WIEN / 8. Februar 2018

Stellungnahme

Zum Ministerialentwurf Datenschutz-Anpassungsgesetz-Inneres (3/ME XXVI.GP)

Für epicenter.works
Mag.ª Angelika Adensamer, MSc,
Ing. Dr. Christof Tschohl,
Mag. Stefan Hirschmann, MSc
Thomas Lohninger, BA

EPICENTER .WORKS
for digital rights

1 VORWORT UND KURZFASSUNG

Der vorliegende Entwurf unternimmt notwendige Anpassungen in einer Reihe von Materiengesetzen um sie an die, im Mai in Kraft tretenden, EU-Vorgaben anzugleichen.[1] Leider versucht das Innenministerium im vorliegenden Entwurf ebenfalls eine Reihe an Verschlechterungen für den Datenschutz vorzunehmen. Betroffenenrechte sollen abgebaut und Kontroll- und Transparenzpflichten der öffentlichen Verwaltung gesenkt werden. Damit werden nicht nur europarechtliche Vorgaben unterlaufen und zum Missbrauch sensibler Daten in staatlichen Stellen eingeladen, es wird auch die große Chance verpasst, die österreichischen Sicherheitsbehörden zeitgemäß und datenschutzkonform aufzustellen.

Bei automatisierten Abfragen soll in den Protokollaufzeichnungen keine Zuordnung zu einem bestimmten Organwalter mehr getroffen werden. Datenmissbrauch wäre so kaum mehr nachzuweisen oder aufzuklären. Um die Einhaltung von Grundrechten und Datenschutzvorschriften zu gewährleisten, ist es unerlässlich, dass jeder Datenzugriff durch (Sicherheits-)Behörden nachvollziehbar ist – auch ein automatisierter. Praktischer Grundrechtsschutz bedeutet, dass natürlich auch Informationen über die Personen protokolliert werden, die auf die Daten zugreifen oder diese empfangen.

Auch eine Senkung der Speicherfristen von Protokolldaten ist geplant. Sie sollen sogar kürzer sein als die Beschwerdefristen. Wer sich etwa fristgerecht mit einer Beschwerde an die Behörden wendet, muss künftig damit rechnen, dass keine Informationen mehr vorliegen, um diese nachzuvollziehen. Ein Beispiel: Die Beschwerdefrist an die Datenschutzbehörde ist mit maximal drei Jahren nach Feststellung des Ereignisses festgesetzt. Die Protokolldaten würden nach dem neuen Gesetz schon nach zwei Jahren gelöscht. Besonders bedenklich ist, dass sie sogar gelöscht werden können, wenn schon eine Beschwerde erhoben wurde. Die Reduktion wird mit Hinweis auf die Grundsätze der „Datenminimierung und Speicherbegrenzung“ (siehe Erl. S. 2) begründet. Der Grundsatz der Datensparsamkeit wurde in der DSGVO aber geschaffen, um die Privatsphäre der Betroffenen zu schützen und nicht die Institutionen, die Daten missbräuchlich verarbeiten.

Darüber hinaus enthält das geplante Gesetz einige Verschärfungen im Zusammenhang mit dem Fremdenrecht. Zum einen werden die Informationspflichten aufgeweicht: Informationsblätter über erkennungsdienstliche Behandlungen nach dem FPG müssen nicht mehr in einer für Betroffene verständlichen Sprache ausgehändigt werden. Zum anderen wird das Auskunftsrecht beschnitten. Mit einer unklar definierten Regelung kann die Auskunft verweigert werden, wenn sie „überwiegenden öffentlichen Interessen“ widerspricht. Es ist nicht nachvollziehbar, was damit gemeint sein könnte.

Im Entwurf wird der Bundesminister für Inneres als Auftragsverarbeiter bezeichnet. Das ist normalerweise ein Dienstleister, der im Auftrag Daten verarbeitet. Damit kommt es zur widersprüchlichen Situation, dass der Bundesminister in vielen Bereichen weisungsbefugt ist, aber dennoch nicht Verantwortlicher im Sinne der DSGVO. Dies scheint auch im Hinblick auf die Bundesverfassung und die europarechtlichen Vorgaben problematisch und trägt auch nicht zu einem effizienten Agieren der öffentlichen Verwaltung bei.

1 **https://www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00003/index.shtml**

Inhaltsverzeichnis

2 PROTOKOLLIERUNGSPFLICHTEN

Aufbewahrungsfristen

Datenschutz bedeutet auch Kontrolle. Nach Art. 24 Abs. 1 DSGVO besteht die Pflicht, geeignete technische und organisatorische Maßnahmen zu setzen, um „sicherzustellen und den Nachweis erbringen zu können, dass die Verarbeitung gemäß [der DSGVO] erfolgt". Organisatorische Maßnahmen i.S.d. Art. 24 Abs. 1 beinhalten u.a. Protokollierungen[2] sowie die Überwachung der Verarbeitung personenbezogener Daten.[3]

Im vorliegenden Entwurf ist eine **Reduzierung der Aufbewahrungsdauer von Protokolldaten von drei auf zwei Jahren** im GedenkstättenG, im MeldeG (§ 14 Abs. 5), im PassG, im PersonenstandsG (§ 44 Abs. 4 und § 44 Abs. 5), im PStSG (§ 9 Abs. 3) im SPG (§ 13a Abs. 4) und im WählerevidenzG (§ 4 Abs. 3) vorgesehen.

Beschwerde an die Datenschutzbehörde ist gem. § 24 Abs. 4 DSG neu **innerhalb eines Jahres ab Kenntnis des Ereignisses** zu erheben, das Gegenstand der Beschwerde ist, **längstens** jedoch **binnen drei Jahren nach dem Ereignis**. Das heißt, die **Protokolldaten könnten noch während der offenen Beschwerdefrist gelöscht werden.** Da es keine gegenteilige Bestimmung gibt, könnten sie sogar während eines laufenden Verfahrens gelöscht werden müssen.

Begründet wird dies in den Erläuterungen mit den Grundsätzen der Datenminimierung (Art. 5 Abs. 1 lit e DSGVO) und Speicherbegrenzung (Art. 5 Abs. 1 lit c DSGVO) in der DSGVO (s. z.B. S. 2 und 4). Diese Grundsätze können aber im Sinne der DSGVO nicht derart ausgelegt werden, dass sie die datenschutzrechtliche Kontrolle, die durch eine Protokollierung gewährleistet wird, einschränken

2 Martini, Art. 24 in Paal/Pauly, Datenschutzgrundverordnung, S. 283, Rz. 22.
3 Martini, Art. 24 in Paal/Pauly, Datenschutzgrundverordnung, S. 283, Rz. 23.

sollen. Zwar ist anzuerkennen, dass eine personenbezogene Protokollierung der Zugriffe auch einen Eingriff in das Datenschutzgrundrecht der Mitarbeiter (Organwalter) der Polizei bedeutet und als solcher ebenso einer Rechtfertigung bedarf. Es ist aber keinesfalls im Sinne der DSGVO, den Datenschutz für BehördenmitarbeiterInnen jenem der von einer staatlichen Datenanwendung betroffenen Personen überzuordnen.

Nach den Grundsätzen der Datenminimierung und Speicherbegrenzung, muss die Datenverarbeitung und die Länge der Datenaufbewahrung den Zwecken der Datenverarbeitung angemessen sein. Der Zweck der Protokollierung ist es, vor Missbrauch zu schützen. Dieser Zweck wird bei einer verkürzten Löschungsfrist nicht erfüllt, daher können diese Grundsätze auch nicht die Verkürzung der Aufbewahrungsfrist für Zugriffsprotokolle rechtfertigen.[4]

Wichtig wäre es, die die Aufbewahrungsfrist von Protokolldaten davon abhängig zu machen, wie lange die Daten gespeichert werden dürfen, wie lange die Betroffenen Beschwerde erheben können und ob es anhängige Verfahren gibt. Damit würde auch eine objektivierte Begründung zur jeweiligen Speicherdauer der Zugriffsprotokolle bestehen. Protokolldaten müssen aber auf jeden Fall so lange aufbewahrt werden, wie es für einen effektiven Rechtsschutz notwendig ist.

Sonderfall sicherheitspolizeilicher Bereich

Für die Verarbeitung personenbezogener Daten durch die Behörden zum Zweck der Verhütung von Straftaten oder der Strafvollstreckung, des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherheit (§ 38 Abs. 1 DSG neu) gilt außerdem § 50 DSG neu.

Durch diese Bestimmung sollen die Vorgaben der im sicherheitspolizeilichen Bereich maßgeblichen DS-RL für Polizei und Strafsachen (Nr. 680/2016) erfüllt werden. In Art. 25 Abs. 2 werden die Zwecke der Protokollierungen angeführt: Sie dienen der „Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung, der Sicherstellung der Integrität und Sicherheit der Daten“. An diesen Zwecken ist also auch die Länge der Aufbewahrung von Protokollen zu messen.

Darüber hinaus heißt es in Erwägungsgrund 56 der oben genannten DS-RL:

> *„Zum Nachweis der Einhaltung dieser Richtlinie sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis aller Kategorien von Tätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage dieses Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieses Verzeichnisses kontrolliert werden können. Der Verantwortliche oder der Auftragsverarbeiter, der personenbezogene Daten in nicht automatisierten Verarbeitungssystemen verarbeitet, sollte über wirksame Methoden zum Nachweis der Rechtmäßigkeit der Verarbeitung, zur Ermöglichung der Eigenüberwachung und zur Sicherstellung der Integrität und Sicherheit der Daten, wie etwa Protokolle oder andere Formen von Verzeichnissen, verfügen.“*

In den Erläuterungen zur Einführung des neuen DSG heißt es zu § 50: „Die Verzeichnisse sind so zu führen, dass eine nachträgliche Überprüfung der Rechtmäßigkeit der Datenverarbeitung möglich ist.“

4 Siehe dazu auch die Stellungnahme des ÖGB, 13/SN-3/ME XXVI. GP, S. 6 https://www.parlament.gv.at/PAKT/VHG/XXVI/SNME/SNME_00078/imfname_680396.pdf und die des ÖRAK, 14/SN-3/ME XXVI:GP, S: 3f https://www.parlament.gv.at/PAKT/VHG/XXVI/SNME/SNME_00080/imfname_680401.pdf.

Außerdem wird hier davon ausgegangen, eine gesetzlich festgelegte Löschungsfrist für Protokolldaten sei „nicht zweckmäßig".[5]

Nunmehr sollen alle Datenverarbeitungen nach dem SPG nach den Bestimmungen des § 63 SPG erfolgen, gem. § 63 Abs. 3 soll die Speicherfrist für Protokolldaten zwei Jahre betragen. Bisher mussten die Protokolldaten gem. § 59 Abs. 3 drei Jahre aufbewahrt werden. Auf die Verkürzung der Aufbewahrungsfrist von Protokolldaten nach dem SPG wird in den Erläuterungen zum vorliegenden Entwurf nicht eingegangen.

Rückführbarkeit auf konkrete Organwalter

§ 63 Abs. 3 SPG und § 11 PolKG sollen in Zukunft lauten: „§ 50 DSG gilt mit der Maßgabe, dass die Zuordnung zu einem bestimmten Organwalter bei automatisierten Abfragen nicht erforderlich ist. Die Protokollaufzeichnungen sind zwei Jahre aufzubewahren und danach zu löschen. Von der Protokollierung ausgenommen sind automatisierte Abfragen gemäß § 54 Abs. 4b, es sei denn, es handelt sich um einen Trefferfall."

Diese Einschränkungen der Protokollierungspflichten im sicherheitspolizeilichen Bereich sind besorgniserregend.[6] Um die Einhaltung von Grundrechten und Datenschutzvorschriften zu gewährleisten, ist es unerlässlich, dass jeder Datenzugriff – auch ein automatisierter – durch die Sicherheitsbehörden genau dokumentiert wird. Praktischer Grundrechtsschutz bedeutet deshalb, dass nicht nur Datum, Uhrzeit und Zweck der Abfrage sowie die verarbeiteten Daten dokumentiert werden müssen, sondern natürlich auch die Identität der Person, die auf die Daten zugreift oder diese empfängt. Bei automatisierten Abfragen ist dies im SPG und PolKG ausdrücklich nicht vorgesehen. So wäre nicht feststellbar, wer die Daten empfangen hat.

Die Auslegung dieser Bestimmung steht und fällt mit der Frage nach der Definition von „automatisierten Abfrage".

Um dies zu beurteilen, hilft ein chronologischer Blick auf die Protokollierungspflichten im SPG. Bis 2005 musste jede Datenabfrage protokolliert werden. 2005 kam eine Ausnahme für die automatisierte Kfz-Kennzeichenerkennung hinzu, die bis heute besteht. Hier müssen jedoch Treffer sehr wohl protokolliert werden.

2016 kam in der gleichen Reform, mit der auch das Polizeiliche Staatsschutzgesetz eingeführt wurde, eine weitere Ausnahme hinzu: die Protokollierung der Identität des Organwalters ist bei automatisierten Abfragen seither nicht mehr erforderlich. Eine Ausnahme für Treffer wie bei der Kfz-Kennzeichenerfassung wurde nicht gemacht. In den Erläuterungen dieser Reform hieß es, bei automatisierten Abfragen erfolge „die gesamte Datenverwendung programmgesteuert".[7] Ein Beispiel sei der Abgleich einer Wohnsitzmeldung mit dem Register zur Personenfahndung. Diese Ausnahme träfe also nur auf vollautomatisierte Abfragen zu, hieß es damals.

Durch die jetzige Reform sollen insbesondere – so wieder die Erläuterungen – „die materienspezifischen Datenschutzregelungen mit der neuen datenschutzrechtlichen Terminologie in

5 Erläuterungen 1664 der Beilagen XXV. GP, S.22f.

6 Siehe dazu auch die Stellungnahme des ÖGB, 13/SN-3/ME XXVI.GP, S. 5f https://www.parlament.gv.at/PAKT/VHG/XXVI/SNME/SNME_00078/imfname_680396.pdf und die des ÖRAK, 14/SN-3/ME XXVI:GP, S: 4f https://www.parlament.gv.at/PAKT/VHG/XXVI/SNME/SNME_00080/imfname_680401.pdf.

7 763 der Beilagen XXV.GP - Regierungsvorlage – Erläuterungen, S.14.

Einklang gebracht werden“ (S. 2). Das Ziel ist also, dass Begrifflichkeiten in den verschiedenen Gesetzen gleich definiert sind.

Nun kennt aber auch das **neue Datenschutzgesetz** eine **Definition des Begriffs „automatisiert“** – und zwar eine sehr viel weitere: so sei, laut Erläuterungen unter einem **„automatisierten“ Abruf „insbesondere die Abfrage von Datenbanken zu verstehen“**.[8]

Somit fällt unter das neue Datenschutzrecht **so gut wie jede Abfrage, nicht nur die vollautomatisierten**. Damit bekäme die zuvor schon problematische Ausnahme der Protokollierungspflichten einen noch viel weiteren Anwendungsbereich.

Es gibt nun also zwei mögliche Lesarten: **Entweder** wird die „automatisierte“ Abfrage im SPG auch weiterhin eine viel engere Bedeutung als im Datenschutzrecht haben, was heißt, dass die **Harmonisierung mit dem neuen Datenschutzrecht nicht erreicht** werden würde. **Oder** aber es gilt die Anwendbarkeit der neuen Definition, die **Protokollierungspflichten würden empfindlich eingeschränkt** und es **entstünde** eine sehr **ernstzunehmende Rechtsschutzlücke**. In beiden Lesarten erweist sich der Entwurf also als problematisch.

Gem. Art. 25 der DS-RL Polizei und Justiz (Nr. 2016/680) müssen die Verarbeitungsvorgänge in automatisierten Verarbeitungssystemen protokolliert werden, und zwar auf eine Weise, dass „so weit wie möglich die Identifizierung der Person, die die bezogenen Daten abgefragt oder offen gelegt hat, und die Identität des Empfängers solcher personenbezogenen Daten“ feststellbar ist. In Erwägungsgrund 57 der DS-RL heißt es zudem: „Die Identifizierung der Person, die personenbezogene Daten abgefragt oder offengelegt hat, sollte protokolliert werden und aus dieser Identifizierung sollt sich die Begründung für die Verarbeitungsvorgänge ableiten lassen.“ Davon kann also nur abgesehen werden, wenn und insoweit dies unmöglich ist. In den Erläuterungen zu § 63 Abs. 3 SPG heißt es dazu nach Art. 25 Abs. 1 DS-RL sei die Identifizierung „nur so weit wie möglich erforderlich“ (S. 49). Es wird aber nicht erklärt, wieso und in welchen Fällen die Identifizierung der Person unmöglich sei. Zu § 11 PolKG heißt es in den Erläuterungen: „Die Zuordnung zu einem bestimmten Organwalter ist bei automatisierten Abfragen nicht erforderlich.“ (S. 56) Diese Rechtsansicht ist im Lichte des Art. 25 DS-RL stark zu bezweifeln. Die hier geschaffene Ausnahme geht insofern zu weit als sie auch Fälle umfasst, in denen die Identifizierung der Person die die Abfrage tätigt, oder die Daten im Trefferfall erhält, sehr wohl möglich wäre. Sie widerspricht somit Art. 25 DS-RL.[9]

Gerade im Hinblick auf vergangene Missbrauchsfälle[10] im österreichischen Sicherheitsapparat ist eine solche Unklarheit bei den Protokollpflichten sehr bedenklich. Die Folge kann sein, dass der Rechtsschutz von Betroffenen, die sich künftig gegen die missbräuchliche Verwendung ihrer Daten oder gegen eine illegale Datenweitergabe beschweren wollen, empfindlich eingeschränkt wird.

8 1664 der Beilagen XXV.GP – Regierungsvorlage – Erläuterungen, S. 17.

9 Siehe dazu auch die Stellungnahme von Urban 5/SN-3/ME XXVI. GP. https://www.parlament.gv.at/PAKT/VHG/XXVI/SNME/SNME_00053/imfname_678368.pdf.

10 Siehe z.B. Weichhart, NÖ: Polizist besorgte sich illegal Telefonnummer, Kurier.at, 21.02.2017, https://kurier.at/chronik/niederoesterreich/polizist-besorgte-sich-illegal-telefonnummer/247.746.752.

3 WIDERSPRUCHSRECHTE FÜR HISTORISCHE UND WISSENSCHAFTLICHE ZWECKE

In § 16b Abs. 5 MeldeG und in § 52 Abs. 4a PersonenstandsG soll es in Zukunft heißen: „Soweit personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken verarbeitet werden, kommen dem Betroffenen die Rechte gemäß Art. 15, 16, 18 und 21 DSGVO nicht zu."

Es sollen also das Auskunftsrecht (Art. 15), das Recht auf Berichtigung (Art. 16), das Recht auf Einschränkung der Verarbeitung (Art. 18) und das Widerspruchsrecht (Art. 21) eingeschränkt werden. Außerdem lässt sich aus den Erläuterungen schließen, dass vorgesehen wird, dass auch die Informationspflicht gem. Art. 14 Abs. 5 keine Anwendung finden soll, „wenn und soweit sich die Erteilung dieser Information als unmöglich erweisen oder einen unverhältnismäßigen Aufwand erfordern würde." (S.7f)

Laut den Erläuterungen (S.7) soll hier das Recht gem. Art. 89 Abs. 2 DSGVO genutzt werden, unter den Voraussetzungen des Abs. 1 gesetzliche Ausnahmen zu den oben aufgezählten Rechten zu schaffen. Hier heißt es: „Da es in der Praxis kaum möglich wäre, gegenüber Betroffenen bei statistischen und wissenschaftlichen oder historischen Erhebungen aufgrund der hohen Datenmengen sämtliche dieser Rechte zu wahren, bzw. die Wahrung der Betroffenenrechte die Verwirklichung der spezifischen Forschungs- bzw. statistischen Zwecke ernsthaft beeinträchtigen, wenn nicht sogar unmöglich machen würde, soll die Ausnahmeermächtigung gemäß Art. 89 Abs. 2 DSGVO in Anspruch genommen werden."

Eine gem. Art. 89 Abs. 2 **zulässige Ausnahmeregelung erfordert** aber die **Durchführung einer Verhältnismäßigkeitsprüfung**.[11] **Eine solche wurde hier nicht vorgenommen.** Die Interessen müssen außerdem für jeden konkreten Fall abgewogen werden.[12] Eine **Pauschalregelung**, wie sie hier vorgenommen wurde, kann also keineswegs von Art. 89 Abs. 2 DSGVO gedeckt sein und ist damit **unionsrechtswidrig.**

Zu § 16b insgesamt wird außerdem darauf hingewiesen, dass mathematische Verfahren zur Bereitstellung von Aggregatdaten zur statistischen Auswertung existieren, die Rückschlüsse von übermittelten Daten auf einzelne Personen mathematisch auszuschließen vermögen. Käme ein solches Verfahren statt der Übermittlung pseudonymisierter Datensätze, wie in Abs. 3 bestimmt, zum Einsatz, wäre es nicht notwendig, sich darauf zu verlassen, dass der Empfänger sich ausschließlich „rechtlich zulässige[r] Mittel" (Abs. 3) bedient. Ein solches Verfahren könnte – soweit möglich – auch bei Anwendung des Abs. 5 vorgesehen werden.

11 Pauly, Art. 89, in Paal/Pauly, Datenschutzgrundverordnung, S. 778, Rz. 14.
12 Ebd.

4 EINSCHRÄNKUNG VON RECHTEN IM FREMDENRECHT

Auskunftsrechte

Allgemein

Nach § 23 Abs. 4 BFA-VG (neu) soll die **Auskunftserteilung** gem. Art. 15 DSGVO **aus verschiedenen Gründen** zu **unterbleiben** haben und zwar **soweit dies**:

> *„1. zum Schutz der nationalen Sicherheit und Landesverteidigung,*
>
> *2. zum Schutz der öffentlichen Sicherheit,*
>
> *3. zum Schutz der verfassungsmäßigen Einrichtungen der Republik Österreich,*
>
> *4. zum Schutz der Betroffenen oder der Rechte und Freiheiten anderer Personen, oder*
>
> *5. aus sonstigen überwiegenden öffentlichen Interessen notwendig und verhältnismäßig ist“*

In § 98 Abs. 1 FPG, § 34 Abs. 1 NAG, § 8 Abs. 1 GrundversorgungsG und § 15 Abs. 1 letzter Satz GrenzkontrollG soll nun auf § 23 Abs. 3 – 5 BFA-VG verwiesen werden, womit die obengenannte Einschränkung des Auskunftsrechts gem. Art. 15 DSGVO auch dort tragend wird. Die Aufzählung der Gründe, aus denen das Auskunftsrecht nach Art. 15 eingeschränkt werden kann, wurde wortwörtlich aus Art. 23 DSGVO übernommen. Die hier einfachgesetzlich erlassene Einschränkung ist nicht konkret und bestimmt genug, um den Voraussetzungen des Art. 23 Abs. 2 DSGVO zu genügen.[13]

Gemäß Art. 23 DSGVO kann eine solche **Einschränkung der Rechte in der DSGVO nur bestehen**, „**sofern** eine solche **Beschränkung** den **Wesensgehalt der Grundrechte und Grundfreiheiten achtet** und **in einer demokratischen Gesellschaft** eine **notwendige und verhältnismäßige Maßnahme** darstellt“. Eine dahingehende Abwägung wurde bei der hier gegenständlichen Bestimmung nicht getroffen, sondern diese vielmehr auf den Einzelfall verschoben. Somit wurde aber die Voraussetzung einer verhältnismäßigen einfachgesetzlichen Determinierung umgangen.

Auch muss eine **Gesetzgebungsmaßnahme** nach Art. 23 DSGVO, wie in Erwägungsgrund 41 angeführt **„klar und präzise“** sein, und ihre **Anwendung** sollte für die Rechtsunterworfenen **vorhersehbar** sein. **Dies ist durch** das **pauschale Abstellen auf Einzelfallentscheidungen** durch die Behörden **nicht gegeben.** Jedenfalls wäre klarzustellen, dass eine begründete Abwägung im Einzelfall zu erfolgen hat.

Darüber hinaus **müssen Ausnahmen** gem. Art. 23 Abs. 2 DSGVO auch

*„**spezifische Vorschriften enthalten** zumindest in Bezug auf*

> *a) die Zwecke der Verarbeitung oder die Verarbeitungskategorien,*
>
> *b) die Kategorien personenbezogener Daten,*
>
> *c) den Umfang der vorgenommenen Beschränkungen,*

13 Siehe dazu auch die Stellungnahme des ÖGB, 13/SN-3/ME XXVI.GP, S. 5.

d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung;

e) die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen,

f) die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,

g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und

h) das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist."

Auf diese Erfordernisse wird im vorliegenden Entwurf nicht ausreichend eingegangen.

Insgesamt kann festgestellt werden, dass die Ausnahme in ihrer Breite wie sie hier vorgesehen ist, unionsrechtswidrig ist.

Die Verfassungsbestimmung des § 1 DSG 2000 determiniert den Datenschutz als Grundrecht und als Jedermannsrecht. Auch Drittstaatsangehörige fallen also unter seinen Schutz. gem. § 1 Abs. 3 DSG 2000 ist auch das Recht auf Auskunft Teil dieses Grundrechts. Auch der VfGH erkannte schon 2003 in VfSlg 16.986, dass der generelle Ausschluss des Auskunftsrechts der Verfassungsbestimmung des § 1 Abs. 3 Z 1 DSG 2000 widerspricht. Sollte es also zum Ausschluss der Auskunftsrechte in diesem Ausmaß kommen, bleibt abzuwarten, ob dies nicht eine Verletzung des Grundrechts auf Datenschutz gem. § 1 DSG darstellt.

Informationspflichten

Bei erkennungsdienstlichen Behandlungen nach dem FPG ist der Betroffene gem. § 100 Abs. 1 FPG „über den Grund der erkennungsdienstlichen Behandlung zu informieren. Ihm ist ein schriftliches Informationsblatt darüber auszufolgen; dabei ist grundsätzlich danach zu trachten, dass dieses in einer ihm verständlichen Sprache abgefasst ist."

Diese Regelung wird nun durch die allgemeinen Informationspflichten in Art. 13f Abs. 1 DSGVO ersetzt, nach denen der Verantwortliche verpflichtet ist, der betroffenen Person zum Zeitpunkt der Datenerhebung eine Reihe von Informationen zu geben, z.B. den Namen und die Kontaktdaten des Verantwortlichen (lit. a), die Verarbeitungszwecke und die Rechtsgrundlage der Verarbeitung (lit. c), gegebenenfalls die Absicht des Verantwortlichen, die Daten an ein Drittland zu übermitteln (lit. f). Erwägungsgrund 60 der DSGVO sieht außerdem vor, dass die betreffenden Informationen in „leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form" bereitgestellt werden.

Diese sehen jedoch keine Übersetzung der Informationen vor, wenn vorherzusehen ist, dass die betroffene Person die Landessprache wahrscheinlich nicht spricht. Insofern stellt die Streichung also eine Verschlechterung für die Betroffenen dar. Die Umsetzung der neuen EU-rechtlichen Datenschutzprinzipien sollte nicht zum Anlass genommen werden, um Betroffenenrechte einzuschränken.

Im Asylverfahren ist die Übersetzung aller verfahrensrelevanten Informationen durch Art. 4 Abs. 2 Dublin III-VO (Nr. 604/2013), Art. 12 der Asylverfahrens-RL (2013/32/EU) und Art. 22 Status-RL (2011(95/EU) garantiert. Die Information über erkennungsdienstliche Behandlung im Asylverfahren ist gem. § 25 Abs. 1 BFA-VG auch in einer dem Betroffenen verständlichen Sprache vorgesehen. Diese

Bestimmung wurde – wohl unter anderem im Hinblick auf die oben genannten EU-Richtlinien – im vorliegenden Entwurf nicht geändert.

Dies führt zur Situation, dass Drittstaatsangehörige, die sich im Asylverfahren befinden einen besseren Rechtsschutz genießen, als die, die andere Aufenthaltstitel haben bzw. anstreben. Dies verstößt sowohl gegen das Verbot der Ungleichbehandlung zwischen Fremden untereinander gem. Art. 2 StGG i.V.m. Art. 7 Abs. 1 B-VG und gegen Art. 1 Abs. 1 BVG-Rassendiskriminierung.

5 AUFTRAGSVERARBEITER UND VERANTWORTLICHE

Durch den vorliegenden Entwurf sollen die verschiedenen Behörden jeweils in ihrem Bereich als gemeinsam Verantwortliche im Sinne von Art. 4 Z 7 i.V.m. Art. 26 Abs. 1 DSGVO agieren. So z.B. die Meldebehörden gem. § 16 Abs. 1 MeldeG (neu), die Passbehörden gem. § 22b Abs. 1 PassG (neu), die Personenstandsbehörden nach § 44 Abs. 1 PersonenstandsG (neu) und die Vereinsbehörden nach § 18 Abs. 1 VereinsG (neu). Dies ergibt insoweit Sinn, als diese gem. Art. 4 Z 7 DSGVO „über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden".

Zugleich soll aber der Bundesminister für Inneres Auftragsverarbeiter i.S.v. Art. 4 Z 8 i.V.m. Art. 28 Abs. 1 DSGVO werden, so z.B. in § 16 Abs. 2a MeldeG (neu), § 22b Abs. 1b PassG (neu), § 44 Abs. 3 PersonenstandsG (neu), § 18 Abs. 1b VereinsG (neu), § 55 Abs. 2 WaffG, in § 26 Abs. 3 BFA-VG (für das zentrale Fremdenregister), § 28 Abs. 2 BFA-VG (für das zentrale Verfahrensregister) und in § 104 Abs. 3 FPG, § 36 Abs. 3 Niederlassungs- und AufenthaltsG.

Gemäß Art. 19 Abs. 1 sind die Bundesminister die obersten Organe der Vollziehung und gem. Art. 20 Abs. 1 B-VG sind den BundesministerInnen alle Organe weisungsgebunden.

Im Bereich der mittelbaren Bundesverwaltung ist dem Bundesminister auch der Landeshauptmann weisungsunterworfen (Art. 102 Abs. 1 B-VG), so also z.B. bei vielen der fremdenrechtlichen Materien, dem Passwesen, dem Meldewesen, dem Waffenwesen, etc.

Das führt zu der widersprüchlichen Situation, dass in vielen der Bereiche, der Bundesminister zwar weisungsbefugt ist, aber dennoch nicht Verantwortlicher i.S.d. DSGVO ist, obwohl er nach der Bundesverfassung die Befugnis hätte, „über der Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden". Das Konzept der Auftragsverarbeitung ist aber gerade dadurch geprägt, dass der Auftragsverarbeiter durch den Auftraggeber (den Verantwortlichen i.S.d. Art. 4 Z 7 DSGVO) vollständig determiniert ist und eine Überschreitung des Auftrages zur Datenverarbeitung regelmäßig rechtswidrig ist (wenngleich dies ausnahmsweise z.B. im lebenswichtigen Interesse Dritter anders sein kann). Die vorgeschlagene Festlegung der Rollenverteilung steht damit sowohl mit der DSGVO als auch mit der Bundesverfassung im Widerspruch.

Holzinger/Oberndorfer/Raschauer schreiben zur Bedeutung der Weisungsgebundenheit: „Das verfassungsrechtliche Weisungsprinzip stellt einen wesentlichen Faktor für die demokratische Verfasstheit eines Staates dar. Mit diesem organisationsrechtlichen Instrument ist sichergestellt, dass die politische Verantwortlichkeit der Exekutive gegenüber dem Parlament gewährleistet ist."[14] Alles

14 Holzinger/Oberndorfer/Raschauer, Österreichischer Verwaltungslehre[3], S. 348.

andere wäre demokratiepolitisch und innerhalb des österreichischen Staatsgefüges höchst problematisch.

Den BMI als Auftragsverarbeiter i.S.d. DSGVO einzusetzen, entspricht nicht ihrem Sinn, so heißt es z.B. in Art. 4 Z 8 DSGVO der Auftragsverarbeiter arbeite „im Auftrag des Verantwortlichen". Die Working Party 29 schreibt zur Auslegung der Begriffe „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" i.S.d. DSGVO: „Es sollte sichergestellt werden, dass die benannte Stelle [die Verantwortlichen] über eine wirksame Kontrolle über die Verarbeitungen verfügt."[15] Außerdem sei die Ermittlung des „»für die Verarbeitung Verantwortlichen«" unter dem Aspekt des Datenschutzes [...] in der Praxis eng mit den zivil-, verwaltungs- und strafrechtlichen Vorschriften über die Zuweisung von Verantwortlichkeiten oder die Verhängung von Sanktionen verknüpft, denen eine juristische oder natürliche Person unterliegen kann".[16] Auch das ist also ein Indiz, dass aufgrund seiner verfassungs- und verwaltungsrechtlichen Weisungsbefugnis der Bundesminister für Inneres tatsächlich Verantwortlicher für die Datenverarbeitung ist. Zwar räumt Art. 6 Abs. 2 DSGVO den Mitgliedstaaten den Spielraum ein, insbesondere im Bereich des öffentlichen Rechts „spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften" der DSGVO zu normieren.

Die Lösung könnte sein, auch den Bundesminister für Inneres gesetzlich als einen der datenschutzrechtlich gemeinsam Verantwortlichen zu bestimmen, soweit die mit der Verarbeitung durch gesetzliche Vorschriften betraute Behörde oder Stelle eine eigenständige öffentlichrechtliche Körperschaft darstellt, wie dies insbesondere im Rahmen der mittelbaren Bundesverwaltung der Fall ist. Soweit die für die Verarbeitung gesetzlich zuständige öffentliche Stelle eine Organisationseinheit des Bundesministeriums für Inneres ohne eigne Rechtspersönlichkeit ist, macht eine Bestimmung zur gemeinsamen Verantwortung jedoch keinen Sinn.

Die Berücksichtigung dieser Anregung wird sowohl aus unionsrechtlicher als auch aus verfassungsrechtlicher Sicht dringend empfohlen. Zwar wird in dieser Stellungnahme darauf verzichtet, besondere Problemkonstellationen zu skizzieren, doch es ist nur eine Frage der Zeit, bis aus dieser doppelten Widersprüchlichkeit reale Probleme mit dem Verantwortungszusammenhang entstehen.

15 Art.ikel-29_Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 15.

16 Art.ikel-29_Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 20.

6 UNSERE FORDERUNGEN

1. Wenn Abfragen aus behördlichen Datenbanken erfolgen, dann müssen diese so protokolliert werden, dass ein allfälliger Missbrauch auch nachvollzogen werden kann. Die Rechtsunsicherheit, die aus der Verwendung des Begriffes „automatisierte Abfragen" entsteht, muss beseitigt werden, auch im Sinne der angestrebten Begriffsharmonisierung.

2. Protokolldaten müssen so lange aufbewahrt werden, wie es für einen effektiven Rechtsschutz notwendig ist. Dies kann von der Speicherdauer der betroffenen personenbezogenen Daten selbst, den Beschwerdefristen, laufenden Verfahren sowie von den Verjährungsfristen von Delikten wie Amtsmissbrauch abhängen.

3. Datenschutz ist ein Menschenrecht. Drittstaatsangehörige dürfen beim Datenschutz nicht schlechter gestellt werden. Auch beim Datenschutz hat Diskriminierung keinen Platz.

4. Verantwortlichkeiten müssen klar geregelt sein und dürfen nicht durch einander widersprechende Weisungsgebundenheit relativiert werden. Eine Lösung für das Problem der Rollenverteilung könnte sein, den Bundesminister für Inneres gesetzlich als einen der datenschutzrechtlich gemeinsam Verantwortlichen zu bestimmen – zumindest für die Fälle, in denen verschiedene öffentlich-rechtliche Körperschaften mit der Durchführung betraut sind.