

TE Bvwg Erkenntnis 2020/5/8 W101 2134867-1

JUSLINE Entscheidung

© Veröffentlicht am 08.05.2020

Entscheidungsdatum

08.05.2020

Norm

B-VG Art133 Abs4

DSG §1 Abs1

DSG §24

SPG §16

SPG §53

SPG §65

SPG §67

SPG §73

SPG §74

VwGVG §28 Abs2

Spruch

W101 2134867-1/16E

IM NAMEN DER REPUBLIK!

Das Bundesverwaltungsgericht hat durch die Richterin Dr. Christine AMANN als Vorsitzende, die fachkundige Laienrichterin Mag. Daniela ZIMMER als Beisitzerin und den fachkundigen Laienrichter Mag. René BOGENDORFER als Beisitzer über die Beschwerde XXXX gegen den Spruchteil 1. des Bescheides der Datenschutzbehörde vom 15.07.2016, Zl. DSB-D122.514/0009-DSB/2016, zu Recht erkannt:

A)

Die Beschwerde wird gemäß § 28 Abs. 2 VwGVG iVm § 24 Abs. 1 und Abs. 5 DSG idgF als unbegründet abgewiesen.

B)

Die Revision ist gemäß Art. 133 Abs. 4 B-VG nicht zulässig.

Text

ENTSCHEIDUNGSGRÜNDE:

I. Verfahrensgang:

Die mitbeteiligte Partei XXXX (= Beschwerdeführer vor der Datenschutzbehörde) erhob am 29.03.2016 eine

mangelhafte Datenschutzbeschwerde, die er nachträglich verbesserte, gegen die Beschwerdeführerin (= Beschwerdegegnerin vor der Datenschutzbehörde) wegen Verletzung im Recht auf Löschung, weil diese entgegen seinem Lösungsbegehren vom 08.04.2015 seine personenbezogenen Daten in der Erkennungsdienstlichen Evidenz (im Folgenden kurz EDE genannt) und in dem Kriminalpolizeilichen Aktenindex (im Folgenden kurz KPA genannt) nicht gelöscht habe.

Die Beschwerdeführerin gab während des Verwaltungsverfahrens auf Aufforderung der Datenschutzbehörde mehrere schriftliche Stellungnahmen ab.

Mit Bescheid vom 15.07.2016, Zl. DSB-D122.514/0009-DSB/2016, gab die Datenschutzbehörde einerseits in Spruchteil 1. der Datenschutzbeschwerde vom 29.03.2016 statt und stellte fest, dass die Beschwerdeführerin die mitbeteiligte Partei XXXX dadurch in deren Recht auf Löschung verletzt habe, indem sie diese Daten nicht gelöscht habe, soweit es die Daten in der EDE betreffe. Andererseits wies die Datenschutzbehörde in Spruchteil 2. diese Datenschutzbeschwerde zurück, soweit es die Daten im KPA betreffe.

Dies begründete die Datenschutzbehörde hinsichtlich des Spruchteiles 1. des Bescheides im Wesentlichen rechtlich folgendermaßen:

Es stehe unbestritten fest, dass XXXX trotz U-Haft und erfolgter Verurteilung nach § 207a StGB - das Verfahren hinsichtlich der ebenfalls angezeigten Delikte nach "§§ 207, 208 und 212 StGB" sei eingestellt worden - eine Rückkehr zu seiner Familie (Ehefrau und sechs Kinder) gestattet worden sei und dass auch die Jugendwohlfahrt nach einer einjährigen regelmäßigen Überprüfung keinen Anlass gesehen habe, weitere Maßnahmen zu ergreifen. Darüber hinaus sei XXXX seit seiner Verurteilung im Dezember 2012 nicht (einschlägig) rückfällig geworden. Die bedingt verhängte Freiheitsstrafe sei endgültig nachgesehen worden.

Diesen individuellen, Hinweise auf die Persönlichkeitsstruktur und eine allfällige Rückfallgefährdung des XXXX Aufschluss gebenden Tatsachen halte die Beschwerdeführerin eine durch Studien beschiedene abstrakt erhöhte Rückfallquote von Sexualstraftätern, insbesondere jenen mit pädophilen Neigungen, entgegen. Die Seriosität dieser Studien werde von der Datenschutzbehörde nicht in Zweifel gezogen, finde jedoch in der erwähnten Statistik keine Deckung.

Auch könne aus der Tatsache, dass eine Eintragung im Strafregister oder in der Sexualstraftäterdatei für einen Betroffenen eine weitaus schlimmere Folge als eine Eintragung in polizei-internen Datenanwendungen nach sich ziehe, nicht ohne weiteres der Schluss gezogen werden, dass deshalb einem Lösungsbegehren in Bezug auf die EDE nicht stattzugeben sei; die Voraussetzungen für die Eintragung und Speicherung unterliege nämlich bei diesen Datenanwendungen völlig unterschiedlichen gesetzlichen Voraussetzungen.

Die Beschwerdeführerin habe somit nicht darlegen können, weshalb trotz der erfolgten Verurteilung nach § 207a StGB aufgrund der individuell zu beurteilenden Persönlichkeit des XXXX eine weitere Speicherung der erkennungsdienstlichen Daten zur Vorbeugung gefährlicher Angriffe erforderlich sei und somit die Voraussetzungen nach § 65 Abs. 1 SPG nach wie vor erfüllt seien.

Durch die nicht erfolgte Löschung habe die Beschwerdeführerin den XXXX in dessen Recht auf Löschung seiner Daten nach § 1 Abs. 3 Z 2 iVm § 27 Abs. 1 Z 2 DSG aF verletzt.

In der gegen den Spruchteil 1. des Bescheides fristgerecht erhobenen Beschwerde brachte die Beschwerdeführerin im Wesentlichen vor:

Es sei durch die Beschwerdeführerin bereits eine umfassende Einzelfallprüfung durchgeführt worden und unter Berücksichtigung einer Verhältnismäßigkeitsprüfung habe der Lösungsantrag des XXXX abgewiesen werden müssen. Eine Löschung dieser Daten wäre insbesondere zum erforderlichen Schutz künftiger potentieller minderjähriger Opfer des XXXX, wegen der zweifelsfrei gegebenen hohen Rückfallwahrscheinlichkeit, nicht zu verantworten. Diese Rückfallwahrscheinlichkeit ergebe sich in diesem Fall sowohl aus subjektiv (§ 207a StGB - Pornografische Darstellungen von Minderjährigen) als auch aus objektiver Sicht nach "Art oder Ausführung der Tat" aufgrund einer überdurchschnittlich hohen Gefährdungsprognose.

Mit Schreiben der Datenschutzbehörde vom 15.09.2016 war die Beschwerde samt Verwaltungsakt an das Bundesverwaltungsgericht übermittelt worden.

Mit Schreiben vom 05.11.2019 legte die Beschwerdeführerin auf Aufforderung des Bundesverwaltungsgerichtes einen aktuellen Auszug aus der EDE betreffend XXXX vor und gab zusätzlich folgende Stellungnahme ab:

Grundsätzlich werde die Löschung erkennungsdienstlicher Daten von Amts wegen gemäß § 73 Abs. 1 Z 4 SPG nur dann vorgenommen, wenn gegen den Betroffenen kein Verdacht mehr bestehe, die mit gerichtlicher Strafe bedrohte vorsätzliche Handlung begangen zu haben, sofern nicht eine weitere Verarbeitung deshalb für erforderlich gehalten werde, weil aufgrund konkreter Umstände zu befürchten sei, der Betroffene werde gefährliche Angriffe begehen.

Daher werde im Regelfall nur bei einem Freispruch durch das Gericht oder einer Einstellung des Verfahrens durch die Staatsanwaltschaft eine Löschung durchgeführt. Im Falle einer gerichtlichen Verurteilung wegen einer Straftat, bei der auch die sonstigen Voraussetzungen (Eignung zur Vorbeugung) nach § 65 oder § 67 SPG gegeben seien, erfolge daher keine Löschung, auch wenn die Eintragung im Strafregister nach den Bestimmungen des Tilgungsgesetzes gelöscht worden sei.

Trotz der Tilgung der Verurteilung im Strafregister sei nach ho. Ansicht davon auszugehen, dass XXXX das strafgesetzliche Tatbild des § 207a StGB verwirklicht und somit einen gefährlichen Angriff iSd § 16 SPG begangen habe.

Eine Löschung von Amts wegen erfolge daher im Fall einer gerichtlichen Verurteilung in der Regel gemäß § 73 Abs. 1 Z 1 SPG, wenn der Betroffene das 80. Lebensjahr vollendet habe und seit der letzten erkennungsdienstlichen Behandlung fünf Jahre verstrichen seien.

Auf Aufforderung des Bundesverwaltungsgerichtes legte das Landesgericht L. am 03.02.2020 die gekürzte Ausfertigung des Urteils vom 19.12.2012, Zl. 22 Hv 164/12a, im vollen Wortlaut vor.

Am 25.03.2020 war beim Bundesverwaltungsgericht eine mündliche Verhandlung anberaumt. Im Vorfeld dieser Verhandlung hatte die mitbeteiligte Partei XXXX schriftlich vorgebracht und durch die Vorlage eines ärztlichen Attests untermauert, "aus gesundheitlichen Gründen den geplanten Termin am 25.03.2020 beim Bundesverwaltungsgericht in Wien nicht wahrnehmen" zu können. Auch der Vertreter der Beschwerdeführerin hat dem Bundesverwaltungsgericht telefonisch bekanntgegeben, aufgrund der derzeitigen Corona-Krise an der Verhandlung nicht teilnehmen zu können.

In der Folge war die mündliche Verhandlung am 24.03.2020 abberaumt worden.

II. Das Bundesverwaltungsgericht hat erwogen:

1. Feststellungen:

Die Datenschutzbeschwerde wegen Verletzung im Recht auf Löschung begründet XXXX damit, dass die Beschwerdeführerin entgegen seinem Löschungsbegehren vom 08.04.2015 seine Daten in der EDE u.a. nicht gelöscht habe.

Laut aktuellem Auszug aus der EDE sind die persönlichen Daten des XXXX samt drei Fotos (aufgenommen am 18.08.2012) sowie einer DNA-Untersuchung darin gespeichert und zwar aufgrund eines erkennungsdienstlichen Verfahrens zu den Straftaten des a) § "208 Sittliche Gefährdung von Personen von unter 16 Jahren" und des b) § "207a Pornografische Darstellungen von Minderjährigen".

Beschwerdegegenstand ist daher die Prüfung der Frage, ob die personenbezogenen Daten des XXXX, die im Zuge eines Ermittlungsverfahrens zu den Straftaten des § 208 StGB und des § 207a StGB gespeichert wurden, in der EDE zu löschen sind.

ad a):

Mit Benachrichtigung vom 29.11.2012 hat die Staatsanwaltschaft L. mitgeteilt, dass das Ermittlungsverfahren gegen den Beschuldigten XXXX wegen der §§ 207, 208, 299, 302 und 313 StGB sowie des § 27 (1) SMG eingestellt wurde.

Es steht diesbezüglich maßgebend fest, dass die personenbezogenen Daten des XXXX zu der verdächtigten Straftat des § 208 StGB nach der erfolgten Einstellung des Strafverfahrens aus der EDE zu löschen gewesen wären.

ad b):

Mit Urteil des Landesgerichts L. vom 19.12.2012 ist XXXX der Straftaten des § 207a Abs. 1 Z 2, Abs. 3 1. und 2. Fall, Abs. 4 Z 1, 2 und 3 lit. a) und b) StGB für schuldig gesprochen und zu einer bedingt nachgesehenen Freiheitsstrafe von 5 Monaten und einer Geldstrafe iHv Euro 1.200,- verurteilt worden.

Als erschwerend gewertet wurden in diesem Urteil einerseits der lange Tatzeitraum von rund 12 1/2 Jahren und andererseits das Zusammentreffen mehrerer Vergehen.

Als mildernd gewertet wurden in diesem Urteil das umfassende reumütige Geständnis des Täters, seine bisherige Unbescholtenheit und seine Therapiebereitschaft.

Die bedingt ausgesprochene Freiheitsstrafe wurde am 24.03.2016 endgültig nachgesehen.

Die bedingt nachgesehene Freiheitsstrafe und Geldstrafe wurde am 16.01.2018 getilgt, sodass sie im Strafregister der Republik Österreich nicht (mehr) aufscheint. XXXX ist seither unbescholten.

Es steht diesbezüglich maßgebend fest, dass auch die personenbezogenen Daten des XXXX zu der begangenen Straftat des § 207a StGB aus der EDE zu löschen sind, weil mit der Tilgung einer Verurteilung (hier am 16.01.2018) alle nachteiligen Folgen ex lege erlöschen.

2. Beweiswürdigung:

Die Feststellungen zum maßgeblichen Sachverhalt ergeben sich aus dem Verwaltungsakt, der Beschwerde und dem Gerichtsakt.

Den aktuellen Auszug aus der EDE zu der Person des XXXX hat die Beschwerdeführerin selbst mit Schreiben vom 05.11.2019 nach entsprechender Aufforderung des Bundesverwaltungsgerichts in Vorlage gebracht (GZ. W101 2134867-1/3).

Es ist eine aktenkundige, nicht widerlegbare Tatsache, dass die gespeicherten personenbezogenen Daten des XXXX sich einerseits auf die Straftat des § 208 StGB und andererseits auf jene des § 207a StGB beziehen.

Die Benachrichtigung über die Einstellung vom 29.11.2012 liegt im Verwaltungsakt auf, weil diese von XXXX bereits zur verfahrenseinleitenden Datenschutzbeschwerde als Beilage vorgelegt wurde.

Das Urteil vom 19.12.2012 wurde auf Ersuchen des Bundesverwaltungsgerichtes vom Landesgericht L. im vollen Wortlaut im Februar 2020 übermittelt (GZ. W101 2134867-1/8). Die diesbezüglichen Feststellungen sind aus dem Strafurteil übernommen.

Die weiteren Feststellungen zur Nachsicht der bedingt ausgesprochenen Freiheitsstrafe und zur Tilgung der gesamten Strafe ergeben sich aus diversen, im Verwaltungsakt aufliegenden, Strafregisterauszügen.

Ebenso ergibt sich die Feststellung, dass zu XXXX im Strafregister keine Verurteilung derzeit aufscheint und er unbescholten ist, aus dem im Gerichtsakt aufliegenden aktuellen Strafregisterauszug.

Der maßgebliche Sachverhalt hat auf Grund der vorliegenden Aktenlage - auch ohne Durchführung einer mündlichen Verhandlung - zweifelsfrei und vollständig festgestellt werden können.

3. Rechtliche Beurteilung:

3.1. Gemäß § 6 BVwGG entscheidet das Bundesverwaltungsgericht durch Einzelrichter, sofern nicht in Bundes- oder Landesgesetzen die Entscheidung durch Senate vorgesehen ist.

Gemäß § 27 Abs. 1 DSG entscheidet das Bundesverwaltungsgericht durch Senat über Beschwerden gegen Bescheide, wegen Verletzung der Unterrichtungspflicht gemäß § 24 Abs. 7 und der Entscheidungspflicht der Datenschutzbehörde. Gemäß § 27 Abs. 2 erster Satz DSG besteht der Senat aus einem Vorsitzenden und je einem fachkundigen Laienrichter aus dem Kreis der Arbeitgeber und aus dem Kreis der Arbeitnehmer. Gegenständlich liegt somit Senatszuständigkeit vor.

Das Verfahren der Verwaltungsgerichte mit Ausnahme des Bundesfinanzgerichtes ist durch das VwGVG, BGBl. I 2013/33 idF BGBl. I 2013/122, geregelt (§ 1 leg.cit.). Gemäß § 58 Abs. 2 VwGVG bleiben entgegenstehende Bestimmungen, die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bereits kundgemacht wurden, in Kraft.

Gemäß § 17 VwGVG sind, soweit in diesem Bundesgesetz nicht anderes bestimmt ist, auf das Verfahren über Beschwerden gemäß Art. 130 Abs. 1 B-VG die Bestimmungen des AVG mit Ausnahme der §§ 1 bis 5 sowie des IV. Teiles, die Bestimmungen der Bundesabgabenordnung - BAO, BGBl. Nr. 194/1961, des Agrarverfahrensgesetzes - AgrVG, BGBl. Nr. 173/1950, und des Dienstrechtsverfahrensgesetzes 1984 - DVG, BGBl. Nr. 29/1984, und im Übrigen jene

verfahrensrechtlichen Bestimmungen in Bundes- oder Landesgesetzen sinngemäß anzuwenden, die die Behörde in dem Verfahren vor dem Verwaltungsgericht vorangegangenen Verfahren angewendet hat oder anzuwenden gehabt hätte.

3.2. Gemäß § 28 Abs. 1 VwGVG hat das Verwaltungsgericht die Rechtssache durch Erkenntnis zu erledigen, sofern die Beschwerde nicht zurückzuweisen oder das Verfahren einzustellen ist.

Gemäß § 28 Abs. 2 VwGVG hat über Beschwerden gemäß Art. 130 Abs. 1 Z 1 B-VG das Verwaltungsgericht dann in der Sache selbst zu entscheiden, wenn der maßgebliche Sachverhalt feststeht oder die Feststellung des maßgeblichen Sachverhalts durch das Verwaltungsgericht selbst im Interesse der Raschheit gelegen oder mit einer erheblichen Kostenersparnis verbunden ist.

Gemäß § 31 Abs. 1 VwGVG erfolgen die Entscheidungen und Anordnungen durch Beschluss, soweit nicht ein Erkenntnis zu fällen ist.

3.3. Zu A)

3.3.1. § 69 Abs. 4 DSGVO enthält keine Übergangsbestimmungen bezüglich der anhängigen Verfahren in Datenschutzangelegenheiten vor dem Bundesverwaltungsgericht. Damit ist die zum Zeitpunkt der Beschlussfassung des Senates geltende Rechtslage anzuwenden (vgl. VwGH vom 19.02.2018, Ra 2015/07/0074; VwGH vom 22.02.2018, Ra 2017/22/0125; u.v.a.).

Die einschlägigen Bestimmungen im DSGVO lauten:

Grundrecht auf Datenschutz

§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;

2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten

Voraussetzungen zulässig.

Anwendungsbereich und Begriffsbestimmungen

§ 36. (1) Die Bestimmungen dieses Hauptstücks gelten für die Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung.

(2) Im Sinne dieses Hauptstücks bezeichnet der Ausdruck:

1. "personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;
2. "Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
3. "Einschränkung der Verarbeitung" die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;
4. "Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
5. "Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;
6. "Dateisystem" jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;
7. "zuständige Behörde"
 - a) eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, die nationale Sicherheit, den Nachrichtendienst oder die militärische Eigensicherung zuständig ist, oder
 - b) eine andere Stelle oder Einrichtung, der durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zum Zweck der nationalen Sicherheit, des Nachrichtendienstes oder der militärischen Eigensicherung übertragen wurde;
8. "Verantwortlicher" die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;
9. "Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
10. "Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags aufgrund von Gesetzen möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;
11. "Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf

sonstige Weise verarbeitet wurden;

12. "genetische Daten" personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;

13. "biometrische Daten" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

14. "Gesundheitsdaten" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

15. "Aufsichtsbehörde" ist die Datenschutzbehörde;

16. "internationale Organisation" eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Staaten geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

Rechtmäßigkeit der Verarbeitung

§ 38. Die Verarbeitung personenbezogener Daten ist, 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.

Recht auf Berichtigung oder Löschung personenbezogener

Daten und auf Einschränkung der Verarbeitung

§ 45. (1) Jede betroffene Person hat das Recht, vom Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten sowie die Vervollständigung unvollständiger personenbezogener Daten zu verlangen. Die Berichtigung oder Vervollständigung kann erforderlichenfalls mittels einer ergänzenden Erklärung erfolgen, soweit eine nachträgliche Änderung mit dem Dokumentationszweck unvereinbar ist. Der Beweis der Richtigkeit der Daten obliegt dem Verantwortlichen, soweit die personenbezogenen Daten nicht ausschließlich aufgrund von Angaben der betroffenen Person ermittelt wurden.

(2) Der Verantwortliche hat personenbezogene Daten aus eigenem oder über Antrag der betroffenen Person unverzüglich zu löschen, wenn

1. die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind,
2. die personenbezogenen Daten unrechtmäßig verarbeitet wurden oder
3. die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen

Verpflichtung erforderlich ist.

(3) Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

1. die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, oder
2. die personenbezogenen Daten für Beweis Zwecke im Rahmen der Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe weiter aufbewahrt werden müssen.

Im Falle einer Einschränkung gemäß Z 1 hat der Verantwortliche die betroffene Person vor einer Aufhebung der Einschränkung zu unterrichten.

(4) Der Verantwortliche hat die betroffene Person schriftlich über eine Verweigerung der Berichtigung oder Löschung personenbezogener Daten oder eine Einschränkung der Verarbeitung und über die Gründe für die Verweigerung zu unterrichten. Der Verantwortliche hat die betroffene Person über die Möglichkeit zu unterrichten, bei der Datenschutzbehörde Beschwerde einzulegen.

(5) Der Verantwortliche hat die Berichtigung von unrichtigen personenbezogenen Daten der zuständigen Behörde, von der die unrichtigen personenbezogenen Daten stammen, mitzuteilen.

(6) In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung gemäß Abs. 1 bis 3 hat der Verantwortliche alle Empfänger der betroffenen personenbezogenen Daten in Kenntnis zu setzen. Die Empfänger sind verpflichtet, die ihrer Verantwortung unterliegenden personenbezogenen Daten unverzüglich zu berichtigen, löschen oder deren Verarbeitung einschränken.

Die relevanten Bestimmungen des SPG lauten:

Allgemeine Gefahr; gefährlicher Angriff; Gefahrenforschung

§ 16. (1) Eine allgemeine Gefahr besteht

1. bei einem gefährlichen Angriff (Abs. 2 und 3) oder

2. sobald sich drei oder mehr Menschen mit dem Vorsatz verbinden, fortgesetzt gerichtlich strafbare Handlungen zu begehen (kriminelle Verbindung).

(2) Ein gefährlicher Angriff ist die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die vorsätzlich begangen und nicht bloß auf Begehren eines Beteiligten verfolgt wird, sofern es sich um einen Straftatbestand

1. nach dem Strafgesetzbuch (StGB), BGBl. Nr. 60/1974, ausgenommen die Tatbestände nach den §§ 278, 278a und 278b StGB, oder

2. nach dem Verbotsgesetz, StGBI. Nr. 13/1945, oder

3. nach dem Fremdenpolizeigesetz 2005 (FPG), BGBl. I Nr. 100, oder

4. nach dem Suchtmittelgesetz (SMG), BGBl. I Nr. 112/1997, ausgenommen der Erwerb oder Besitz von Suchtmitteln zum ausschließlich persönlichen Gebrauch (§§ 27 Abs. 2, 30 Abs. 2 SMG), oder

5. nach dem Anti-Doping-Bundesgesetz 2007 (ADBG 2007), BGBl. I Nr. 30, oder 6. nach dem Neue-Psychoaktive-Substanzen-Gesetz (NPSG), BGBl. I Nr. 146/2011, handelt.

(3) Ein gefährlicher Angriff ist auch ein Verhalten, das darauf abzielt und geeignet ist, eine solche Bedrohung (Abs. 2) vorzubereiten, sofern dieses Verhalten in engem zeitlichen Zusammenhang mit der angestrebten Tatbestandsverwirklichung gesetzt wird.

(4) Gefahrenforschung ist die Feststellung einer Gefahrenquelle und des für die Abwehr einer Gefahr sonst maßgeblichen Sachverhaltes.

Zulässigkeit der Verarbeitung

§ 53. (1) Die Sicherheitsbehörden dürfen personenbezogene Daten verarbeiten

1. für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht (§ 19);

2. für die Abwehr krimineller Verbindungen (§§ 16 Abs. 1 Z 2 und 21);

(Anm.: Z 2a aufgehoben durch BGBl. I Nr. 5/2016)

3. für die Abwehr gefährlicher Angriffe (§§ 16 Abs. 2 und 3 sowie 21 Abs. 2); einschließlich der im Rahmen der Gefahrenabwehr notwendigen Gefahrenforschung (§ 16 Abs. 4 und § 28a);

4. für die Vorbeugung wahrscheinlicher gefährlicher Angriffe gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen oder Umwelt (§ 22 Abs. 2 und 3) oder für die Vorbeugung gefährlicher Angriffe mittels Kriminalitätsanalyse, wenn nach der Art des Angriffes eine wiederholte Begehung wahrscheinlich ist;

5. für Zwecke der Fahndung (§ 24);

6. um bei einem bestimmten Ereignis die öffentliche Ordnung aufrechterhalten zu können.

(Anm.: Z 7 aufgehoben durch BGBl. I Nr. 5/2016)

[...].

Erkennungsdienstliche Behandlung

§ 65. (1) Die Sicherheitsbehörden sind 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.

(2) Die Sicherheitsbehörden sind ermächtigt, im Zusammenhang mit der Klärung der Umstände einer mit gerichtlicher Strafe bedrohten vorsätzlichen Handlung Menschen erkennungsdienstlich zu behandeln, wenn diese nicht im Verdacht stehen, diese Handlung begangen zu haben, aber Gelegenheit hatten, Spuren zu hinterlassen, soweit dies zur Auswertung vorhandener Spuren notwendig ist.

(3) Die Sicherheitsbehörden sind ermächtigt, Menschen erkennungsdienstlich zu behandeln, deren Identität gemäß § 35 Abs. 1 festgestellt werden muss, sofern eine Anknüpfung an andere Umstände nicht möglich ist oder unverhältnismäßig wäre.

(4) Wer erkennungsdienstlich zu behandeln ist, hat an den dafür erforderlichen Handlungen mitzuwirken.

(Anm.: Abs. 5 aufgehoben durch Art. 1 Z 59, BGBl. I Nr. 29/2018)

(6) Die Sicherheitsbehörden sind ermächtigt, Namen, Geschlecht, frühere Namen, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Namen der Eltern, Ausstellungsbehörde, Ausstellungsdatum und Nummer mitgeführter Dokumente, allfällige Hinweise über die Gefährlichkeit beim Einschreiten einschließlich besonderer Kategorien personenbezogener Daten, soweit deren Verarbeitung zur Wahrung lebenswichtiger Interessen erforderlich ist, und Aliasdaten eines Menschen (erkennungsdienstliche Identitätsdaten), den sie erkennungsdienstlich behandelt haben, zu ermitteln und zusammen mit den erkennungsdienstlichen Daten und mit dem für die Ermittlung maßgeblichen Grund zu verarbeiten. In den Fällen des Abs. 1 sind die Sicherheitsbehörden ermächtigt, eine Personsfeststellung vorzunehmen.

DNA-Untersuchungen

§ 67. (1) Eine erkennungsdienstliche Behandlung, bei der die DNA eines Menschen ermittelt werden soll, ist zulässig, wenn der Betroffene im Verdacht steht, eine strafbare Handlung gegen die sexuelle Integrität und Selbstbestimmung oder eine mit mindestens einjähriger Freiheitsstrafe bedrohte vorsätzliche gerichtlich strafbare Handlung begangen zu haben und wegen der Art oder Ausführung der Tat oder der Persönlichkeit des Betroffenen zu befürchten ist, er werde gefährliche Angriffe begehen und dabei Spuren hinterlassen, die seine Wiedererkennung auf Grund der ermittelten genetischen Daten im Sinne des § 36 Abs. 2 Z 12 DSGVO ermöglichen würden. Soweit dies zur Auswertung vorhandener DNA-Spuren erforderlich ist, darf eine solche erkennungsdienstliche Behandlung auch bei Menschen im Sinne des § 65 Abs. 2 erfolgen. Im Übrigen gilt § 65 Abs. 4 bis 6.

(1a) Eine erkennungsdienstliche Maßnahme in Bezug auf Abgängige (§ 65a) und an Leichen (§ 66) darf auch die Ermittlung der DNA umfassen.

(2) Genetische Daten, die durch erkennungsdienstliche Maßnahmen ermittelt wurden, dürfen ausschließlich für Zwecke des Erkennungsdienstes ausgewertet werden. Die molekulargenetische Untersuchung hat durch einen Auftragsverarbeiter zu erfolgen, dem zwar das gesamte Untersuchungsmaterial auszufolgen, nicht aber erkennungsdienstliche Identitätsdaten des Betroffenen zu übermitteln sind.

(3) Die Sicherheitsbehörden haben vertraglich dafür vorzusorgen, dass der Auftragsverarbeiter nur jene Bereiche in der DNA untersucht, die der Wiedererkennung dienen, sowie dafür, dass er das Untersuchungsmaterial vernichtet, wenn die

Sicherheitsbehörde zur Löschung der erkennungsdienstlichen Daten verpflichtet ist.

Löschen erkennungsdienstlicher Daten von Amts wegen

§ 73. (1) Erkennungsdienstliche Daten, die gemäß § 65 oder § 67 ermittelt wurden, sind von Amts wegen zu löschen,

1. wenn der Betroffene das 80. Lebensjahr vollendet hat und seit der letzten erkennungsdienstlichen Behandlung fünf Jahre verstrichen sind;
2. wenn die Daten von einer gemäß § 65 Abs. 1 vorgenommenen erkennungsdienstlichen Behandlung eines Strafmündigen stammen und seither drei Jahre verstrichen sind, ohne dass es neuerlich zu einer erkennungsdienstlichen Behandlung gekommen wäre;
3. wenn seit dem Tod des Betroffenen fünf Jahre verstrichen sind;
4. wenn gegen den Betroffenen kein Verdacht mehr besteht, die mit gerichtlicher Strafe bedrohte vorsätzliche Handlung begangen zu haben, es sei denn, weiteres Verarbeiten wäre deshalb erforderlich, weil auf Grund konkreter Umstände zu befürchten ist, der Betroffene werde gefährliche Angriffe begehen;
5. im Fall des § 65 Abs. 2, sobald sie ihre Funktion für den Anlassfall erfüllt haben, im Falle einer Verarbeitung der Daten in der Spurenausscheidungsevidenz nach § 70, sobald das Organ der Sicherheitsbehörde die berufliche Tätigkeit nicht mehr regelmäßig ausübt;
6. im Fall des § 65 Abs. 3, sobald sie ihre Funktion für den Anlassfall erfüllt haben.

(2) Der Bundesminister für Inneres kann nach Maßgabe der technischen Möglichkeiten durch Verordnung bestimmen, dass erkennungsdienstliche Daten, deren Aufbewahrung für Zwecke der Vorbeugung entbehrlich wurde, vor Ablauf der im Abs. 1 Z 1 bis 3 festgelegten Zeit von Amts wegen gelöscht werden.

(3) Von einer gemäß Abs. 1 Z 4 erfolgten Löschung ist der Betroffene ohne Zustellnachweis zu verständigen, sofern eine Abgabestelle bekannt ist oder ohne Schwierigkeiten festgestellt werden kann. Inwieweit eine solche Verständigung auch in den Fällen des Abs. 2 zu erfolgen hat, ist in der Verordnung festzulegen.

(4) Erkennungsdienstliche Daten, die gemäß § 65a ermittelt wurden, sind von Amts wegen nach Auffindung des Betroffenen, im Falle der Feststellung des Todes nach fünf Jahren zu löschen.

(5) Erkennungsdienstliche Daten, die gemäß § 66 ermittelt wurden, sind von Amts wegen spätestens nach fünf Jahren oder sobald sie ihre Funktion für den Anlassfall erfüllt haben, zu löschen.

(6) Erkennungsdienstliche Daten, die gemäß § 68 Abs. 1, 3 oder 4 ermittelt wurden, sind von Amts wegen nach dem Tod des Betroffenen zu löschen.

(7) Wenn aus Gründen der Wirtschaftlichkeit die physische Löschung erkennungsdienstlicher Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern nur zu bestimmten Zeitpunkten vorgenommen werden kann, so sind die Daten bis dahin logisch und sodann physisch zu löschen.

Löschen erkennungsdienstlicher Daten auf Antrag des Betroffenen

§ 74. (Anm.: Abs. 1 und 2 aufgehoben durch VfGH, BGBl. I Nr. 55/2013)

(3) Erkennungsdienstliche Daten, die gemäß § 68 Abs. 1, 3 oder 4 ermittelt wurden, sind auf Antrag des Betroffenen zu löschen; Abbildungen können dem Betroffenen ausgefolgt werden.

3.3.2. Unter Berücksichtigung dieser Rechtslage ergibt sich für den vorliegenden Fall Folgendes:

Gegenständlich kommt das 3. Hauptstück des DSG zur "Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei (...), der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs" zur Anwendung.

Die EDE ist als strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, ein "Dateisystem" iSd Begriffsbestimmung des § 36 Abs. 2 Z 6 DSG.

Im Jahr 2012 wurde gegen XXXX wegen der Begehung mehrere Straftaten erkennungsdienstlich ermittelt.

Die personenbezogenen Daten des XXXX als identifizierte betroffene Person sind - wie oben festgestellt - in der EDE zum Zweck der Aufklärung und Verfolgung von Straftaten gespeichert worden und können seitdem von allen Zugangsberechtigten dieses Dateisystems abgerufen werden. D.h. auch die Begriffsbestimmungen des leg.cit. Z 1

("personenbezogene Daten") und der Z 2 ("Verarbeitung") sind hier erfüllt.

Die Beschwerdeführerin macht im Schreiben vom 05.11.2019 dazu geltend, dass grundsätzlich die Löschung erkennungsdienstlicher Daten von Amts wegen gemäß § 73 Abs. 1 Z 4 SPG nur dann vorgenommen werde, wenn gegen den Betroffenen kein Verdacht mehr bestehe, die mit gerichtlicher Strafe bedrohte vorsätzliche Handlung begangen zu haben, sofern nicht eine weitere Verarbeitung deshalb für erforderlich gehalten werde, weil aufgrund konkreter Umstände zu befürchten sei, der Betroffene werde gefährliche Angriffe begehen.

3.3.2.1. Zu § 208 StGB:

Die betroffene Person XXXX war iSd § 37 Abs. 4 Z 1 DSG verdächtig, u.a. die Straftat des § 208 StGB begangen zu haben.

Wie oben bereits festgestellt, wurde aber das Strafverfahren gegen XXXX zu dieser Straftat u.a. im November 2019 von der Staatsanwaltschaft L. eingestellt.

Die Beschwerdeführerin hat im Schreiben vom 05.11.2019 auch mitgeteilt, dass "im Regelfall nur bei einem Freispruch durch das Gericht oder einer Einstellung des Verfahrens durch die Staatsanwaltschaft eine Löschung durchgeführt" werde.

Es hätte folglich sogar der eigenen Mitteilung der Beschwerdeführerin entsprochen, wenn die Speicherung der personenbezogenen Daten zur bloß verdächtigten Straftat des § 208 StGB in der EDE gelöscht worden wären, da ja auch das Strafverfahren zu dieser Straftat (ebenso wie zu den festgestellten anderen Delikten) im November 2012 eingestellt worden ist.

Die Beschwerdeführerin hat sich im genannten Schreiben auch nicht dahingehend geäußert, dass hinsichtlich der zur verdächtigten Straftat des § 208 StGB gespeicherten Daten des XXXX ein Ausnahmefall vorliegen würde.

Kann ein Verdacht nach erfolgter erkennungsdienstlicher Behandlung nicht bestätigt werden, so sind die Daten des Betroffenen zu löschen (Thanner/Vogl (Hrsg), Sicherheitspolizeigesetz, 2. Auflage, Stand: 01.01.2013, S. 706).

Von der Löschung der Daten ist aber trotz der Entkräftung des Verdachts gemäß § 73 Abs. 1 Z 4 SPG abzusehen, wenn konkrete Hinweise künftige gefährliche Angriffe durch den Betroffenen befürchten lassen (Thanner/Vogl (Hrsg), Sicherheitspolizeigesetz, 2. Auflage, Stand: 01.01.2013, S. 706), d.h. eine Rückfallgefahr im konkreten Fall vorliegt.

Eine solche Rückfallgefahr setzt aber voraus, dass der Betroffene zumindest einen Sachverhalt erfüllt hat, der einer strafbaren Handlung entspricht, wenn nicht überhaupt straffällig geworden ist (vgl. VwGH 30.01.2001, Zl. 2000/01/0061). Gerade ein solcher Umstand ergibt sich jedoch aus der Begründung der Einstellung durch die Staatsanwaltschaft nicht, sondern muss in Bindung daran davon ausgegangen werden, dass XXXX die Straftat des § 208 StGB gar nicht begangen hat (siehe auch einen diesbezüglich vergleichbaren Fall, Erkenntnis des BVWG vom 04.06.2019, Zl. W214 2213623-1/15E).

Folglich liegen im Fall des XXXX zur bloß verdächtigten Straftat des § 208 StGB neben der evidenten Entkräftung der Verdachtslage auch die weiteren Tatbestandsvoraussetzungen des § 73 Abs. 1 Z 4 SPG nicht vor. Dementsprechend ist es nicht nachvollziehbar, wieso diese Daten des XXXX in der EDE nicht gelöscht worden sind.

3.3.2.2. Zu § 207a StGB:

Wie oben bereits festgestellt, wurde XXXX gemäß § 207a Abs. 1 Z 2, Abs. 3 1. und 2. Fall, Abs. 4 Z 1, 2 und 3 lit. a) und b) StGB rechtskräftig mit Urteil vom 19.12.2012 verurteilt.

Bezüglich dieser Straftat fällt XXXX daher in die Kategorie der "verurteilten Straftäter" iSd § 37 Abs. 4 Z 3 DSG.

Die Beschwerdeführerin macht im Schreiben vom 05.11.2019 dazu insbesondere geltend, dass "im Fall einer gerichtlichen Verurteilung wegen einer Straftat, bei der auch die sonstigen Voraussetzungen (Eignung zur Vorbeugung) nach § 65 oder § 67 SPG gegeben" seien, daher keine Löschung erfolge, auch wenn die Eintragung im Strafregister nach den Bestimmungen des Tilgungsgesetzes gelöscht worden seien.

Dem kann im Ergebnis - die Löschung betreffend - aus nachstehenden Erwägungen nicht gefolgt werden.

Im Fall des XXXX ist durch die nachfolgende gerichtliche Verurteilung gemäß § 207a StGB eine Bestätigung des vorherigen Verdachts erfolgt (Thanner/Vogl (Hrsg), Sicherheitspolizeigesetz, 2. Auflage, Stand: 01.01.2013, S. 706), sodass hier gemäß § 73 Abs. 1 Z 4 SPG im Rahmen einer einzelfallbezogenen Prognose das Vorliegen einer Rückfallgefahr zu prüfen ist.

Betrachtet man aus spezialpräventiven Gesichtspunkten die konkreten Tatumstände, so fallen - laut Urteil vom 19.12.2012 - die Erschwerungsgründe des sehr langen Tatzeitraumes von 12 1/2 Jahren und des Zusammentreffens mehrerer Vergehen, vielmehr ins Gewicht als die dort auch berücksichtigten Milderungsgründe.

So hebt auch der Verwaltungsgerichtshof im Fall des XXXX hinsichtlich der Verhängung einer Disziplinarstrafe den sehr langen Tatzeitraum sowie auch den Umstand von Bedeutung hervor, dass XXXX pornografische Bilder von Kindern nicht bloß aus dem Internet heruntergeladen habe, sondern auch zugelassen habe, dass von seinem Computer derartige Bilder an Dritte weitergegeben worden seien. Weiters betont der Verwaltungsgerichtshof, dass XXXX auch nicht bestreite, die im Tatvorwurf umschriebenen Handlungen begangen zu haben (VwGH 24.01.2014, Zl. 2013/09/0149, S. 16).

Betrachtet man darüber hinaus noch die Persönlichkeitsstruktur des XXXX so ändert auch die Berücksichtigung des für ihn sprechenden Umstandes, dass er im Jahr 2012 durch einen Sprung in die hochwasserführende Donau ein Menschenleben gerettet hat, nichts an der obigen Gewichtung der Erschwerungsgründe (vgl. VwGH 24.01.2014, Zl. 2013/09/0149, S. 16).

Aus spezialpräventiven Gesichtspunkten ist daher eine Rückfallgefahr im Fall des XXXX eindeutig zu bejahen.

Aber auch aus generalpräventiven Gesichtspunkten ist die nachfolgende Frage zu bejahen, ob sich eine weitere erkennungsdienstliche Behandlung der personenbezogenen Daten des XXXX zu § 207a StGB vorbeugend (auch für andere) auswirken würde.

So hat selbst der Verwaltungsgerichtshof im obigen Erkenntnis im Fall des XXXX die begangene Straftat des § 207a StGB bei einer Prüfung aus spezial- und generalpräventiven Gesichtspunkten als eine derart schwere und langandauernde Dienstpflichtverletzung gewertet, dass die Disziplinarstrafe der Entlassung ausgesprochen wurde (VwGH 24.01.2014, Zl. 2013/09/0149, S. 16).

Daher kann der Argumentation in der Beschwerde, bezogen auf den Zeitpunkt von deren Einbringung, die Löschung der personenbezogenen Daten des XXXX zu § 207a sei gemäß § 73 Abs. 1 Z 4 SPG in der EDE wegen der gegebenen Rückfallgefahr nicht geboten, nur beigetreten werden. Anzumerken bleibt, dass es nicht nachvollziehbar ist, wieso die Datenschutzbehörde sich im angefochtenen Bescheid erkennbar nur mit der begangenen Straftat des § 207a StGB auseinandersetzt und im Zuge einer darauf bezogenen sicherheitspolizeilichen Prüfung eine Rückfallgefahr im Fall des XXXX verneint.

Der erkennende Senat hat aber die maßgebende Frage der Löschung der personenbezogenen Daten in der EDE nach dem jetzigen Entscheidungspunkt zu beurteilen.

Mittlerweile ist - wie oben festgestellt - die Verurteilung vom 19.12.2012 getilgt (und zwar seit 16.01.2018) und wurde die Verurteilung folgerichtig im Strafregister gelöscht. XXXX ist seither eine unbescholtene Person.

Dies entspricht dem § 1 Abs. 4 Tilgungsgesetz. Diese Gesetzesbestimmung normiert nämlich, dass der Verurteilte fortan (als gerichtlich) unbescholten gilt, wenn eine Verurteilung getilgt ist, soweit dem nicht eine andere ungetilgte Verurteilung entgegensteht.

Letztlich ist hier maßgebend, dass § 1 Abs. 2 Tilgungsgesetz ausdrücklich bestimmt, dass mit der Tilgung einer Verurteilung alle nachteiligen Folgen erlöschen, "die kraft Gesetzes mit der Verurteilung verbunden sind".

Aus dem Wortlaut dieser Gesetzesbestimmung (argum "alle nachteiligen Folgen") ergibt sich somit zwingend, dass die während des Ermittlungsverfahrens gespeicherten Daten des Täters XXXX in der EDE mit der Tilgung der Verurteilung (hier gemäß § 207a StGB) grundsätzlich zu löschen sind.

Der Vollständigkeit halber bleibt noch hervorzuheben, dass der Gesetzgeber für Sexualstraftaten, darunter auch jene nach § 207a StGB, im Falle einer unbedingten Freiheitsstrafe gemäß § 4a TilgG die Verdoppelung der Tilgungsfrist vorsehen würde, was aber gegenständlich - wie oben festgestellt - nicht zutrifft.

Gemäß § 37 Abs. 6 DSGVO dürfen grundsätzlich "unrichtige, unvollständige, nicht mehr aktuelle oder zu löschende personenbezogene Daten" weder übermittelt noch zum automatisierten Abruf aus Dateisystemen bereitgestellt werden. Zum automatisierten Abruf bereit gehaltene personenbezogene Daten sind entsprechend laufend vollständig und aktuell zu halten.

Gemäß § 38 DSGVO ist die Verarbeitung personenbezogener Daten u.a. nur rechtmäßig, soweit sie gesetzlich vorgesehen und für die Erfüllung einer Aufgabe erforderlich und verhältnismäßig ist.

Aus obigen Gründen widerspricht die weitere Speicherung der zur Straftat des § 207a StGB gespeicherten Daten des XXXX in der EDE sowohl dem datenschutzrechtlichen Grundsatz der Speicherbegrenzung als auch jenem der Rechtmäßigkeit der Verarbeitung.

3.3.2.3. Gemäß § 45 Abs. 2 Z 1 DSGVO hat der Verantwortliche personenbezogene Daten aus eigenem oder über Antrag der betroffenen Person unverzüglich zu löschen, wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind.

Aus oben dargelegten Gründen ist die weitere Speicherung der personenbezogenen Daten des XXXX - weder in Bezug auf die verdächtige Straftat des § 208 StGB noch hinsichtlich der begangenen Straftat des § 207a StGB - notwendig und wären daher diese Daten von Amts wegen zu löschen gewesen.

Da dem angefochtenen Bescheid aus diesen Gründen im Ergebnis eine Rechtswidrigkeit iSd Art. 130 Abs. 1 Z 1 B-VG nicht anhaftet, war die dagegen erhobene Beschwerde gemäß § 28 Abs. 2 VwGVG iVm § 24 Abs. 1 und Abs. 5 DSGVO idGF abzuweisen.

3.3.3. Gemäß § 24 Abs. 1 VwGVG hat das Verwaltungsgericht auf Antrag oder, wenn es dies für erforderlich hält, von Amts wegen eine öffentliche mündliche Verhandlung durchzuführen.

Der Beschwerdeführerin hat gegenständlich keinen Antrag auf Durchführung einer öffentlichen mündlichen Verhandlung gestellt.

Da im Zuge des Ermittlungsverfahrens beim Bundesverwaltungsgericht hervorgekommen ist, dass der erkennende Senat andere Sachverhaltsfeststellungen als die Datenschutzbehörde treffen wird, ist für den 25.03.2020 eine mündliche Verhandlung anberaumt worden. Diese Verhandlung wurde aber am Tag zuvor noch abberaumt, weil ohnehin weder die Beschwerdeführerin noch die mitbeteiligte Partei XXXX zu der Verhandlung erschienen wären.

In weiterer Folge hat sich herausgestellt, dass die Durchführung einer mündlichen Verhandlung im gegenständlichen Fall gar nicht erforderlich ist, weil der Sachverhalt durch aktenkundige, nicht widerlegbare Tatsachen geklärt und rechtlich im Besonderen auf einen XXXX betreffenden Fall im obigen Erkenntnis des VwGH vom 24.01.2014 gestützt werden hat können.

Von der Durchführung einer mündlichen Verhandlung war demzufolge gemäß § 24 Abs. 1 VwGVG abzusehen.

3.3.4. Es war daher spruchgemäß zu entscheiden.

3.4. Zu B) Unzulässigkeit der Revision:

Gemäß § 25a Abs. 1 VwGG hat das Verwaltungsgericht im Spruch seines Erkenntnisses oder Beschlusses auszusprechen, ob die Revision gemäß Art. 133 Abs. 4 B-VG zulässig ist. Der Ausspruch ist kurz zu begründen.

Die Revision ist gemäß Art. 133 Abs. 4 B-VG nicht zulässig, weil die Entscheidung nicht von der Lösung einer Rechtsfrage abhängt, der grundsätzliche Bedeutung zukommt. Die gegenständliche Entscheidung weicht nicht von der bisherigen Rechtsprechung des Verwaltungsgerichtshofes zum DSGVO 2000 (und zum SPG) ab, vielmehr hat sich der Senat im Wesentlichen auf zwei maßgebende (oben zitierte) Erkenntnisse des Verwaltungsgerichtshofes gestützt. Dem Fehlen einer Rechtsprechung des Verwaltungsgerichtshofes zur neuen seit 25.05.2018 geltenden Rechtslage nach dem DSGVO kommt gegenständlich keine Bedeutung zu.

Auch liegen keine sonstigen Hinweise auf eine grundsätzliche Bedeutung der zu lösenden Rechtsfrage vor.

Schlagworte

Dateisystem Datenschutz Datenschutzbehörde Datenschutzbeschwerde Datenschutzverfahren erkennungsdienstliche Daten Löschung Lösungsbegehren Lösungsinteresse Rückfallsgefahr strafgerichtliche Verurteilung Straftat Tilgung Verdacht

European Case Law Identifier (ECLI)

ECLI:AT:BVWG:2020:W101.2134867.1.00

Im RIS seit

24.09.2020

Zuletzt aktualisiert am

24.09.2020

Quelle: Bundesverwaltungsgericht BVwG, <https://www.bvwg.gv.at>

© 2024 JUSLINE

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

www.jusline.at