGE 100, 313, 376; 115, 320, 347; 109, 279, 353). Daher können etwa auf die Ermittlungsgeneralklausel der §§ 161, 163 StPO nur solche Maßnahmen gestützt werden, die nicht selbst spezial-



SEITE 8 VON 12

gesetzlich geregelt sind, solchen Maßnahmen in ihrer grundrechtlichen Eingriffswirkung aber auch nicht gleichkommen (vgl. Erb in: Löwe-Rosenberg, StPO, 26. Auflage 2007, § 161 Rn. 3b). Erst recht gilt dies für die Zentralstellengeneralklausel des § 7 BKAG. Diesem kommt insofern nur die Funktion einer informationellen Verzahnung und Koordinierung zu (vgl. Bäcker, Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 22). Die Vorschrift kann schwerer wiegende Grundrechtseingriffe aufgrund ihrer zu weiten und zu pauschalen Fassung nicht rechtfertigen (Bäcker a.a.O.). Der Abgleich im hier geplanten Umfang geht aber über Grundrechtseingriffe von geringerer Intensität sehr deutlich hinaus, wie sich aus den nachfolgendem Erläuterungen ergibt.

Für ein einzelnes Strafverfahren können mehrere Funkzellenabfragen auf strafprozessualer Grundlage durchgeführt werden. Schon dafür stellt sich die die Frage, auf welcher Rechtsgrundlage ein Datenabgleich – z.B. wie hier als [REDACTED] – durchgeführt werden kann. Mir liegt z.B. ein (geschwärzter) Beschluss des Ermittlungsrichters beim AG München vor, der für diesen Fall eine Rasterfahndung nach § 98a StPO anordnet. Das ist aus meiner Sicht ein rechtlich zutreffender Ansatz. Denn die Funkzellendaten werden von vornherein mit dem Ziel eines Abgleichs mit weiteren Daten erhoben. Die Staatsanwaltschaft erhebt die Daten dabei bei einer privaten Stelle und lässt den Abgleich mit weiteren Daten nicht von der privaten Stelle, sondern von der Polizeibehörde durchführen. Im Einzelnen sind diese Fragen in der Rechtsprechung und Literatur noch nicht abschließend geklärt.

[REDACTED]

Wenn schon innerhalb des Strafverfahrens darauf zu achten ist, den § 98a StPO nicht zu umgehen, dann gilt dies erst Recht verfahrensübergreifend.

Der Sache nach handelt es sich um einen äußerst umfassenden Datenabgleich, der – und dies war von vornherein einzukalkulieren – in erster Linie die Daten unbeteiligter Personen betrifft, die selbst keinen Anlass für die Maßnahme gegeben haben.



SEITE 9 VON 12

Diese ist inhaltlich als Rasterfahndung einzustufen oder kommt dieser – rechtlich und tatsächlich gesehen – zumindest sehr nahe. In ihrem Datenumfang und in ihrer Eingriffsintensität dürfte die Maßnahme die bisher durchgeführten Rasterfahndungen mindestens erreichen. Gleichzeitig ist zu berücksichtigen, dass sie das Grundrecht der Betroffenen aus Art. 10 Abs. 1 GG berührt. Das Bundeskriminalamt durchsucht die Daten nach einem bestimmten Raster, hier dem oben beschriebenen.

Eine solche Maßnahme kann damit nicht mehr auf die Generalklausel des § 7 Abs. 1 BKAG gestützt werden.

2. § 98a StPO

Da die Funkzellendaten von vornherein mit dem Ziel des Datenabgleichs – [REDACTED] – erhoben werden, wäre Rechtsgrundlage dafür § 98a StPO. Nur auf diese Weise wäre im Übrigen sichergestellt, dass die Voraussetzungen des § 477 Abs. 2 Satz 1 StPO in die Prüfung einbezogen werden. Andernfalls könnten im Übrigen auch Zweifel an der Verwertbarkeit der gewonnenen Erkenntnisse aufkommen. Dies wäre nicht nur datenschutzrechtlich heikel, sondern läge auch nicht im Interesse der Strafverfolgung. Wenn insoweit **auf Grundlage eines richterlichen Beschlusses** eine strafprozessual tragfähige Situation geschaffen wird, ist **denkbar**, dass das **BKA auch für die Länder unterstützend tätig wird**, soweit es die Ermittlungen nicht selbst übernimmt bzw. übertragen bekommt.

Wie mir das Bundesministerium des Innern im Anhörungsverfahren zur EAO mitgeteilt hatte, ist der Generalbundesanwalt beteiligt worden. Dieser habe allerdings mitgeteilt, ein Strafverfahren wegen des Verdachts des § 129a StGB, das eine Rasterfahndung nach § 98a StPO rechtfertigen könnte, komme nicht in Betracht.

Daher lässt sich in der vorliegenden Fallgestaltung das Ansinnen der Strafverfolgungsbehörden auf gegenwärtiger Gesetzesgrundlage durch eine konsequente Anwendung des § 98a StPO offenbar nicht lösen, auch wenn angesichts der Erfahrungen der letzten Jahre durchaus naheliegend ist, dass hier ein Anfangsverdacht wegen der Bildung terroristischer bzw. krimineller Vereinigungen bestehen könnte. Das zu prüfen ist aber Sache der Strafverfolgungsbehörden und offenbar auch Ziel der gegenwärtigen Bemühungen.

3. Weitere Vorschriften



Weitere Rechtsgrundlagen, die die Speicherung der Daten und den darauf basierenden Datenabgleich rechtfertigen könnten, sind nicht ersichtlich.

In meiner Stellungnahme zum Gesetzentwurf der Bundesregierung zur Wiedereinführung der sogenannten Vorratsdatenspeicherung hatte ich auf die grundsätzlichen Probleme bei der Datenverarbeitung im Zusammenhang mit Funkzellenabfragen hingewiesen. Insbesondere hatte ich darauf hingewiesen, dass es verfassungsrechtlich nicht tragbar wäre, Verkehrsdaten ohne die notwendige Reduktion zu speichern, um diese für Strukturermittlungen zu nutzen. Denn in solchen Fällen würde aus der Vorratsspeicherung eine „doppelte Vorratsspeicherung“ resultieren. Ich hatte kritisiert, dass der Gesetzentwurf die bestehenden Probleme der Funkzellenabfrage nicht angeht. Dass der Gesetzgeber trotzdem keine spezifischen Lösungsmöglichkeiten geschaffen hat, darf jetzt nicht dazu führen, dass Maßnahmen in unzulässiger Weise auf hier nicht greifende Rechtsgrundlagen gestützt werden. Die bestehenden Probleme sind also mit den vorhandenen Vorschriften der Strafprozessordnung zu lösen.

4. Zwischenergebnis

An meiner bereits im Anhörungsverfahren zur Errichtungsanordnung geäußerten Ansicht halte ich – nunmehr auf Basis der datenschutzrechtlichen Kontrolle – fest. Für den Datenabgleich fehlt es an einer Rechtsgrundlage. § 7 Abs. 1 BKAG genügt dem nicht, weil die Maßnahme inhaltlich eine Rasterfahndung darstellt oder dieser zumindest gleichkommt.

Gemäß § 25 Abs. 1 BDSG ist dies als datenschutzrechtlicher Mangel zu beanstanden. Es ist nicht gemäß 25 Abs. 2 BDSG möglich, von einer Beanstandung abzusehen. Es handelt sich um einen erheblichen Mangel. Der Datenabgleich ist angesichts der Vielzahl der betroffenen Personen, die größtenteils keinen Anlass dafür gegeben haben, und aufgrund der Heimlichkeit ein besonders intensiver Grundrechtseingriff. Ein solcher darf nicht ohne ausreichend normenklare und bestimmte Rechtsgrundlage durchgeführt werden.

II. Nutzung des VBS

Als technische Grundlage der Datei nutzt das BKA das Vorgangsbearbeitungssystem (VBS).



SEITE 11 VON 12

Die Errichtungsanordnung zum Vorgangsbearbeitungssystem (VBS) nennt als Rechtsgrundlagen § 30 Abs. 2 BKAG und § 14 Abs. 1 BDSG und bezeichnet das System als „Amtsdatei“. Dies lässt zunächst fraglich erscheinen, ob dies Raum für Speicherungen von Daten nach § 7 Abs. 1 BKAG bzw. § 98a StPO lässt.

In der von mir bewerteten Errichtungsanordnung für die Datei St15 FZA vom 15.12.2015 war das **VBS** als „technische Grundlage“ **noch nicht benannt**. Im späteren mit E-Mail vom 28. Dezember 2016 übersandten Entwurf der Errichtungsanordnung wurde dies in Nr. 6.1 und Nr. 9 nachgepflegt.

Es bestehen jedoch grundsätzliche Zweifel, ob der Zweck des VBS in dieser Weise neu definiert werden kann.

Dies kann jedoch nicht datenschutzrechtlich beurteilt werden, ohne auf die Details und die Zweckbestimmung des VBS als solches einzugehen und geht über den Prüfgegenstand dieser datenschutzrechtlichen Kontrolle deutlich hinaus. Darauf wird in einer späteren Kontrolle des VBS als solchem einzugehen sein.

III. Datensicherheit

Die fehlende Verschlüsselung des USB-Sticks ist im Hinblick auf die technisch organisatorische Sicherheit nicht optimal. Angesichts des engen Personenkreises, der Zugang zu dem Stick hat, sehe ich aber von einer Beanstandung ab. Das BKA hat darüber hinaus angekündigt, auf eine andere Methode umzustellen. Daher wäre ich für eine zeitnahe Mitteilung dankbar, wie weit die entsprechenden Bemühungen gediehen sind.

III. Protokollierung

Nach Nr. 9 des geänderten Entwurfs der EAO mit Stand vom 28. Dezember 2016 gelten für die Protokollierung die allgemeinen Regelungen zum VBS. Der Mangel der ersten EAO mit Stand vom 15.12.2015 (Nr. 10) ist insofern nicht mehr in der Form vorhanden, die ich in meiner damaligen Stellungnahme angemerkt hatte. Von einer Beanstandung dieses Mangels sehe ich daher gemäß § 25 Abs. 2 BDSG vorerst ab.

Auf die technischen Einzelheiten der nunmehr vorgesehenen Protokollierung kann hier nicht eingegangen werden. Dies hätte erfordert, technisch die Protokollierung des VBS zu analysieren. Dies ist aber nur in einer Kontrolle des VBS als solchem möglich und muss daher einer späteren Kontrolle vorbehalten sein.



SEITE 12 VON 12

D. Fazit

Im Ergebnis ist der Betrieb der geprüften Datei **datenschutzrechtlich unzulässig**.

Für eine Stellungnahme innerhalb von acht Wochen nach Zugang dieses Schreibens bin ich dankbar.

Mit freundlichen Grüßen

Andrea Voßhoff