

TE Dsk BescheidBeschwerde 2026/7/22 2026-0.396.500

JUSLINE Entscheidung

🕒 Veröffentlicht am 22.07.2026

Norm

DSG §1 Abs1

DSG §1 Abs2

DSG §36 Abs1

DSG §36 Abs2 Z1

DSG §36 Abs2 Z2

DSG §36 Abs2 Z13

DSG §38

DSG §39 Z1

SPG §64 Abs1

SPG §64 Abs2

SPG §64 Abs3

SPG §65 Abs1

SPG §75 Abs1

SPG §75 Abs1a

SPG §75 Abs2

DSGVO Art2 Abs2 litd

DSRL-PJ Art10

DSRL-PJ ErwGr37

WP258 Stellungnahme Datenschutz bei der Strafverfolgung Seite7

WP258 Stellungnahme Datenschutz bei der Strafverfolgung Seite8

WP258 Stellungnahme Datenschutz bei der Strafverfolgung Seite9

1. DSG Art. 1 § 1 heute

2. DSG Art. 1 § 1 gültig ab 01.01.2014 zuletzt geändert durch BGBl. I Nr. 51/2012

3. DSG Art. 1 § 1 gültig von 01.01.2000 bis 31.12.2013

1. DSG Art. 1 § 1 heute

2. DSG Art. 1 § 1 gültig ab 01.01.2014 zuletzt geändert durch BGBl. I Nr. 51/2012

3. DSG Art. 1 § 1 gültig von 01.01.2000 bis 31.12.2013

1. DSG Art. 2 § 36 heute

2. DSG Art. 2 § 36 gültig ab 29.06.2024 zuletzt geändert durch BGBl. I Nr. 62/2024

3. DSG Art. 2 § 36 gültig von 01.12.2021 bis 28.06.2024 zuletzt geändert durch BGBl. I Nr. 148/2021

4. DSG Art. 2 § 36 gültig von 25.05.2018 bis 30.11.2021 zuletzt geändert durch BGBl. I Nr. 24/2018

5. DSGVO Art. 2 § 36 gültig von 25.05.2018 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 120/2017
6. DSGVO Art. 2 § 36 gültig von 01.01.2014 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 83/2013
7. DSGVO Art. 2 § 36 gültig von 01.07.2010 bis 31.12.2013 zuletzt geändert durch BGBl. I Nr. 133/2009
8. DSGVO Art. 2 § 36 gültig von 01.01.2010 bis 30.06.2010 zuletzt geändert durch BGBl. I Nr. 133/2009
9. DSGVO Art. 2 § 36 gültig von 01.01.2000 bis 31.12.2009

5. SPG § 64 gültig von 01.10.2002 bis 30.06.2014 zuletzt geändert durch BGBl. I Nr. 104/2002
6. SPG § 64 gültig von 01.09.1999 bis 30.09.2002 zuletzt geändert durch BGBl. I Nr. 146/1999
7. SPG § 64 gültig von 01.05.1993 bis 31.08.1999

1. SPG § 64 heute
2. SPG § 64 gültig ab 25.05.2018 zuletzt geändert durch BGBl. I Nr. 29/2018
3. SPG § 64 gültig von 01.08.2016 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 61/2016
4. SPG § 64 gültig von 01.07.2014 bis 31.07.2016 zuletzt geändert durch BGBl. I Nr. 43/2014
5. SPG § 64 gültig von 01.10.2002 bis 30.06.2014 zuletzt geändert durch BGBl. I Nr. 104/2002
6. SPG § 64 gültig von 01.09.1999 bis 30.09.2002 zuletzt geändert durch BGBl. I Nr. 146/1999
7. SPG § 64 gültig von 01.05.1993 bis 31.08.1999

1. SPG § 64 heute
2. SPG § 64 gültig ab 25.05.2018 zuletzt geändert durch BGBl. I Nr. 29/2018
3. SPG § 64 gültig von 01.08.2016 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 61/2016
4. SPG § 64 gültig von 01.07.2014 bis 31.07.2016 zuletzt geändert durch BGBl. I Nr. 43/2014
5. SPG § 64 gültig von 01.10.2002 bis 30.06.2014 zuletzt geändert durch BGBl. I Nr. 104/2002
6. SPG § 64 gültig von 01.09.1999 bis 30.09.2002 zuletzt geändert durch BGBl. I Nr. 146/1999
7. SPG § 64 gültig von 01.05.1993 bis 31.08.1999

1. SPG § 65 heute
2. SPG § 65 gültig ab 07.03.2023 zuletzt geändert durch BGBl. I Nr. 206/2021
3. SPG § 65 gültig von 25.05.2018 bis 06.03.2023 zuletzt geändert durch BGBl. I Nr. 29/2018
4. SPG § 65 gültig von 01.08.2016 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 61/2016
5. SPG § 65 gültig von 01.07.2014 bis 31.07.2016 zuletzt geändert durch BGBl. I Nr. 43/2014
6. SPG § 65 gültig von 01.04.2012 bis 30.06.2014 zuletzt geändert durch BGBl. I Nr. 13/2012
7. SPG § 65 gültig von 01.01.2008 bis 31.03.2012 zuletzt geändert durch BGBl. I Nr. 114/2007
8. SPG § 65 gültig von 01.10.2002 bis 31.12.2007 zuletzt geändert durch BGBl. I Nr. 104/2002
9. SPG § 65 gültig von 11.08.2000 bis 30.09.2002 zuletzt geändert durch BGBl. I Nr. 85/2000
10. SPG § 65 gültig von 01.09.1999 bis 10.08.2000 zuletzt geändert durch BGBl. I Nr. 146/1999
11. SPG § 65 gültig von 01.05.1993 bis 31.08.1999

1. SPG § 75 heute
2. SPG § 75 gültig ab 23.07.2024 zuletzt geändert durch BGBl. I Nr. 122/2024
3. SPG § 75 gültig von 25.05.2018 bis 22.07.2024 zuletzt geändert durch BGBl. I Nr. 29/2018
4. SPG § 75 gültig von 01.03.2016 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 5/2016
5. SPG § 75 gültig von 01.04.2012 bis 29.02.2016 zuletzt geändert durch BGBl. I Nr. 13/2012
6. SPG § 75 gültig von 01.01.2008 bis 31.03.2012 zuletzt geändert durch BGBl. I Nr. 114/2007
7. SPG § 75 gültig von 01.10.2002 bis 31.12.2007 zuletzt geändert durch BGBl. I Nr. 104/2002
8. SPG § 75 gültig von 01.05.1993 bis 30.09.2002

1. SPG § 75 heute
2. SPG § 75 gültig ab 23.07.2024 zuletzt geändert durch BGBl. I Nr. 122/2024
3. SPG § 75 gültig von 25.05.2018 bis 22.07.2024 zuletzt geändert durch BGBl. I Nr. 29/2018
4. SPG § 75 gültig von 01.03.2016 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 5/2016
5. SPG § 75 gültig von 01.04.2012 bis 29.02.2016 zuletzt geändert durch BGBl. I Nr. 13/2012
6. SPG § 75 gültig von 01.01.2008 bis 31.03.2012 zuletzt geändert durch BGBl. I Nr. 114/2007
7. SPG § 75 gültig von 01.10.2002 bis 31.12.2007 zuletzt geändert durch BGBl. I Nr. 104/2002
8. SPG § 75 gültig von 01.05.1993 bis 30.09.2002

1. SPG § 75 heute
2. SPG § 75 gültig ab 23.07.2024 zuletzt geändert durch BGBl. I Nr. 122/2024
3. SPG § 75 gültig von 25.05.2018 bis 22.07.2024 zuletzt geändert durch BGBl. I Nr. 29/2018
4. SPG § 75 gültig von 01.03.2016 bis 24.05.2018 zuletzt geändert durch BGBl. I Nr. 5/2016
5. SPG § 75 gültig von 01.04.2012 bis 29.02.2016 zuletzt geändert durch BGBl. I Nr. 13/2012

6. SPG § 75 gültig von 01.01.2008 bis 31.03.2012 zuletzt geändert durch BGBl. I Nr. 114/2007
7. SPG § 75 gültig von 01.10.2002 bis 31.12.2007 zuletzt geändert durch BGBl. I Nr. 104/2002
8. SPG § 75 gültig von 01.05.1993 bis 30.09.2002

Text

GZ: 2026-0.396.500 vom 22. Juli 2026 (Verfahrenszahl: DSB-D124.1003/25)

[Anmerkung Bearbeiter/in: Namen und Firmen, Rechtsformen und Produktbezeichnungen, Adressen (inkl. URLs, IP- und E-Mail-Adressen), Aktenzahlen (und dergleichen), statistische Angaben etc., sowie deren Initialen und Abkürzungen können aus Pseudonymisierungsgründen abgekürzt und/oder verändert sein. Offenkundige Rechtschreib-, Grammatik- und Satzzeichenfehler wurden korrigiert.]

Die Bezeichnung (Firma) des Herstellers der eingesetzten Software geht aus öffentlich zugänglichen Dokumenten (insbesondere der Beantwortung parlamentarischer Anfragen) hervor.]

BESCHEID

SPRUCH

Die Datenschutzbehörde entscheidet über die Datenschutzbeschwerde von Paul A*** (beschwerdeführende Partei), vertreten durch die B*** Grundrechte-Schutzvereinigung, vom 18. April 2025 gegen die Landespolizeidirektion Wien (beschwerdegegnerische Partei) wegen behaupteter Verletzung im Recht auf Geheimhaltung wie folgt:

?

Der Beschwerde wird stattgegeben und es wird festgestellt, dass die beschwerdegegnerische Partei die beschwerdeführende Partei dadurch im Recht auf Geheimhaltung verletzt hat, indem sie am 5. April 2023 rechtsgrundlos einen Abgleich von Lichtbildern der beschwerdeführenden Partei mittels Gesichtserkennungssoftware durchgeführt hat.

Rechtsgrundlagen: §§ 1 Abs. 1 und Abs. 2, 18 Abs. 1, 24 Abs. 1 und Abs. 5, 36 Abs. 2 Z 1, Z 2 und Z 13, 38 sowie 39 des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999 idgF; §§ 64, 65 Abs. 1 sowie 75 des Sicherheitspolizeigesetzes (SPG), BGBl. Nr. 566/1991 idF idgF. Rechtsgrundlagen: Paragraphen eins, Absatz eins und Absatz 2, 18, Absatz eins, 24, Absatz eins und Absatz 5, 36, Absatz 2, Ziffer eins,, Ziffer 2 und Ziffer 13, 38, sowie 39 des Datenschutzgesetzes (DSG), Bundesgesetzblatt Teil eins, Nr. 165 aus 1999, idgF; Paragraphen 64, 65, Absatz eins, sowie 75 des Sicherheitspolizeigesetzes (SPG), Bundesgesetzblatt Nr. 566 aus 1991, in der Fassung Bundesgesetzblatt Nr. 662 aus 1992, idgF.

BEGRÜNDUNG

A. Vorbringen der Parteien und Verfahrensgang

1. Die beschwerdeführende Partei (nachfolgend auch: „bFP“) erhob am 18. April 2025 Beschwerde gegen die beschwerdegegnerische Partei (nachfolgend auch: „bgP“) wegen einer behaupteten Verletzung im Recht auf Geheimhaltung aufgrund eines behaupteterweise unrechtmäßigen Einsatzes einer Gesichtserkennungssoftware durch die bgP.
2. Die beschwerdegegnerische Partei gab dazu jeweils mit Schreiben vom 4. Juni 2025, vom 28. August 2025 und vom 24. Oktober 2025 Stellungnahmen ab.
3. Die beschwerdeführende Partei äußerte sich dazu jeweils mit Stellungnahme vom 26. Juni 2025 und vom 15. Dezember 2025.

B. Beschwerdegegenstand

Beschwerdegegenstand ist die Frage, ob die bgP die bFP dadurch im Recht auf Geheimhaltung verletzt hat, indem sie im Zuge von Ermittlungen zur Ausforschung unbekannter Tatverdächtiger ein Lichtbild der bFP mittels Gesichtserkennungssoftware mit den in der Zentralen Erkennungsdienstlichen Evidenz vorhandenen Lichtbildern abgeglichen hat.

C. Sachverhaltsfeststellungen

1. Das Bundesministerium für Inneres setzt seit spätestens 2020 im polizeilichen Bereich bei Verdacht der Begehung

vorsätzlicher gerichtlich strafbarer Handlungen bei unbekannten Tatverdächtigen die Gesichtserkennungssoftware „FaceVACS-DBScan“ des Herstellers Cognitec Systems GmbH zum digitalen und automatisierten Bildabgleich ein. Der Bildabgleich erfolgt dabei ausschließlich mit den in der Datenbank „Zentrale Erkennungsdienstliche Evidenz“ (nachfolgend auch: „EDE“) vorhandenen Bilddaten.

2. Am 27. März 2023 nahm die bFP an einer Demonstration gegen die Europäische Gaskonferenz in Wien teil, bei welcher es zu Ausschreitungen kam und im Zuge dessen die bFP wegen des Verdachtes der Begehung mit gerichtlicher Strafe bedrohten vorsätzlichen Handlungen gem. §§ 12, 269 StGB und § 274 StGB von den einschreitenden Beamt*innen der bgP festgenommen wurde. Mangels Identitätsbekanntgabe durch die bFP wurde ein Lichtbild des Gesichtes der bFP von den Beamt*innen erstellt. 2. Am 27. März 2023 nahm die bFP an einer Demonstration gegen die Europäische Gaskonferenz in Wien teil, bei welcher es zu Ausschreitungen kam und im Zuge dessen die bFP wegen des Verdachtes der Begehung mit gerichtlicher Strafe bedrohten vorsätzlichen Handlungen gem. Paragraphen 12, 269, StGB und Paragraph 274, StGB von den einschreitenden Beamt*innen der bgP festgenommen wurde. Mangels Identitätsbekanntgabe durch die bFP wurde ein Lichtbild des Gesichtes der bFP von den Beamt*innen erstellt.

Am 5. April 2023 glichen Beamt*innen der bgP das Lichtbild der bFP unter Verwendung der unter Punkt C.1. genannten Gesichtserkennungssoftware mit dem Datenbestand der Datenanwendung EDE ab. In dem „Ergebnisbericht zum Gesichtserkennungsabgleich“ eines Suchbildes wurde ein Lichtbild der bFP mit einem Score von 91,15 % an erster Stelle ausgewiesen.

Infolgedessen wurde die bFP als Beschuldigte geführt und fand am 6. Juni 2023 eine Vernehmung der bFP statt, im Zuge dieser die bFP erneut erkennungsdienstlich behandelt worden ist. Mit Schreiben der Staatsanwaltschaft Wien vom 8. Februar 2024 wurde das Ermittlungsverfahren gegen die bFP eingestellt.

3. Infolge eines entsprechenden Antrags erteilte die bgP der bFP am 19. April 2024 eine datenschutzrechtliche Auskunft. Die bFP erlangte dadurch erstmals Kenntnis von dem Lichtbildabgleich vom 5. April 2023.

Beweiswürdigung: Die getroffenen Feststellungen beruhen auf den schriftlichen Eingaben der Verfahrensparteien sowie auf den durch die bFP in Kopie vorgelegten Unterlagen. Des Weiteren auf der Beantwortung der Anfrage #1709 vom 19. April 2019 durch den Bundesminister für Inneres vom 11. Juni 2019, abrufbar unter www.fragdenstaat.at sowie auf der Anfragebeantwortung des BMI 3457/AB vom 20. November 2020 zu 3445/J, 3500/AB vom 23. November 2020 zu 3483/J und 3494/AB vom 23. November 2020 zu 3457/J, alles abrufbar unter www.parlament.gv.at (letztmalig abgerufen durch die Datenschutzbehörde am 7. Mai 2026).

D. In rechtlicher Hinsicht folgt daraus:

D1. Zum Beschwerdegegenstand

Gem. § 24 Abs. 1 DSG hat jede betroffene Person das Recht auf Beschwerde bei der Datenschutzbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO oder gegen § 1 oder Artikel 2 des 1. Hauptstücks des DSG verstößt. Gem. Paragraph 24, Absatz eins, DSG hat jede betroffene Person das Recht auf Beschwerde bei der Datenschutzbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO oder gegen Paragraph eins, oder Artikel 2 des 1. Hauptstücks des DSG verstößt.

Sowohl die Datenschutzbehörde als auch das BVwG vertreten in ständiger Judikatur, dass bei antragsgebunden Fällen - wie insbesondere dem Beschwerdeverfahren gemäß Art. 77 DSGVO iVm § 24 Abs. 1 DSG - der Inhalt des Antrags (vorliegend: der Beschwerde) den Prozessgegenstand des Verwaltungsverfahrens (vorliegend: den Beschwerdegegenstand) konstituiert und begrenzt (vgl. etwa BVwG Erkenntnis vom 17. Mai 2022, W214 2233132-1). Sowohl die Datenschutzbehörde als auch das BVwG vertreten in ständiger Judikatur, dass bei antragsgebunden Fällen - wie insbesondere dem Beschwerdeverfahren gemäß Artikel 77, DSGVO in Verbindung mit Paragraph 24, Absatz eins, DSG - der Inhalt des Antrags (vorliegend: der Beschwerde) den Prozessgegenstand des Verwaltungsverfahrens (vorliegend: den Beschwerdegegenstand) konstituiert und begrenzt vergleiche etwa BVwG Erkenntnis vom 17. Mai 2022, W214 2233132-1).

Für den vorliegenden Fall ist daher festzuhalten, dass sich die Beschwerde der bFP ausdrücklich nicht gegen die erkennungsdienstliche Behandlung (Aufnahme des Lichtbildes) oder gegen die Speicherung von erkennungsdienstlichen Daten in der EDE, sondern ausschließlich gegen den Lichtbildabgleich mittels

Gesichtserkennungssoftware richtete.

Damit ist ausschließlich dieser Vorgang auf seine Rechtmäßigkeit hin zu überprüfen.

D2. Zur behaupteten Verletzung im Recht auf Geheimhaltung

a.

Zum Anwendungsbereich

Nach § 1 Abs. 1 DSG hat jede Person Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse darin besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf die Betroffene einem Geheimhaltungsanspruch nicht zugänglich sind. Nach Paragraph eins, Absatz eins, DSG hat jede Person Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse darin besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf die Betroffene einem Geheimhaltungsanspruch nicht zugänglich sind.

Da der verfahrensgegenständliche Lichtbildabgleich in unmittelbarem Zusammenhang mit einem strafrechtlichen Ermittlungsverfahren steht und es sich bei der bgP um die zuständige Behörde handelt, sind gemäß § 36 Abs. 1 DSG die Bestimmungen des 3. Hauptstücks des DSG in Umsetzung der Richtlinie (EU) 2016/680 (in weiterer Folge: DSRL-PJ) - unter gleichzeitigem Ausschluss der Bestimmungen der DSGVO gemäß Art. 2 Abs. 2 lit. d - anzuwenden. Da der verfahrensgegenständliche Lichtbildabgleich in unmittelbarem Zusammenhang mit einem strafrechtlichen Ermittlungsverfahren steht und es sich bei der bgP um die zuständige Behörde handelt, sind gemäß Paragraph 36, Absatz eins, DSG die Bestimmungen des 3. Hauptstücks des DSG in Umsetzung der Richtlinie (EU) 2016/680 (in weiterer Folge: DSRL-PJ) - unter gleichzeitigem Ausschluss der Bestimmungen der DSGVO gemäß Artikel 2, Absatz 2, Litera d, - anzuwenden.

Weiters handelt es sich bei einem (automatisierten) Lichtbildabgleich unbestrittenermaßen um eine Verarbeitung von personenbezogenen Daten iSv. § 36 Abs. 2 Z 1 und Z 2 DSG. Weiters handelt es sich bei einem (automatisierten) Lichtbildabgleich unbestrittenermaßen um eine Verarbeitung von personenbezogenen Daten iSv. Paragraph 36, Absatz 2, Ziffer eins und Ziffer 2, DSG.

Darüber hinaus stellen Gesichtsbilder biometrische Daten iSv. § 36 Abs. 2 Z 13 DSG dar. Darüber hinaus stellen Gesichtsbilder biometrische Daten iSv. Paragraph 36, Absatz 2, Ziffer 13, DSG dar.

Gemäß § 38 DSG ist die Verarbeitung personenbezogener Daten, soweit sie nicht zur Wahrung lebenswichtiger Interessen einer Person erforderlich ist, nur rechtmäßig, soweit sie gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, vorgesehen und für die Erfüllung einer Aufgabe erforderlich und verhältnismäßig ist, die von der zuständigen Behörde zu den in § 36 Abs. 1 genannten Zwecken wahrgenommen wird. Gemäß Paragraph 38, DSG ist die Verarbeitung personenbezogener Daten, soweit sie nicht zur Wahrung lebenswichtiger Interessen einer Person erforderlich ist, nur rechtmäßig, soweit sie gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, vorgesehen und für die Erfüllung einer Aufgabe erforderlich und verhältnismäßig ist, die von der zuständigen Behörde zu den in Paragraph 36, Absatz eins, genannten Zwecken wahrgenommen wird.

Die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person für die in § 36 Abs. 1 genannten Zwecke ist gemäß § 39 DSG nur zulässig, wenn die Verarbeitung unbedingt erforderlich ist und wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden und die Verarbeitung gemäß § 38 zulässig ist. Die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person für die in Paragraph 36, Absatz eins, genannten Zwecke ist gemäß Paragraph 39, DSG nur zulässig, wenn die Verarbeitung unbedingt erforderlich ist und wirksame Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden und die Verarbeitung gemäß Paragraph 38, zulässig ist.

b.

Zur Rechtsgrundlage

Die bgP brachte im Rahmen ihrer Stellungnahme vor, dass das Gesichtserkennungssystem ein Subsystem der EDE sei. Konkrete Rechtsgrundlage für den verfahrensgegenständlichen Lichtbildabgleich sei § 75 Abs. 2 SPG. Die bgP brachte im Rahmen ihrer Stellungnahme vor, dass das Gesichtserkennungssystem ein Subsystem der EDE sei. Konkrete

Rechtsgrundlage für den verfahrensgegenständlichen Lichtbildabgleich sei Paragraph 75, Absatz 2, SPG.

Vorab ist festzuhalten, dass unter Erkennungsdienst laut § 64 Abs. 1 SPG das Ermitteln personenbezogener Daten durch erkennungsdienstliche Maßnahmen sowie das weitere Verarbeiten und Übermitteln dieser Daten zu verstehen ist. Laut § 64 Abs. 2 SPG sind erkennungsdienstliche Maßnahmen technische Verfahren zur Feststellung von biometrischen oder genetischen Daten (§ 36 Abs. 2 Z 12 und 13 DSG), wie insbesondere die Abnahme von Papillarlinienabdrücken, die Vornahme von Mundhöhlenabstrichen, die Herstellung von Abbildungen, die Vornahme von Messungen oder die Erhebung von Stimmproben, sowie die Feststellung äußerlicher körperlicher Merkmale und die Erhebung von Schriftproben eines Menschen zum Zweck der Wiedererkennung. Erkennungsdienstliche Behandlung ist laut § 64 Abs. 3 SPG das Ermitteln personenbezogener Daten durch erkennungsdienstliche Maßnahmen, an dem der Betroffene mitzuwirken hat. Vorab ist festzuhalten, dass unter Erkennungsdienst laut Paragraph 64, Absatz eins, SPG das Ermitteln personenbezogener Daten durch erkennungsdienstliche Maßnahmen sowie das weitere Verarbeiten und Übermitteln dieser Daten zu verstehen ist. Laut Paragraph 64, Absatz 2, SPG sind erkennungsdienstliche Maßnahmen technische Verfahren zur Feststellung von biometrischen oder genetischen Daten (Paragraph 36, Absatz 2, Ziffer 12 und 13 DSG), wie insbesondere die Abnahme von Papillarlinienabdrücken, die Vornahme von Mundhöhlenabstrichen, die Herstellung von Abbildungen, die Vornahme von Messungen oder die Erhebung von Stimmproben, sowie die Feststellung äußerlicher körperlicher Merkmale und die Erhebung von Schriftproben eines Menschen zum Zweck der Wiedererkennung. Erkennungsdienstliche Behandlung ist laut Paragraph 64, Absatz 3, SPG das Ermitteln personenbezogener Daten durch erkennungsdienstliche Maßnahmen, an dem der Betroffene mitzuwirken hat.

Gemäß § 65 Abs. 1 SPG sind die Sicherheitsbehörden ermächtigt, einen Menschen, der im Verdacht steht, eine mit gerichtlicher Strafe bedrohte vorsätzliche Handlung begangen zu haben, erkennungsdienstlich zu behandeln, wenn er im Rahmen einer kriminellen Verbindung tätig wurde oder dies wegen der Art oder Ausführung der Tat oder der Persönlichkeit des Betroffenen zur Vorbeugung gefährlicher Angriffe erforderlich scheint. Gemäß Paragraph 65, Absatz eins, SPG sind die Sicherheitsbehörden ermächtigt, einen Menschen, der im Verdacht steht, eine mit gerichtlicher Strafe bedrohte vorsätzliche Handlung begangen zu haben, erkennungsdienstlich zu behandeln, wenn er im Rahmen einer kriminellen Verbindung tätig wurde oder dies wegen der Art oder Ausführung der Tat oder der Persönlichkeit des Betroffenen zur Vorbeugung gefährlicher Angriffe erforderlich scheint.

Gemäß § 75 Abs. 1 SPG sind die Sicherheitsbehörden als gemeinsam Verantwortliche ermächtigt, die von ihnen gemäß den §§ 65 Abs. 1, 65a, 66 Abs. 1, 67 Abs. 1 erster Satz und Abs. 1a sowie § 68 ermittelten erkennungsdienstlichen Daten, die allenfalls vorhandenen erkennungsdienstlichen Identitätsdaten (§ 65 Abs. 6) und den für die Ermittlung maßgeblichen Grund im Rahmen einer Zentralen erkennungsdienstlichen Evidenz gemeinsam zu verarbeiten. Personenbezogene Daten, die Sicherheitsbehörden nach anderen Bestimmungen rechtmäßig ermittelt haben, dürfen sie in der EDE weiterverarbeiten, wenn diese Verarbeitung für sicherheitspolizeiliche Zwecke in diesem Zeitpunkt zulässig wäre. Gemäß Paragraph 75, Absatz eins, SPG sind die Sicherheitsbehörden als gemeinsam Verantwortliche ermächtigt, die von ihnen gemäß den Paragraphen 65, Absatz eins, 65 a, 66, Absatz eins, 67, Absatz eins, erster Satz und Absatz eins a, sowie Paragraph 68, ermittelten erkennungsdienstlichen Daten, die allenfalls vorhandenen erkennungsdienstlichen Identitätsdaten (Paragraph 65, Absatz 6,) und den für die Ermittlung maßgeblichen Grund im Rahmen einer Zentralen erkennungsdienstlichen Evidenz gemeinsam zu verarbeiten. Personenbezogene Daten, die Sicherheitsbehörden nach anderen Bestimmungen rechtmäßig ermittelt haben, dürfen sie in der EDE weiterverarbeiten, wenn diese Verarbeitung für sicherheitspolizeiliche Zwecke in diesem Zeitpunkt zulässig wäre.

Laut § 75 Abs. 1a SPG sind die Sicherheitsbehörden ermächtigt, eine nach den Bestimmungen der StPO ermittelte Spur, die einer Person, die im Verdacht steht, eine mit gerichtlicher Strafe bedrohte vorsätzliche Handlung begangen zu haben, zugehört oder zugehören dürfte, und deren Ermittlung durch erkennungsdienstliche Maßnahmen erfolgen könnte (§ 64 Abs. 2), zum Zweck ihrer Zuordnung zu einer Person in der Zentralen erkennungsdienstlichen Evidenz zu verarbeiten. Zur Spur dürfen auch Verwaltungsdaten verarbeitet werden. Laut Paragraph 75, Absatz eins a, SPG sind die Sicherheitsbehörden ermächtigt, eine nach den Bestimmungen der StPO ermittelte Spur, die einer Person, die im Verdacht steht, eine mit gerichtlicher Strafe bedrohte vorsätzliche Handlung begangen zu haben, zugehört oder zugehören dürfte, und deren Ermittlung durch erkennungsdienstliche Maßnahmen erfolgen könnte (Paragraph 64, Absatz 2,), zum Zweck ihrer Zuordnung zu einer Person in der Zentralen erkennungsdienstlichen Evidenz zu verarbeiten. Zur Spur dürfen auch Verwaltungsdaten verarbeitet werden.

Gemäß § 75 Abs. 2 SPG sind die Sicherheitsbehörden ermächtigt, die von ihnen in der Zentralen erkennungsdienstlichen Evidenz gespeicherten Daten zu verarbeiten. Abfragen und Übermittlungen der gemäß Abs. 1 und 1a verarbeiteten Daten sind an Behörden für Zwecke der Sicherheitspolizei, der Strafrechtspflege und in anderen Aufgabenbereichen der Sicherheitsverwaltung, soweit dies für Zwecke der Wiedererkennung erforderlich ist, zulässig. Im Übrigen sind Übermittlungen zulässig, wenn hierfür eine ausdrückliche gesetzliche Ermächtigung besteht. Gemäß Paragraph 75, Absatz 2, SPG sind die Sicherheitsbehörden ermächtigt, die von ihnen in der Zentralen erkennungsdienstlichen Evidenz gespeicherten Daten zu verarbeiten. Abfragen und Übermittlungen der gemäß Absatz eins, und 1a verarbeiteten Daten sind an Behörden für Zwecke der Sicherheitspolizei, der Strafrechtspflege und in anderen Aufgabenbereichen der Sicherheitsverwaltung, soweit dies für Zwecke der Wiedererkennung erforderlich ist, zulässig. Im Übrigen sind Übermittlungen zulässig, wenn hierfür eine ausdrückliche gesetzliche Ermächtigung besteht.

§ 75 Abs. 2 SPG stellt aus nachfolgenden Gründen keine taugliche Rechtsgrundlage für die verfahrensgegenständlich monierte Datenverarbeitung dar: Paragraph 75, Absatz 2, SPG stellt aus nachfolgenden Gründen keine taugliche Rechtsgrundlage für die verfahrensgegenständlich monierte Datenverarbeitung dar:

Eingangs ist festzuhalten, dass es zur Zulässigkeit des verfahrensgegenständlichen Lichtbildabgleichs nicht nur einer „einfachen“ gesetzlichen Grundlage iSv. § 38 DSGVO bedarf, sondern eine solche Gesetzesgrundlage - aufgrund der besonderen Sensibilität von biometrischen Daten - überdies die Voraussetzungen des § 39 DSGVO - dabei insbesondere das Vorhandensein wirksamer Maßnahmen zum Schutz der Rechte und Freiheiten betroffener Personen - erfüllen muss. Eingangs ist festzuhalten, dass es zur Zulässigkeit des verfahrensgegenständlichen Lichtbildabgleichs nicht nur einer „einfachen“ gesetzlichen Grundlage iSv. Paragraph 38, DSGVO bedarf, sondern eine solche Gesetzesgrundlage - aufgrund der besonderen Sensibilität von biometrischen Daten - überdies die Voraussetzungen des Paragraph 39, DSGVO - dabei insbesondere das Vorhandensein wirksamer Maßnahmen zum Schutz der Rechte und Freiheiten betroffener Personen - erfüllen muss.

Dies wurde von der bGP nicht weiter in Zweifel gezogen, sondern führte diese vielmehr aus, dass „entsprechende materielle Maßnahmen bereits die materiengesetzliche Bestimmung gem. § 75 SPG [vorsieht], in der die Verarbeitung an Voraussetzungen und Zwecke gebunden ist. Verfahrensrechtliche bzw. organisatorische Maßnahmen [Anmerkung der DSB: iSv. § 39 DSGVO] [werden] durch den Verantwortlichen [offenbar gemeint: die bGP] getroffen“. Dies wurde von der bGP nicht weiter in Zweifel gezogen, sondern führte diese vielmehr aus, dass „entsprechende materielle Maßnahmen bereits die materiengesetzliche Bestimmung gem. Paragraph 75, SPG [vorsieht], in der die Verarbeitung an Voraussetzungen und Zwecke gebunden ist. Verfahrensrechtliche bzw. organisatorische Maßnahmen [Anmerkung der DSB: iSv. Paragraph 39, DSGVO] [werden] durch den Verantwortlichen [offenbar gemeint: die bGP] getroffen“.

Weitere Konkretisierungen, insbesondere zu den verfahrensrechtlichen und organisatorischen Maßnahmen, waren der Stellungnahmen der bGP nicht zu entnehmen.

In diesem Zusammenhang ist darauf hinzuweisen, dass mit § 39 DSGVO Art. 10 der DSRL-PJ umgesetzt wird. Art. 10 der DSRL-PJ hält mitunter zur Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person fest, dass diese nur dann erlaubt ist, wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und wenn sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist, der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dient oder wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat. In diesem Zusammenhang ist darauf hinzuweisen, dass mit Paragraph 39, DSGVO Artikel 10, der DSRL-PJ umgesetzt wird. Artikel 10, der DSRL-PJ hält mitunter zur Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person fest, dass diese nur dann erlaubt ist, wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und wenn sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist, der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dient oder wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.

Die Artikel-29-Datenschutzgruppe führt zu Art. 10 der DSRL-PJ aus, dass die Verarbeitung besonderer Kategorien personenbezogener Daten, sofern sie nicht bereits durch das Unionsrecht vorgesehen ist, stets eine spezifische Rechtsgrundlage im nationalen Recht bedarf. Diese spezifische Rechtsgrundlage muss die zusätzlichen Anforderungen des Art. 10 erfüllen. Im Vergleich zu Art. 8 der DSRL-PJ muss die Verarbeitung unbedingt erforderlich sein, und es

müssen angemessene Garantien vorgesehen werden (vgl. Artikel-29-Datenschutzgruppe, Opinion on some key issues of the Law Enforcement Directive [EU 2016/680], WP 258 29.11.2017, S. 7). Die Artikel-29-Datenschutzgruppe führt zu Artikel 10, der DSRL-PJ aus, dass die Verarbeitung besonderer Kategorien personenbezogener Daten, sofern sie nicht bereits durch das Unionsrecht vorgesehen ist, stets eine spezifische Rechtsgrundlage im nationalen Recht bedarf. Diese spezifische Rechtsgrundlage muss die zusätzlichen Anforderungen des Artikel 10, erfüllen. Im Vergleich zu Artikel 8, der DSRL-PJ muss die Verarbeitung unbedingt erforderlich sein, und es müssen angemessene Garantien vorgesehen werden (vgl. Artikel-29-Datenschutzgruppe, Opinion on some key issues of the Law Enforcement Directive [EU 2016/680], WP 258 29.11.2017, S. 7).

In den ErlAB zu § 39 i d F des Datenschutz-Anpassungsgesetzes 2018 (1761 BlgNR 25. GP 20) wird u.a. wie folgt festgehalten (Hervorhebungen durch die Datenschutzbehörde): In den ErlAB zu Paragraph 39, in der Fassung des Datenschutz-Anpassungsgesetzes 2018 (1761 BlgNR 25. Gesetzgebungsperiode 20,) wird u.a. wie folgt festgehalten (Hervorhebungen durch die Datenschutzbehörde):

„[...] überdies muss die Verarbeitung unbedingt erforderlich sein und es müssen wirksame Maßnahmen auf gesetzlicher Ebene zum Schutz der Rechte und Freiheiten der betroffenen Personen getroffen werden [...]“

In ErwG 37 der DSRL-PJ wird zu sensiblen Daten festgehalten, dass solche Daten nur dann verarbeitet werden sollen, wenn die Verarbeitung vorbehaltlich geeigneter Garantien für die durch Rechtsvorschriften festgelegten Rechte und Freiheiten der betroffenen Person erfolgt und in durch Rechtsvorschriften geregelten Fällen erlaubt ist [...]. Unter „geeigneten Garantien“ im Sinne des Art. 10 DSRL-PJ können beispielsweise Regelungen verstanden werden, dass diese Daten nur in Verbindung mit anderen Daten über die betroffene natürliche Person erhoben werden dürfen, die erhobenen Daten hinreichend gesichert werden müssen, der Zugang der Mitarbeiter der zuständigen Behörde zu den Daten strenger geregelt und die Übermittlung dieser Daten verboten wird. In ErwG 37 der DSRL-PJ wird zu sensiblen Daten festgehalten, dass solche Daten nur dann verarbeitet werden sollen, wenn die Verarbeitung vorbehaltlich geeigneter Garantien für die durch Rechtsvorschriften festgelegten Rechte und Freiheiten der betroffenen Person erfolgt und in durch Rechtsvorschriften geregelten Fällen erlaubt ist [...]. Unter „geeigneten Garantien“ im Sinne des Artikel 10, DSRL-PJ können beispielsweise Regelungen verstanden werden, dass diese Daten nur in Verbindung mit anderen Daten über die betroffene natürliche Person erhoben werden dürfen, die erhobenen Daten hinreichend gesichert werden müssen, der Zugang der Mitarbeiter der zuständigen Behörde zu den Daten strenger geregelt und die Übermittlung dieser Daten verboten wird.

Die Artikel-29-Datenschutzgruppe hält in diesem Zusammenhang fest, dass bei der Verarbeitung von Daten i S d. Art. 10 DSRL-PJ das Recht auf Achtung der Privatsphäre und das öffentliche Interesse sorgfältig gegeneinander abgewogen werden müssen. Dabei wird nahegelegt, dass die zuständigen Behörden dazu verpflichtet werden sollen, eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen und dabei beurteilt bzw. nachgewiesen werden muss, ob der Zweck der Verarbeitung (z. B. strafrechtliche Ermittlung) nicht durch eine Verarbeitung erreicht werden kann, bei der die Rechte und Freiheiten der betroffenen Person weniger stark beeinträchtigt werden, und ob die Verarbeitung besonderer Kategorien von Daten nicht eine Diskriminierungsgefahr für die betroffene Person darstellt. Zu den geeigneten Garantien (im Original: „Appropriate safeguards“) führt die Artikel-29-Datenschutzgruppe aus, dass dies etwa zusätzliche (gesetzliche) Einschränkungen des Zwecks der Verarbeitung (z. B. auf bestimmte Kategorien von Straftaten) oder im Falle von Vorkehrungsmaßnahmen eine bestimmte Dringlichkeit sein könnten. Zusätzliche Verfahrensgarantien könnten die vorherige Genehmigung eines Gerichts oder einer anderen unabhängigen Einrichtung und das Verbot der Weitergabe dieser Daten sein. Rechtliche Garantien sollten laut Artikel-29-Datenschutzgruppe in der Regel durch technische und organisatorische Maßnahmen wie zusätzliche Datensicherheitsmaßnahmen flankiert/umgesetzt werden, um die Vertraulichkeit und Integrität der Daten sowie strengere Vorschriften für den Zugang des Personals der zuständigen Behörde zu den Daten zu gewährleisten (vgl. Artikel-29-Datenschutzgruppe, Opinion on some key issues of the Law Enforcement Directive [EU 2016/680], WP 258 29.11.2017, S.8-9). Die Artikel-29-Datenschutzgruppe hält in diesem Zusammenhang fest, dass bei der Verarbeitung von Daten i S d. Artikel 10, DSRL-PJ das Recht auf Achtung der Privatsphäre und das öffentliche Interesse sorgfältig gegeneinander abgewogen werden müssen. Dabei wird nahegelegt, dass die zuständigen Behörden dazu verpflichtet werden sollen, eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen und dabei beurteilt bzw. nachgewiesen werden muss, ob der Zweck der Verarbeitung (z. B. strafrechtliche Ermittlung) nicht durch eine Verarbeitung erreicht werden kann, bei der die Rechte und Freiheiten der betroffenen Person weniger stark beeinträchtigt werden, und ob

die Verarbeitung besonderer Kategorien von Daten nicht eine Diskriminierungsgefahr für die betroffene Person darstellt. Zu den geeigneten Garantien (im Original: „Appropriate safeguards“) führt die Artikel-29-Datenschutzgruppe aus, dass dies etwa zusätzliche (gesetzliche) Einschränkungen des Zwecks der Verarbeitung (z. B. auf bestimmte Kategorien von Straftaten) oder im Falle von Verhütungsmaßnahmen eine bestimmte Dringlichkeit sein könnten. Zusätzliche Verfahrensgarantien könnten die vorherige Genehmigung eines Gerichts oder einer anderen unabhängigen Einrichtung und das Verbot der Weitergabe dieser Daten sein. Rechtliche Garantien sollten laut Artikel-29-Datenschutzgruppe in der Regel durch technische und organisatorische Maßnahmen wie zusätzliche Datensicherheitsmaßnahmen flankiert/umgesetzt werden, um die Vertraulichkeit und Integrität der Daten sowie strengere Vorschriften für den Zugang des Personals der zuständigen Behörde zu den Daten zu gewährleisten (vergleiche Artikel-29-Datenschutzgruppe, Opinion on some key issues of the Law Enforcement Directive [EU 2016/680], WP 258 29.11.2017, S.8-9).

Für den vorliegenden Fall bedeutet dies zunächst, dass geeignete Maßnahmen iSv. § 39 DSG in erster Linie auf gesetzlicher Ebene vorgesehen sein müssen. Bloß durch den Verantwortlichen bzw. die bgP tatsächlich gesetzte technische und organisatorische Maßnahmen vermögen diese Anforderungen demgegenüber nicht zu erfüllen. Für den vorliegenden Fall bedeutet dies zunächst, dass geeignete Maßnahmen iSv. Paragraph 39, DSG in erster Linie auf gesetzlicher Ebene vorgesehen sein müssen. Bloß durch den Verantwortlichen bzw. die bgP tatsächlich gesetzte technische und organisatorische Maßnahmen vermögen diese Anforderungen demgegenüber nicht zu erfüllen.

Soweit die bgP daher vorbringt, dass verfahrensrechtliche bzw. organisatorische Maßnahmen „durch den Verantwortlichen“ getroffen worden seien, ist daher darauf hinzuweisen, dass derartige - von der bgP nicht näher konkretisierte - Maßnahmen bereits deshalb nicht geeignet erscheinen, da es sich dabei um keine gesetzlichen Maßnahmen handelt.

§ 75 Abs. 2 SPG selbst sind derartige spezifischen Garantien iSv. § 39 DSG nicht zu entnehmen. Die Bestimmung stellt vielmehr lediglich eine allgemeine Ermächtigung zur Verarbeitung der in der EDE gespeicherten Daten dar und enthält insbesondere keinerlei nähere Regelungen hinsichtlich besonderer Schutzmaßnahmen oder spezifischer Garantien, wie etwa besondere Zugriffsbeschränkungen, spezifische Verfahrensgarantien, besondere Voraussetzungen für den automationsunterstützten Lichtbildabgleich oder gesetzliche Einschränkungen der Verarbeitung biometrischer Daten. Paragraph 75, Absatz 2, SPG selbst sind derartige spezifischen Garantien iSv. Paragraph 39, DSG nicht zu entnehmen. Die Bestimmung stellt vielmehr lediglich eine allgemeine Ermächtigung zur Verarbeitung der in der EDE gespeicherten Daten dar und enthält insbesondere keinerlei nähere Regelungen hinsichtlich besonderer Schutzmaßnahmen oder spezifischer Garantien, wie etwa besondere Zugriffsbeschränkungen, spezifische Verfahrensgarantien, besondere Voraussetzungen für den automationsunterstützten Lichtbildabgleich oder gesetzliche Einschränkungen der Verarbeitung biometrischer Daten.

Soweit die bgP vorbringt, entsprechende materielle Maßnahmen seien bereits in § 75 SPG (offenbar gemeint: allgemein) vorgesehen, ist zunächst darauf hinzuweisen, dass § 75 Abs. 2 erster Satz SPG, auf welchen die bgP ihre Argumentation maßgeblich stützt, seinem Wortlaut nach gerade keinen wie in § 75 Abs. 1 SPG normierte Voraussetzungen oder einen Verweis auf ebendiese enthält. Die dort vorgesehene Beschränkung auf gemäß §§ 65 ff SPG erhobene erkennungsdienstliche Daten gilt daher nicht automatisch auch für sämtliche Verarbeitungsvorgänge iSv. § 75 Abs. 2 erster Satz SPG. Soweit die bgP vorbringt, entsprechende materielle Maßnahmen seien bereits in Paragraph 75, SPG (offenbar gemeint: allgemein) vorgesehen, ist zunächst darauf hinzuweisen, dass Paragraph 75, Absatz 2, erster Satz SPG, auf welchen die bgP ihre Argumentation maßgeblich stützt, seinem Wortlaut nach gerade keinen wie in Paragraph 75, Absatz eins, SPG normierte Voraussetzungen oder einen Verweis auf ebendiese enthält. Die dort vorgesehene Beschränkung auf gemäß Paragraphen 65, ff SPG erhobene erkennungsdienstliche Daten gilt daher nicht automatisch auch für sämtliche Verarbeitungsvorgänge iSv. Paragraph 75, Absatz 2, erster Satz SPG.

Davon abgesehen, stellt auch § 75 Abs. 1 SPG (isoliert betrachtet) keine taugliche Rechtsgrundlage für den gegenständlichen automationsunterstützten Lichtbildabgleich dar. Die Bestimmung regelt ihrem Inhalt nach primär die gemeinsame Verarbeitung (und Verantwortlichkeit) bzw. Führung der EDE und damit die Speicherung erkennungsdienstlicher Daten als solche, nicht jedoch die konkrete Verarbeitung biometrischer Daten im Wege eines automationsunterstützten Lichtbildabgleiches. Zudem würde auch diese Bestimmung keine spezifischen Garantien iSv. § 39 DSG für die Verarbeitung biometrischer Daten enthalten. Sie beschränkt sich - wie ausgeführt - vielmehr darauf festzulegen, welche Datenkategorien in der EDE verarbeitet werden dürfen, ohne besondere Schutzmaßnahmen oder

sonstige gesetzliche Sicherungen für den automationsunterstützten Lichtbildabgleich vorzusehen. Davon abgesehen, stellt auch Paragraph 75, Absatz eins, SPG (isoliert betrachtet) keine taugliche Rechtsgrundlage für den gegenständlichen automationsunterstützten Lichtbildabgleich dar. Die Bestimmung regelt ihrem Inhalt nach primär die gemeinsame Verarbeitung (und Verantwortlichkeit) bzw. Führung der EDE und damit die Speicherung erkennungsdienstlicher Daten als solche, nicht jedoch die konkrete Verarbeitung biometrischer Daten im Wege eines automationsunterstützten Lichtbildabgleiches. Zudem würde auch diese Bestimmung keine spezifischen Garantien iSv. Paragraph 39, DSGVO für die Verarbeitung biometrischer Daten enthalten. Sie beschränkt sich - wie ausgeführt - vielmehr darauf festzulegen, welche Datenkategorien in der EDE verarbeitet werden dürfen, ohne besondere Schutzmaßnahmen oder sonstige gesetzliche Sicherungen für den automationsunterstützten Lichtbildabgleich vorzusehen.

Der Vollständigkeit halber ist noch festzuhalten, dass auch § 75 Abs. 1a SPG keine taugliche Rechtsgrundlage für den gegenständlichen automationsunterstützten Lichtbildabgleich darstellt. Abgesehen davon, dass es sich bei den gegenständlich verarbeiteten Lichtbildern bereits dem Wortlaut nach nicht um eine nach den Bestimmungen der StPO ermittelte Spur handelt, enthält auch diese Bestimmung keinerlei spezifische Garantie im Sinne des § 39 DSGVO. Der Vollständigkeit halber ist noch festzuhalten, dass auch Paragraph 75, Absatz eins a, SPG keine taugliche Rechtsgrundlage für den gegenständlichen automationsunterstützten Lichtbildabgleich darstellt. Abgesehen davon, dass es sich bei den gegenständlich verarbeiteten Lichtbildern bereits dem Wortlaut nach nicht um eine nach den Bestimmungen der StPO ermittelte Spur handelt, enthält auch diese Bestimmung keinerlei spezifische Garantie im Sinne des Paragraph 39, DSGVO.

Auch den sonstigen Bestimmungen des SPG sind keine spezifischen gesetzlichen Garantien oder besondere Schutzmaßnahmen iSv. § 39 DSGVO für die Durchführung eines automationsunterstützten Lichtbildabgleiches zu entnehmen. Auch den sonstigen Bestimmungen des SPG sind keine spezifischen gesetzlichen Garantien oder besondere Schutzmaßnahmen iSv. Paragraph 39, DSGVO für die Durchführung eines automationsunterstützten Lichtbildabgleiches zu entnehmen.

Soweit die bgP ins Treffen führt, dass der erste Satz von § 75 Abs. 2 SPG ursprünglich anstelle des Wortes „verarbeiten“ die Wortfolge „benützen und vergleichen“ enthalten habe und den Erläuterungen (vgl. ErlRV 763 BlgNR XXV. GP, 15) zufolge hiervon auch ein automationsunterstützter Lichtbildabgleich umfasst sein solle, ist zunächst darauf hinzuweisen, dass Erläuterungen selbst keine gesetzliche Grundlage darstellen können und insbesondere die nach § 39 DSGVO erforderlichen wirksamen Maßnahmen auf gesetzlicher Ebene nicht zu ersetzen vermögen. Soweit die bgP ins Treffen führt, dass der erste Satz von Paragraph 75, Absatz 2, SPG ursprünglich anstelle des Wortes „verarbeiten“ die Wortfolge „benützen und vergleichen“ enthalten habe und den Erläuterungen vergleiche ErlRV 763 BlgNR römisch 25 . GP, 15) zufolge hiervon auch ein automationsunterstützter Lichtbildabgleich umfasst sein solle, ist zunächst darauf hinzuweisen, dass Erläuterungen selbst keine gesetzliche Grundlage darstellen können und insbesondere die nach Paragraph 39, DSGVO erforderlichen wirksamen Maßnahmen auf gesetzlicher Ebene nicht zu ersetzen vermögen.

Hinzu kommt, dass der Gesetzgeber die ursprünglich vorgesehene Wortfolge „benützen und vergleichen“ letztlich gerade nicht in den aktuellen Gesetzestext übernommen, sondern dies durch den allgemeineren Begriff „verarbeiten“ ersetzt hat. Wäre beabsichtigt gewesen, den automationsunterstützten Lichtbildabgleich ausdrücklich gesetzlich zu regeln, wäre vielmehr zu erwarten gewesen, dass der Begriff des „Vergleiches“ im Gesetzestext beibehalten oder noch näher konkretisiert worden wäre. Aus den Erläuterungen kann daher keinesfalls eindeutig abgeleitet werden, dass der Gesetzgeber eine derart eingriffsintensive Verarbeitung biometrischer Daten ohne ausdrückliche gesetzliche Regelungen und ohne spezifische gesetzliche Garantien zulassen wollte.

Soweit die bgP vorbringt, dass dem automationsunterstützten Lichtbildabgleich im vorliegenden Fall eine besonders hohe Relevanz zugekommen sei und die Identifizierung mit gelinderen Mitteln nicht erreicht werden hätte können, kann diesen Ausführungen grundsätzlich zugestimmt werden. Allerdings stellt die unbedingte Erforderlichkeit lediglich eine (von mehreren) Voraussetzungen des § 39 DSGVO dar und vermag für sich genommen das Fehlen spezifischer gesetzlicher Garantien nicht zu ersetzen. Soweit die bgP vorbringt, dass dem automationsunterstützten Lichtbildabgleich im vorliegenden Fall eine besonders hohe Relevanz zugekommen sei und die Identifizierung mit gelinderen Mitteln nicht erreicht werden hätte können, kann diesen Ausführungen grundsätzlich zugestimmt werden. Allerdings stellt die unbedingte Erforderlichkeit lediglich eine (von mehreren) Voraussetzungen des Paragraph 39, DSGVO dar und vermag für sich genommen das Fehlen spezifischer gesetzlicher Garantien nicht zu ersetzen.

Zusammenfassend ist festzuhalten, dass der gegenständliche automationsunterstützte Lichtbildabgleich mittels Gesichtserkennungssoftware einen (besonders eingriffsintensiven) Verarbeitungsvorgang im Zusammenhang mit biometrischen Daten darstellt, dessen Zulässigkeit nach dem klaren Wortlaut des § 39 DSG (Art. 10 DSRL-PJ) einer (hinreichend konkreten) gesetzlichen Grundlage sowie besonderen, gesetzlich vorgesehenen Schutzmaßnahmen bedarf, welche im vorliegenden Fall jedoch nicht vorlagen. Zusammenfassend ist festzuhalten, dass der gegenständliche automationsunterstützte Lichtbildabgleich mittels Gesichtserkennungssoftware einen (besonders eingriffsintensiven) Verarbeitungsvorgang im Zusammenhang mit biometrischen Daten darstellt, dessen Zulässigkeit nach dem klaren Wortlaut des Paragraph 39, DSG (Artikel 10, DSRL-PJ) einer (hinreichend konkreten) gesetzlichen Grundlage sowie besonderen, gesetzlich vorgesehenen Schutzmaßnahmen bedarf, welche im vorliegenden Fall jedoch nicht vorlagen.

Vor diesem Hintergrund erfolgt der am 5. April 2023 durchgeführte Lichtbildabgleich mittels Gesichtserkennungssoftware ohne gesetzliche Grundlage und war der Beschwerde wegen behaupteter Verletzung im Recht auf Geheimhaltung gemäß § 24 Abs. 5 DSG stattzugeben. Vor diesem Hintergrund erfolgt der am 5. April 2023 durchgeführte Lichtbildabgleich mittels Gesichtserkennungssoftware ohne gesetzliche Grundlage und war der Beschwerde wegen behaupteter Verletzung im Recht auf Geheimhaltung gemäß Paragraph 24, Absatz 5, DSG stattzugeben.

Es war daher spruchgemäß zu entscheiden.

Schlagworte

Geheimhaltung, Rechtmäßigkeit der Verarbeitung, erkennungsdienstliche Daten, Zentrale Erkennungsdienstliche Evidenz, EDE, Sicherheitspolizei, Kriminalpolizei, Beschuldigter, Gesichtsbild, biometrische Daten, automationsunterstützter Lichtbildabgleich, Gesichtserkennungssoftware, eindeutige Identifizierung einer natürlichen Person

European Case Law Identifier (ECLI)

ECLI:AT:DSB:2026:2026.0.396.500

Zuletzt aktualisiert am

27.07.2026

Quelle: Datenschutzbehörde Dsb, <https://www.dsb.gv.at>

© 2026 JUSLINE

JUSLINE® ist eine Marke der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH.

www.jusline.at