Änderungsantrag

der Fraktionen der SPD, von BÜNDNIS 90/DIE GRÜNEN und der FDP

zu dem Gesetzentwurf der Fraktionen SPD, BÜNDNIS 90/DIE GRÜNEN und FDP

Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung – Drucksache BT 20/12806 –

Der Deutsche Bundestag wolle beschließen,

den Gesetzentwurf auf Drucksache BT 20/12806 mit folgenden Maßgaben - im Übrigen unverändert – anzunehmen

1. Artikel 1 wird wie folgt geändert:

a) Nummer 1 wird wie folgt gefasst:

‚1. Die Inhaltsübersicht wird wie folgt geändert:

a) Nach der Angabe zu § 10a wird folgende Angabe eingefügt:

„§ 10b Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung“

b) Nach der Angabe zu § 16 wird folgende Angabe eingefügt:

„§ 16a Automatisierte Datenanalyse; Verordnungsermächtigung“

c) Die Angabe zu § 22 wird wie folgt gefasst:

„§ 22 Weiterverarbeitung von Daten zu weiteren Zwecken; Verordnungsermächtigung“

d) Nach der Angabe zu § 39 wird folgende Angabe eingefügt:

„§ 39a Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung“

e) Nach der Angabe zu § 63a wird folgende Angabe eingefügt:

„§ 63b Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung“ ‘.

b) Nummer 3 wird wie folgt gefasst:

‚3. Nach § 10a wird der folgende § 10b eingefügt:

„§ 10b

Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung

(1) Das Bundeskriminalamt kann zur Ergänzung vorhandener Sachverhalte biometrische Daten zu Gesichtern und Stimmen, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, mit allgemein öffentlich zugänglichen personenbezogenen Daten aus

dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen, sofern

1. dies im Rahmen der Erfüllung seiner Aufgabe als Zentralstelle nach § 2 Absatz 2 Nummer 1 zur Identifizierung oder Ermittlung des Aufenthaltsorts der Zielperson erforderlich ist,
2. bestimmte Tatsachen den Verdacht begründen, dass eine Straftat im Sinne des § 100b Absatz 2 der Strafprozessordnung begangen worden ist oder die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine solche Straftat begehen wird, und
3. die Verfolgung oder Verhütung der Straftat auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Ein Abgleich mit Daten nach Satz 1 aus im Internet allgemein öffentlich zugänglichen in Echtzeit erhobenen Daten ist ausgeschlossen.

(2) Die Maßnahme nach Absatz 1 Satz 1 darf gegen die in § 18 Absatz 1 sowie § 19 Absatz 1 Satz 1 Nummer 2 bezeichneten Personen durchgeführt werden. Bezüglich einer Person nach § 19 Absatz 1 Satz 1 Nummer 2 ist die Maßnahme unzulässig, wenn überwiegende schutzwürdige Interessen der betreffenden Person entgegenstehen.

(3) Für die nach Absatz 1 Satz 1 abzugleichenden Daten gilt § 12 Absatz 2 entsprechend. Der Abgleich mit Daten, die durch die in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist ausgeschlossen.

(4) Maßnahmen nach Absatz 1 Satz 1 dürfen nur auf Antrag der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Präsidentin oder den Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung getroffen werden. Sofern die Anordnung der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung nicht binnen drei Tagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. die Person, zu deren Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird,
2. die biometrischen Daten aus dem Strafverfahren oder dem Vorgang, die dieser Person zuzuordnen sind und die zum Abgleich herangezogen werden sollen,
3. der Tatvorwurf oder Sachverhalt, auf Grund dessen die Maßnahme angeordnet wird, und
4. die eingesetzte automatisierte Anwendung zur Datenverarbeitung.

(5) In der Begründung der Anordnung sind die Voraussetzungen für die Maßnahme nach Absatz 1 Satz 1 und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind

einzelfallbezogen die bestimmten Tatsachen, die den Verdacht begründen, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme, die wesentlichen Einzelheiten zur technischen Funktionsweise der automatisierten Anwendung zur Datenverarbeitung sowie die Subsidiarität zu anderen Maßnahmen anzugeben.

(6) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 Satz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 Satz 1 erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Bei Maßnahmen nach Absatz 1 Satz 1 ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach Absatz 1 Satz 1 erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder von der der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend.

(7) Die im Rahmen des Abgleichs nach Absatz 1 Satz 1 erhobenen Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, sofern sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt aufweisen. Die Weiterverarbeitung der beim Abgleich erhobenen Daten ist im Übrigen unzulässig.

(8) Bei jeder Maßnahme nach Absatz 1 Satz 1 ist die Bezeichnung der eingesetzten automatisierten Anwendung zur Datenverarbeitung, der Zeitpunkt ihres Einsatzes sowie die Organisationseinheit einschließlich einer individuellen Kennung der Person, die die Maßnahme durchführt, zu protokollieren. Nach Beendigung einer Maßnahme nach Absatz 1 Satz 1 ist die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist.

(9) Soweit zur Durchführung des Abgleichs nach Absatz 1 Satz 1 Dritte im Wege der Auftragsverarbeitung für das Bundeskriminalamt tätig werden, müssen diese ihren Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten zur Durchführung der Maßnahme nach Absatz 1 Satz 1 ist nur innerhalb der Europäischen Union, einschließlich der Schengen-assoziierten Staaten, zulässig. Die Weiterverarbeitung durch Dritte von personenbezogenen Daten, die aus in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist ausgeschlossen. Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 1 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Durch

organisatorische und technische Maßnahmen ist zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(10) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit führt Kontrollen bezüglich der Datenverarbeitung der Maßnahme nach Absatz 1 Satz 1 mindestens alle zwei Jahre durch.

(11) Die Bundesregierung bestimmt vor dem Einsatz von Maßnahmen nach Absatz 1 Satz 1 durch Rechtsverordnung ohne Zustimmung des Bundesrats nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und, soweit eine Speicherung der abzugleichenden, öffentlich zugänglichen Lichtbild- Video- und Audiodateien für die Durchführung von Maßnahmen nach Absatz 1 technisch erforderlich ist, nähere Vorgaben zu Art, Umfang und Dauer. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. Eingabe- und Zugangsberechtigung,
2. Speicher- und Löschfristen,
3. Art der zu speichernden Daten,
4. Personenkreis, der von der Speicherung betroffen ist,
5. Dauer der Speicherung,
6. Protokollierung.“ ‘

c) Nummer 4 wird wie folgt gefasst:

‚4. Nach § 16 wird der folgende § 16a eingefügt:

„§ 16a

Automatisierte Datenanalyse; Verordnungsermächtigung

(1) Das Bundeskriminalamt kann im Informationssystem oder im polizeilichen Informationsverbund gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenführen und darüber hinaus zum Zwecke der Analyse weiterverarbeiten, sofern dies zur Abwehr einer im Einzelfall bestehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, im Zusammenhang mit Straftaten nach § 5 Absatz 1 Satz 2 erforderlich ist. Eine Maßnahme nach Satz 1 ist auch zulässig, sofern

1. Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird, oder
2. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines

übersehbaren Zeitraums eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird,

und dies zur Verhütung dieser Straftat erforderlich ist.

(2) Absatz 1 gilt zur Verhütung von Straftaten von auch im Einzelfall erheblicher Bedeutung gegen Leib, Leben oder Freiheit der nach § 6 zu schützenden Personen entsprechend.

(3) Zur Erfüllung der Aufgabe als Zentralstelle kann das Bundeskriminalamt die Zusammenführung und Weiterverarbeitung personenbezogener Daten nach Absatz 1 vornehmen, sofern bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat im Sinne des § 100b Absatz 2 der Strafprozessordnung begehen wird oder begangen hat, diese auch im Einzelfall besonders schwer wiegt, und dies zur Verhütung oder Verfolgung der Straftat erforderlich ist.

(4) Im Rahmen der Weiterverarbeitung nach den Absätzen 1 bis 3 können insbesondere datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, Suchkriterien gewichtet, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden. Für die Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen oder einen verdeckten Eingriff in informationstechnische Systeme erlangt wurden, gilt § 12 Absatz 3.

(5) Beim Einsatz selbstlernender Systeme gilt § 22 Absatz 3 Satz 2 und 3 entsprechend.

(6) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit führt Kontrollen bezüglich der Datenverarbeitung der Maßnahme nach Absatz 1 mindestens alle zwei Jahre durch.

(7) Die Bundesregierung bestimmt vor dem Einsatz von Maßnahmen nach Absatz 1 Satz 1 durch Rechtsverordnung ohne Zustimmung des Bundesrats nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und nähere Vorgaben zu Art und Umfang der verarbeiteten Daten. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. Eingabe- und Zugangsberechtigung,
2. Art der zu verarbeitenden Daten,
3. Personenkreis, der von der Verarbeitung betroffen ist,
4. besondere Regelungen über die Verarbeitung von Daten, die durch besonders eingriffsintensive Maßnahmen erhoben wurden,
5. Protokollierung, einschließlich einer individuellen Kennung der handelnden Personen.“ ‘

d) Nummer 5 wird wie folgt gefasst:

‚5. § 22 wird wie folgt geändert:

a) Die Überschrift wird wie folgt gefasst:

„§ 22

Weiterverarbeitung von Daten zu weiteren Zwecken; Verordnungsermächtigung“

b) Die folgenden Absätze 3 und 4 werden angefügt:

„(3) Das Bundeskriminalamt darf zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten bei ihm vorhandene personenbezogene Daten weiterverarbeiten und an Dritte übermitteln, soweit dies erforderlich ist, weil

1. unveränderte Daten benötigt werden oder
2. eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Es hat dabei sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Soweit wie technisch möglich muss die Nachvollziehbarkeit des verwendeten Verfahrens sichergestellt werden. Sofern Daten im Sinne von Satz 1 an Dritte übermittelt werden, müssen diese ihren Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten zur Durchführung der Maßnahme nach Absatz 1 Satz 1 ist nur innerhalb der Europäischen Union, einschließlich der Schengen-assoziierten Staaten, zulässig. Die Weiterverarbeitung von personenbezogenen Daten, die aus in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist unzulässig. Eine Übermittlung der in Satz 6 genannten Daten ist unzulässig. Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 1 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Durch organisatorische und technische Maßnahmen hat das Bundeskriminalamt zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(4) Die Bundesregierung bestimmt vor der Übermittlung von personenbezogenen Daten an Dritte nach Absatz 3 Satz 1 durch Rechtsverordnung ohne Zustimmung des Bundesrats nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und nähere Vorgaben zu Art und Umfang der verarbeiteten Daten. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. Art der zu verarbeitenden Daten,
2. Definition von unveränderten Daten,

3. Personenkreis, der von der Verarbeitung betroffen ist,

4. Sicherungsmaßnahmen zur Datenaktualität und -qualität,

5. Mindeststandards zur technischen Durchführung der Anonymisierung und Pseudonymisierung von Daten einschließlich einer näheren Bestimmung des unverhältnismäßigen Aufwands im Sinne von Absatz 3 Satz 1 Nummer 2,

6. Protokollierung, einschließlich einer individuellen Kennung der handelnden Personen.“ ‘

e) Nummer 8 wird wie folgt gefasst:

‚8. Nach § 39 wird folgender § 39a eingefügt:

„§ 39a

Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung

(1) Das Bundeskriminalamt kann biometrische Daten zu Gesichtern und Stimmen, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, mit allgemein öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen, sofern

1. dies im Rahmen der Abwehr einer im Einzelfall bestehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, im Zusammenhang mit Straftaten nach § 5 Absatz 1 Satz 2 zur Identifizierung oder Ermittlung des Aufenthaltsorts der Zielperson erforderlich ist und

2. die Abwehr der Gefahr auf andere Weise aussichtslos ist oder wesentlich erschwert wäre.

Die Maßnahme nach Satz 1 ist auch zulässig, sofern

1. Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird oder

2. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird

und die Verhütung der Straftat auf andere Weise aussichtslos ist oder wesentlich erschwert wäre. Ein Abgleich mit Daten nach Satz 1 aus im Internet allgemein öffentlich zugänglichen in Echtzeit erhobenen Daten ist ausgeschlossen.

(2) Die Maßnahme nach Absatz 1 Satz 1 darf gegen die entsprechend § 17 oder § 18 des Bundespolizeigesetzes

Verantwortlichen sowie Personen im Sinne von Absatz 1 Satz 2 Nummer 1 oder 2 durchgeführt werden.

(3) Für die nach Absatz 1 Satz 1 abzugleichenden Daten gilt § 12 Absatz 2 entsprechend. Der Abgleich mit Daten, die durch die in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist ausgeschlossen.

(4) Maßnahmen nach Absatz 1 Satz 1 dürfen nur auf Antrag der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Präsidentin oder den Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung getroffen werden. Sofern die Anordnung der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung nicht binnen drei Tagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. die Person, zu deren Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird,
2. die biometrischen Daten aus dem Strafverfahren oder dem Vorgang, die dieser Person zuzuordnen sind und die zum Abgleich herangezogen werden sollen,
3. der Tatvorwurf oder Sachverhalt, auf Grund dessen die Maßnahme angeordnet wird, und
4. die eingesetzte automatisierte Anwendung zur Datenverarbeitung.

(5) In der Begründung der Anordnung sind die Voraussetzungen für die Maßnahme nach Absatz 1 Satz 1 und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen die bestimmten Tatsachen, die den Verdacht begründen, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme, die wesentlichen Einzelheiten zur technischen Funktionsweise der automatisierten Anwendung zur Datenverarbeitung sowie die Subsidiarität zu anderen Maßnahmen anzugeben.

(6) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 Satz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 Satz 1 erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Bei Maßnahmen nach Absatz 1 Satz 1 ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach Absatz 1 Satz 1 erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder von der der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten

vorzulegen. Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend.

(7) Die im Rahmen des Abgleichs nach Absatz 1 Satz 1 erhobenen Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, sofern sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt aufweisen. Die Weiterverarbeitung der beim Abgleich erhobenen Daten ist im Übrigen unzulässig.

(8) Bei jeder Maßnahme nach Absatz 1 Satz 1 ist die Bezeichnung der eingesetzten automatisierten Anwendung zur Datenverarbeitung, der Zeitpunkt ihres Einsatzes sowie die Organisationseinheit einschließlich einer individuellen Kennung der Person, die die Maßnahme durchführt, zu protokollieren. Nach Beendigung einer Maßnahme nach Absatz 1 ist die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist.

(9) Soweit zur Durchführung des Abgleichs nach Absatz 1 Satz 1 Dritte im Wege der Auftragsverarbeitung für das Bundeskriminalamt tätig werden, müssen diese ihren Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten zur Durchführung der Maßnahme nach Absatz 1 Satz 1 ist nur innerhalb der Europäischen Union, einschließlich der Schengen-assoziierten Staaten, zulässig. Die Weiterverarbeitung durch Dritte von personenbezogenen Daten, die aus in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist ausgeschlossen. Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 1 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Durch organisatorische und technische Maßnahmen ist zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(10) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit führt Kontrollen bezüglich der Datenverarbeitung der Maßnahme nach Absatz 1 Satz 1 mindestens alle zwei Jahre durch.

(11) Die Bundesregierung bestimmt vor dem Einsatz von Maßnahmen nach Absatz 1 Satz 1 durch Rechtsverordnung ohne Zustimmung des Bundesrats nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und, soweit eine Speicherung der abzugleichenden, öffentlich zugänglichen Lichtbild- Video- und Audiodateien für die Durchführung von Maßnahmen nach Absatz 1 technisch erforderlich ist, nähere Vorgaben zu Art, Umfang und Dauer. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. Eingabe- und Zugangsberechtigung,
2. Speicher- und Löschfristen,
3. Art der zu speichernden Daten,
4. Personenkreis, der von der Speicherung betroffen ist,

5. Dauer der Speicherung,

6. Protokollierung.“ ‘

f) Nummer 9 wird wie folgt gefasst:

‚9. Nach § 63a wird folgender § 63b eingefügt:

„§ 63b

Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung

(1) Das Bundeskriminalamt kann biometrische Daten zu Gesichtern und Stimmen, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, mit allgemein öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen, sofern dies im Einzelfall erforderlich ist zur Identifizierung oder Ermittlung des Aufenthaltsorts der Zielperson

1. zur Abwehr einer erheblichen Gefahr für Leib, Leben oder Freiheit für eine zu schützende Person oder für eine zu schützende Räumlichkeit nach § 6 oder

2. zum Schutz von Leib, Leben, Freiheit, sexueller Selbstbestimmung oder bedeutenden Sachwerten einer zu schützenden Person oder zum Schutz einer zu schützenden Räumlichkeit nach § 6 vor einer gemeingefährlichen Straftat, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, an dem bestimmte Personen beteiligt sein werden, oder

3. zum Schutz von Leib, Leben, Freiheit oder sexueller Selbstbestimmung einer zu schützenden Person oder zum Schutz einer zu schützenden Räumlichkeit nach § 6 vor einer gemeingefährlichen Straftat„ wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in einem übersehbaren Zeitraum eine Straftat gegen eines dieser Rechtsgüter der zu schützenden Person oder gegen eine zu schützende Räumlichkeit begehen wird,

die Gefahr nach den Nummern 1 bis 3 auch im Einzelfall von erheblicher Bedeutung ist und die Abwehr der Gefahr auf andere Weise aussichtlos oder wesentlich erschwert wäre. Ein Abgleich mit Daten nach Satz 1 aus im Internet allgemein öffentlich zugänglichen in Echtzeit erhobenen Daten ist ausgeschlossen.

(2) Die Maßnahme nach Absatz 1 Satz 1 darf gegen die entsprechend § 17 oder § 18 des Bundespolizeigesetzes Verantwortlichen sowie Personen im Sinne von Absatz 1 Satz 2 Nummer 1 oder 2 durchgeführt werden.

(3) Für die nach Absatz 1 Satz 1 abzugleichenden Daten gilt § 12 Absatz 2 entsprechend. Der Abgleich mit Daten, die durch die in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist ausgeschlossen.

(4) Maßnahmen nach Absatz 1 Satz 1 dürfen nur auf Antrag der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Präsidentin oder den Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung getroffen werden. Sofern die Anordnung der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung nicht binnen drei Tagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. die Person, zu deren Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird,
2. die biometrischen Daten aus dem Strafverfahren oder dem Vorgang, die dieser Person zuzuordnen sind und die zum Abgleich herangezogen werden sollen,
3. der Tatvorwurf oder Sachverhalt, auf Grund dessen die Maßnahme angeordnet wird, und
4. die eingesetzte automatisierte Anwendung zur Datenverarbeitung.

(5) In der Begründung der Anordnung sind die Voraussetzungen für die Maßnahme nach Absatz 1 Satz 1 und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen die bestimmten Tatsachen, die den Verdacht begründen, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme, die wesentlichen Einzelheiten zur technischen Funktionsweise der automatisierten Anwendung zur Datenverarbeitung sowie die Subsidiarität zu anderen Maßnahmen anzugeben.

(6) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 Satz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 Satz 1 erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Bei Maßnahmen nach Absatz 1 Satz 1 ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach Absatz 1 Satz 1 erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder von der der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend.

(7) Die im Rahmen des Abgleichs nach Absatz 1 Satz 1 erhobenen Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, sofern sie keinen konkreten Ermittlungsansatz für

den Ausgangssachverhalt aufweisen. Die Weiterverarbeitung der beim Abgleich erhobenen Daten ist im Übrigen unzulässig.

(8) Bei jeder Maßnahme nach Absatz 1 Satz 1 ist die Bezeichnung der eingesetzten automatisierten Anwendung zur Datenverarbeitung, der Zeitpunkt ihres Einsatzes sowie die Organisationseinheit einschließlich einer individuellen Kennung der Person, die die Maßnahme durchführt, zu protokollieren. Nach Beendigung einer Maßnahme nach Absatz 1 ist die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist.

(9) Soweit zur Durchführung des Abgleichs nach Absatz 1 Satz 1 Dritte im Wege der Auftragsverarbeitung für das Bundeskriminalamt tätig werden, müssen diese ihren Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten zur Durchführung der Maßnahme nach Absatz 1 Satz 1 ist nur innerhalb der Europäischen Union, einschließlich der Schengen-assoziierten Staaten, zulässig. Die Weiterverarbeitung durch Dritte von personenbezogenen Daten, die aus in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist ausgeschlossen. Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 1 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Durch organisatorische und technische Maßnahmen ist zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(10) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit führt Kontrollen bezüglich der Datenverarbeitung der Maßnahme nach Absatz 1 Satz 1 mindestens alle zwei Jahre durch.

(11) Die Bundesregierung bestimmt vor dem Einsatz von Maßnahmen nach Absatz 1 Satz 1 durch Rechtsverordnung ohne Zustimmung des Bundesrats nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und, soweit eine Speicherung der abzugleichenden, öffentlich zugänglichen Lichtbild- Video- und Audiodateien für die Durchführung von Maßnahmen nach Absatz 1 technisch erforderlich ist, nähere Vorgaben zu Art, Umfang und Dauer. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. Eingabe- und Zugangsberechtigung,
2. Speicher- und Löschfristen,
3. Art der zu speichernden Daten,
4. Personenkreis, der von der Speicherung betroffen ist,
5. Dauer der Speicherung,
6. Protokollierung.“ ‘

2. Artikel 2 wird wie folgt geändert:

a) Nummer 1 wird wie folgt gefasst:

‚1. In der Inhaltsübersicht werden nach der Angabe zu § 34 die folgenden Angaben eingefügt:

„§ 34a Automatisierte Datenanalyse; Verordnungsermächtigung

§ 34b Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung“.‘

b) Nummer 2 wird wie folgt gefasst:

„2. Nach § 22 Absatz 1a wird folgender Absatz 1b eingefügt:

„(1b) Die Bundespolizei kann zur Durchsetzung von Waffenverbotszonen nach § 42b Absatz 2 des Waffengesetzes sowie zur Durchsetzung von Allgemeinverfügungen der Bundespolizei auf dem Gebiet der Eisenbahnen des Bundes, welche das Mitführen von konkret bezeichneten gefährlichen Gegenständen und Waffen untersagt, in den jeweiligen räumlichen Geltungsbereichen Personen kurzzeitig anhalten, befragen und verlangen, dass mitgeführte Ausweispapiere zur Prüfung ausgehändigt werden, sowie mitgeführte Sachen in Augenschein nehmen und durchsuchen. Die Auswahl der nach Satz 1 durch die Bundespolizei kontrollierten Person anhand eines Merkmals im Sinne des Artikels 3 Absatz 3 des Grundgesetzes ohne sachlichen, durch den Zweck der Maßnahme gerechtfertigten Grund ist unzulässig.“

c) Nummer 3 wird wie folgt gefasst:

‚3. Nach § 34 werden die folgenden §§ 34a und 34b eingefügt:

„§ 34a

Automatisierte Datenanalyse; Verordnungsermächtigung

(1) Die Bundespolizei kann zur Erfüllung ihrer Aufgaben nach den §§ 1 bis 8 personenbezogene Daten, die sie zur Erfüllung der ihr obliegenden Aufgaben weiterverarbeitet oder für die sie eine Berechtigung zum Abruf hat, mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenführen und darüber hinaus zum Zwecke der Analyse weiterverarbeiten, sofern

1. dies zur Abwehr einer im Einzelfall bestehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, erforderlich ist,

2. bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat von auch im Einzelfall erheblicher Bedeutung im Zusammenhang mit lebensgefährdenden Schleusungen oder eine Straftat von auch im Einzelfall erheblicher Bedeutung, die gegen die Sicherheit der Anlagen oder des Betriebes des Luft-, See- oder Bahnverkehrs, insbesondere Straftaten von auch im Einzelfall erheblicher Bedeutung nach den §§ 315, 315b, 316b und 316c des Strafgesetzbuches, gerichtet ist und eine nicht unerhebliche Gefährdung eines der in Nummer 1

genannten Rechtsgüter erwarten lässt, begehen wird, und dies zur Verhütung der Straftat erforderlich ist, oder

3. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine Straftat von auch im Einzelfall erheblicher Bedeutung im Zusammenhang mit lebensgefährdenden Schleusungen oder eine Straftat von auch im Einzelfall erheblicher Bedeutung, die gegen die Sicherheit der Anlagen oder des Betriebes des Luft-, See- oder Bahnverkehrs gerichtet ist, insbesondere Straftaten von auch im Einzelfall erheblicher Bedeutung nach den §§ 315, 315b, 316b und 316c des Strafgesetzbuches, und eine nicht unerhebliche Gefährdung eines der in Nummer 1 genannten Rechtsgüter erwarten lässt, begehen wird, und dies zur Verhütung der Straftat erforderlich ist.

(2) Im Rahmen der Weiterverarbeitung nach den Absatz 1 können insbesondere datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, Suchkriterien gewichtet, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden.

(3) Beim Einsatz selbstlernender Systeme gilt § 22 Absatz 3 Satz 2 und 3 des Bundeskriminalamtgesetzes entsprechend.

(4) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit führt Kontrollen bezüglich der Datenverarbeitung der Maßnahme nach Absatz 1 mindestens alle zwei Jahre durch.

(5) Die Bundesregierung bestimmt vor dem Einsatz von Maßnahmen nach Absatz 1 Satz 1 durch Rechtsverordnung ohne Zustimmung des Bundesrats nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und nähere Vorgaben zu Art und Umfang der verarbeiteten Daten. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. Eingabe- und Zugangsberechtigung,
2. Art der zu verarbeitenden Daten,
3. Personenkreis, der von der Verarbeitung betroffen ist,
4. besondere Regelungen über die Verarbeitung von Daten, die durch besonders eingriffsintensive Maßnahmen erhoben wurden,
5. Protokollierung, einschließlich einer individuellen Kennung der handelnden Personen.

§ 34b

Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung

(1) Die Bundespolizei kann biometrische Daten zu Gesichtern und Stimmen, die sie zur Erfüllung ihrer Aufgaben nach den §§ 1 bis 8 weiterverarbeitet oder für die sie eine Berechtigung zum Abruf hat, mit allgemein öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen, sofern

1. dies im Rahmen der Abwehr einer im Einzelfall bestehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, zur Identifizierung oder Ermittlung des Aufenthaltsorts der Zielperson erforderlich ist und
2. die Abwehr der Gefahr auf andere Weise aussichtslos ist oder wesentlich erschwert wäre.

Die Maßnahme nach Satz 1 ist auch zulässig, sofern im Rahmen der Aufgaben nach den §§ 1 bis 8

1. bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat von auch im Einzelfall erheblicher Bedeutung im Zusammenhang mit lebensgefährdenden Schleusungen oder eine Straftat von auch im Einzelfall erheblicher Bedeutung, die gegen die Sicherheit der Anlagen oder des Betriebes des Luft-, See- oder Bahnverkehrs, insbesondere Straftaten von auch im Einzelfall erheblicher Bedeutung nach den §§ 315, 315b, 316b und 316c des Strafgesetzbuches, gerichtet ist und eine nicht unerhebliche Gefährdung eines der in Satz 1 Nummer 1 genannten Rechtsgüter erwarten lässt, begehen wird, oder
2. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine Straftat von auch im Einzelfall erheblicher Bedeutung im Zusammenhang mit lebensgefährdenden Schleusungen oder eine Straftat von auch im Einzelfall erheblicher Bedeutung, die gegen die Sicherheit der Anlagen oder des Betriebes des Luft-, See- oder Bahnverkehrs gerichtet ist, insbesondere Straftaten von auch im Einzelfall erheblicher Bedeutung nach den §§ 315, 315b, 316b und 316c des Strafgesetzbuches, und eine nicht unerhebliche Gefährdung eines der in Satz 1 Nummer 1 genannten Rechtsgüter erwarten lässt, begehen wird

und die Verhütung der Straftat auf andere Weise aussichtslos oder wesentlich erschwert wäre. Ein Abgleich mit Daten nach Satz 1 aus im Internet allgemein öffentlich zugänglichen in Echtzeit erhobenen Daten ist ausgeschlossen.

(2) Die Maßnahme nach Absatz 1 Satz 1 darf gegen die § 17 oder § 18 Verantwortlichen sowie Personen im Sinne von Absatz 1 Satz 2 Nummer 1 oder 2 durchgeführt werden.

(3) Maßnahmen nach Absatz 1 Satz 1 dürfen nur auf Antrag die Präsidentin oder den Präsidenten des Bundespolizeipräsidiums oder ihre oder seine Vertretung durch das Gericht angeordnet werden. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit mit Ausnahme des § 23 Absatz 2 und des § 37 Absatz 2 entsprechend. Die Anordnung wird mit Erlass wirksam. Bei Gefahr im Verzug kann die Anordnung auch durch die Präsidentin oder den Präsidenten des Bundespolizeipräsidiums oder ihre oder seine Vertretung getroffen werden. Sofern die Anordnung die Präsidentin oder den Präsidenten des Bundespolizeipräsidiums oder ihre oder seine Vertretung nicht binnen drei Tagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. die Person, zu deren Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird,
2. die biometrischen Daten aus dem Vorgang, die dieser Person zuzuordnen sind und die zum Abgleich herangezogen werden sollen,
3. der Sachverhalt, auf Grund dessen die Maßnahme angeordnet wird, und
4. die eingesetzte automatisierte Anwendung zur Datenverarbeitung.

(4) In der Begründung der Anordnung sind die Voraussetzungen für die Maßnahme nach Absatz 1 Satz 1 und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen die bestimmten Tatsachen, die den Verdacht begründen, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme, die wesentlichen Einzelheiten zur technischen Funktionsweise der automatisierten Anwendung zur Datenverarbeitung sowie die Subsidiarität zu anderen Maßnahmen anzugeben.

(5) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 Satz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 Satz 1 erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Bei Maßnahmen nach Absatz 1 Satz 1 ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach Absatz 1 Satz 1 erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder von der der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder ihrer oder seiner Vertretung dem anordnenden Gericht zur

Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend.

(6) Die im Rahmen des Abgleichs nach Absatz 1 Satz 1 erhobenen Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, sofern sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt aufweisen. Die Weiterverarbeitung der beim Abgleich erhobenen Daten ist im Übrigen unzulässig.

(7) Bei jeder Maßnahme nach Absatz 1 Satz 1 ist die Bezeichnung der eingesetzten automatisierten Anwendung zur Datenverarbeitung, der Zeitpunkt ihres Einsatzes sowie die Organisationseinheit einschließlich einer individuellen Kennung der Person, die die Maßnahme durchführt, zu protokollieren. Nach Beendigung einer Maßnahme nach Absatz 1 ist die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist.

(8) Soweit zur Durchführung des Abgleichs nach Absatz 1 Satz 1 Dritte im Wege der Auftragsverarbeitung für die Bundespolizei tätig werden, müssen diese ihren Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten zur Durchführung der Maßnahme nach Absatz 1 Satz 1 ist nur innerhalb der Europäischen Union, einschließlich der Schengen-assoziierten Staaten, zulässig. Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 1 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Durch organisatorische und technische Maßnahmen ist zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(9) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit führt Kontrollen bezüglich der Datenverarbeitung der Maßnahme nach Absatz 1 Satz 1 mindestens alle zwei Jahre durch.

(10) Die Bundesregierung bestimmt vor dem Einsatz von Maßnahmen nach Absatz 1 Satz 1 durch Rechtsverordnung ohne Zustimmung des Bundesrats nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und, soweit eine Speicherung der abzugleichenden, öffentlich zugänglichen Lichtbild- Video- und Audiodateien für die Durchführung von Maßnahmen nach Absatz 1 technisch erforderlich ist, nähere Vorgaben zu Art, Umfang und Dauer. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. Eingabe- und Zugangsberechtigung,
2. Speicher- und Löschfristen,
3. Art der zu speichernden Daten,
4. Personenkreis, der von der Speicherung betroffen ist,
5. Dauer der Speicherung,

6. Protokollierung“ ‘

3. Artikel 3 wird wie folgt geändert:

a) Nummer 1 wird wie folgt gefasst:

‚1. In der Inhaltsübersicht wird nach der Angabe zu § 98c folgende Angabe eingefügt:

„§ 98 Nachträglicher Abgleich biometrischer Daten mit im Internet allgemein öffentlich zugänglichen Daten mittels einer automatisierten Anwendung zur Datenverarbeitung; Verordnungsermächtigung“.‘

b) Nummer 2 wird wie folgt gefasst:

‚2. Nach § 98c wird folgender § 98d eingefügt:

„§ 98d

Nachträglicher Abgleich biometrischer Daten mit im Internet allgemein öffentlich zugänglichen Daten mittels einer automatisierten Anwendung zur Datenverarbeitung; Verordnungsermächtigung

(1) Zur Identitätsfeststellung oder Ermittlung des Aufenthaltsorts eines Beschuldigten oder eines Verletzten durch Erkennung des Gesichts und der Stimme dürfen deren biometrische Daten aus einem Strafverfahren mit biometrischen Daten aus im Internet allgemein öffentlich zugänglichen Lichtbild-, Audio- und Videodateien nachträglich mittels einer automatisierten Anwendung zur Datenverarbeitung abgeglichen werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100b Absatz 2 bezeichnete besonders schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat,
2. die Tat auch im Einzelfall besonders schwer wiegt und
3. die Identitätsfeststellung oder die Ermittlung des Aufenthaltsortes auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Ein Abgleich mit Daten nach Satz 1 aus im Internet öffentlich zugänglichen in Echtzeit erhobenen Daten ist ausgeschlossen. Die Identitätsfeststellung oder Ermittlung des Aufenthaltsorts des Verletzten hat zu unterbleiben, wenn überwiegende schutzwürdige Interessen des Verletzten entgegenstehen.

(2) Maßnahmen nach Absatz 1 dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Tagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. die Person, zu deren Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird,

2. die biometrischen Daten aus dem Strafverfahren, die dieser Person zuzuordnen sind und die zum Abgleich herangezogen werden sollen,

3. der Tatvorwurf, auf Grund dessen die Maßnahme angeordnet wird, und

4. die zur Datenverarbeitung eingesetzte automatisierte Anwendung.

(3) In der Begründung der Anordnung sind die Voraussetzungen für die Maßnahme nach Absatz 1 und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen die bestimmten Tatsachen, die den Verdacht begründen, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme, die wesentlichen Einzelheiten zur technischen Funktionsweise der automatisierten Anwendung zur Datenverarbeitung sowie die Subsidiarität zu anderen Maßnahmen anzugeben.

(4) § 100d Absatz 1 bis 3 gilt entsprechend.

(5) Die im Rahmen des Abgleichs nach Absatz 1 erhobenen Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, soweit sie keinen konkreten Ermittlungsansatz aufweisen. Dies gilt auch für sonstige erhobene Daten, soweit schutzwürdige Interessen des Betroffenen im Einzelfall gegenüber dem Strafverfolgungsinteresse überwiegen. Im Fall des Absatzes 2 Satz 3 sind alle bereits erhobenen Daten unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen. Die Weiterverarbeitung der beim Abgleich erhobenen Daten ist im Übrigen unzulässig.

(6) Bei jeder Maßnahme ist die Bezeichnung der eingesetzten automatisierten Anwendung zur Datenverarbeitung, der Zeitpunkt ihres Einsatzes und die Organisationseinheit, die die Maßnahme durchführt, einschließlich einer individuellen Kennung der Person, die die Maßnahme durchführt, zu protokollieren. Nach Beendigung einer Maßnahme nach Absatz 1 ist die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist.

(7) Dritte dürfen im Rahmen einer Auftragsverarbeitung nur tätig werden, wenn sichergestellt ist, dass die Verarbeitung personenbezogener Daten im Rahmen des Abgleichs nur durch Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete oder zur Geheimhaltung verpflichtete Mitarbeiterinnen oder Mitarbeiter erfolgt. § 1 Absatz 2, 3 und 4 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Durch organisatorische und technische Maßnahmen ist zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind. Sofern zur Durchführung des Abgleichs nach Absatz 1 Satz 1 Dritte im Wege der Auftragsverarbeitung tätig werden, müssen diese ihren Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten zur Durchführung der Maßnahme nach Absatz 1 Satz 1 ist nur innerhalb der Europäischen Union, einschließlich der Schengen-assoziierten Staaten, zulässig.

(8) Die Bundesregierung bestimmt vor dem Einsatz von Maßnahmen nach Absatz 1 durch Rechtsverordnung ohne Zustimmung des Bundesrats nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und, sofern eine Speicherung der abzugleichenden, allgemein öffentlich zugänglichen Lichtbild- Video- und Audiodateien für die Durchführung von Maßnahmen nach Absatz 1 technisch erforderlich ist, nähere Vorgaben zu Art, Umfang und Dauer. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. nähere Vorgaben für die Eingabe- und Zugangsberechtigung,
2. die Speicher- und Löschfristen,
3. die Art und den Umfang der zu speichernden Daten, und
4. die Dauer der Speicherung

(9) Die Stelle, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist, führt mindestens alle zwei Jahre Kontrollen über die die Maßnahme nach Absatz 1 betreffende Datenverarbeitung durch.“ ‘

„§ 98d

Nachträglicher Abgleich Nummer 3 Buchstabe b wird wie folgt gefasst:

‚b) Nach Absatz 4 Satz 1 Nummer 1 wird folgende Nummer 1a eingefügt:

„1a. des § 98d die Person, zu deren Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird.“ ‘

4. Nach Artikel 3 wird folgender Artikel 4 eingefügt:

„ Artikel 4

Evaluierung

Das Bundesministerium des Innern und für Heimat und das Bundesministerium der Justiz beauftragen gemeinsam eine fachunabhängige wissenschaftliche Einrichtung, die Anwendung von §§ 10b, 16a, 39a, 63b des Bundeskriminalamtgesetzes, §§ 34a und 34b des Bundespolizeigesetzes und § 98d der Strafprozessordnung zu evaluieren. Der Evaluierungszeitraum beginnt am [1. Januar des auf das Datum des Inkrafttretens dieses Gesetzes folgenden Jahres] und beträgt drei Jahre.“

5. Der bisherige Artikel 4 wird Artikel 5.

Begründung

Zu Artikel 1:

1) Übergreifend:

Soweit der Anwendungsbereich der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) eröffnet ist, gelten die jeweiligen Vorgaben unmittelbar und sind bei der Entwicklung und Nutzung von KI-Systemen zu beachten. Zwingend sicherzustellen ist insbesondere, dass die Rechtskonformität der verwendeten KI-Systeme entsprechend der Verordnung zertifiziert ist. Dies ist in geeigneter Form in der Rechtsverordnung zu konkretisieren. Zur Erprobung von KI-Systemen sollte das Instrument der KI-Reallabore Anwendung finden.

2) Zu den §§ 10b, 39a, 63b BKAG-E:

Unter allgemein öffentlich zugängliche Daten fallen solche Daten, die von jedermann verwendet werden können, beispielsweise aus sozialen Medien, soweit sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten (BT-Drs. 20/12806, S. 18). Konkretisierend fallen darunter Daten, wenn sie jede Person ohne oder nach vorheriger Registrierung, Genehmigung oder Entgeltzahlung nutzen kann. Nicht umfasst sind Daten, die einer spezifischen Schwelle unterzogen sind, beispielsweise der Einstellung von Daten in sozialen Medien für einen begrenzten Kreis, dessen Zugang einer Kontrolle unterzogen wird. Privatkommunikation über Messenger-Dienste von sozialen Medien können nicht von der Maßnahme erfasst werden.

3) Zu § 16a BKAG-E:

§ 16a des Bundeskriminalamtgesetzes sieht die automatisierte Datenanalyse des polizeilichen Datenbestands vor. Eine Delegation der Durchführung Datenanalyse an Dritte und eine Übermittlung an diese zu diesem Zweck erlaubt die Vorschrift nicht.

Zu Artikel 2:

Die Änderung in Artikel 2 enthält eine redaktionelle Anpassung. Die Verordnungsermächtigung in § 42 Absatz 7 des Waffengesetzes ist aus Gründen der Rechtssystematik in § 42b Absatz 2 Waffengesetz verschoben worden. Insofern ist eine redaktionelle Verweisanpassung erforderlich.

Auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes ist für die Abwehr von Gefahren für die Nutzerinnen und Nutzer des Bahnverkehrs sowie die Anlagen des Bahnbetriebs die Bundespolizei zuständig. Die Bundespolizei wird auf

Grundlage des neuen § 22 Absatz 1b des Bundespolizeigesetzes tätig, sofern eine Waffenverbotszone nach § 42b Absatz 2 des Waffengesetzes besteht oder eine Allgemeinverfügung, die das Mitführen von Waffen oder bestimmten gefährlichen Gegenständen verbietet. § 22 Absatz 1b ermöglicht es der Bundespolizei, in diesen Bereichen strichprobenartige und anlasslose Kontrollen durchzuführen. Anders lassen sich Führensverbote von Waffen- und Messern nicht effektiv durchsetzen. Insbesondere Messer können verdeckt am Körper getragen werden. Ohne die Möglichkeit einer Durchsuchung der Person würde die Kontrolle und die Durchsetzung von Führensverboten sonst teilweise leerlaufen. Indem Kontrollen jederzeitig und damit für den Betroffenen nicht berechenbar oder planbar durchgeführt werden können, hat dies zugleich eine abstrakt abschreckende Wirkung auf potentielle Täter. Andererseits gilt es zu beachten, dass diese Kontrollen nur in einem räumlich und ggf. auch zeitlich begrenzten Bereich zulässig sind.

Bei Ausübung der Kontrollen hat die zuständige Behörde das ihr obliegende Entschließungsermessen anhand rechtstaatlicher Grundsätze auszuüben. Ob im konkreten Einzelfall vor Ort eine Kontrolle durchgeführt wird, bemisst sich anhand aktueller Lageerkenntnisse im Einzelfall. Ein maßgebliches Kriterium kann dabei u.a. sein, zu welchem Zeitpunkt auf Grund polizeilicher Erkenntnisse mit den meisten Verstößen zu rechnen ist. § 22 Absatz 1b stellt zudem klar, dass die Kontrollen nicht allein an Merkmale im Sinne des Artikels 3 Absatz 3 des Grundgesetzes anknüpfen dürfen. Die Kontrollen sind grundsätzlich anlasslos und stichprobenartig möglich. Ein sachlicher Grund für eine Steuerung der Kontrollen im Einzelfall können aber besondere Lageerkenntnisse sein.

Zu Artikel 3:

Zu § 98d StPO-E

Als Eingriffsschwelle für die Maßnahme ist der Verdacht einer besonders schweren Straftat nach § 100b der Strafprozessordnung vorgesehen, die auch im Einzelfall besonders schwer wiegt.

Der Begriff „öffentlich zugänglich“ wird durch den Zusatz „allgemein“ ergänzt. Unter allgemein öffentlich zugängliche Daten fallen solche Daten, die von jedermann verwendet werden können, beispielsweise aus sozialen Medien, soweit sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten (BT-Drs. 20/12806, S. 18). Konkretisierend fallen darunter Daten, wenn sie jede Person ohne oder nach vorheriger Registrierung, Genehmigung oder Entgeltzahlung nutzen kann. Nicht umfasst sind Daten, die einer spezifischen Schwelle unterzogen sind, beispielsweise der Einstellung von Daten in sozialen Medien für einen begrenzten Kreis, dessen Zugang einer Kontrolle unterzogen wird. Privatkommunikation über Messenger-Dienste von sozialen Medien können nicht von der Maßnahme erfasst werden.

Die Regelung in Absatz 7 stellt sicher, dass Dritte im Rahmen einer Auftragsverarbeitung nur tätig werden dürfen, wenn sichergestellt ist, dass die Verarbeitung personenbezogener Daten im Rahmen des Abgleichs nur durch Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete oder zur Geheimhaltung verpflichtete Mitarbeiterinnen oder Mitarbeiter erfolgt. Zudem wird sichergestellt, dass eine Datenverarbeitung stets im Geltungsbereich des EU-Datenschutzregimes stattfindet.

Absatz 8 sieht eine Verordnungsermächtigung vor. Mit der Rechtsverordnung soll das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und, sofern eine Speicherung der abzugleichenden, allgemein öffentlich zugänglichen Lichtbild- Video- und Audiodateien für die Durchführung von Maßnahmen nach Absatz 1 technisch erforderlich ist,

nähere Vorgaben zu Art, Umfang und Dauer der Speicherung bestimmt werden. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sind hierbei anzuhören.

Zu Artikel 4:

Der fachunabhängigen wissenschaftlichen Einrichtung, die die Anwendung der Vorschriften evaluiert, sind die für die Erledigung des Auftrags erforderlichen Informationen zur Verfügung zu stellen. Dazu gehören insbesondere statistische Informationen über Häufigkeit und Dauer der Maßnahmen, detaillierte Einblicke in die Funktionsweise und konkrete Nutzung der eingesetzten Systeme sowie in Leitfäden und Verfahrensvorschriften, in einzelne Verfahrensakten sowie eine teilnehmende Beobachtung bei Durchführung der Maßnahmen. Sofern notwendig sind die beteiligten Einrichtungen und Personen auf geeignete Weise zur Geheimhaltung zu verpflichten.

Die Evaluierung ist mit der Evaluierung der Anwendung von § 15b AsylG zu verbinden.