Epizentrum – Plattform für grundrechtsbasierte Zukunftspolitik
(vormals AKVorrat)

Annagasse 8/1/8, 1010 Wien
team@epicenter.works
www.epicenter.works
ZVR: 140062668

Wien, 22. Juni 2017

Betreff:

Stellungnahme im Begutachtungsverfahren zum Entwurf eines Bundesgesetzes, mit dem das Bundes-Verfassungsgesetz geändert, das Datenschutzgesetz erlassen und das Datenschutzgesetz 2000 aufgehoben wird (Datenschutz-Anpassungsgesetz 2018) (XXV. GP 322/ME, unter Berücksichtigung der am 07.06.2017 beschlossenen Regierungsvorlage[1] [1664 d.B.])

Für epicenter.works:

Mag.iur. Alexander Czadilek, Dipl.-Ing. Dr.iur. Walter Hötzendorfer, Ing. Dr.iur. Christof Tschohl

epicenter.works nimmt zum vorliegenden Gesetzesentwurf wie folgt Stellung:

Inhaltsverzeichnis

1 https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_01664/index.shtml.

I. Vorwort und Kurzfassung

Vorweg zu kritisieren ist, dass das Datenschutz-Anpassungsgesetz 2018 während offener Begutachtungsfrist und zudem ohne Notwendigkeit bereits Anfang Juni als Regierungsvorlage zur Übermittlung an den Nationalrat beschlossen wurde. **Ein solches Vorgehen ist demokratiepolitisch höchst bedenklich und abzulehnen, da den privaten wie öffentlichen Organisationen oder Einrichtungen die Möglichkeit genommen wird, dass ihre vorgebrachten Kritikpunkte eingehend behandelt werden und in das weitere Gesetzgebungsverfahren Einzug halten.** Eine Einarbeitung von Stellungnahmen im Begutachtungsverfahren im Rahmen des parlamentarischen Prozesses (Verfassungsauschuss, Plenum) wird nämlich kaum eine so ausführliche Diskussion und Auseinandersetzung mit der von verschiedensten Stellen vorgebrachten Kritik zulassen, wie eine ernsthafte Evaluierung der Vorbringen auf Ministerialebene. Besondere Brisanz bekommt solch eine Vorgehensweise aufgrund der möglichen Beschlussfassung im Nationalrat bereits wenige Tage nach Ende der Begutachtungsfrist[2].

Bei der notwendigen Anpassung des österreichischen Datenschutzgesetzes an die Datenschutzgrundverordnung (DSGVO) hat die Bundesregierung eine Minimalanpassung vorgenommen. Die Nichtinanspruchnahme der zahlreichen in der DSGVO enthaltenen Öffningsklauseln macht diesen Umstand deutlich. Andererseits werden gegenüber den Vorgaben der DSGVO z.T. höhere nationale Datenschutzstandards beibehalten und die Vorgaben sogar übererfüllt (sog Gold-Plating). Die Mindestumsetzung leistet zwar einen Beitrag zur Vollharmonisierung, mögliche Ergänzungen durch spezifische Materiengesetze[3] könnten aber wiederum zu einer Zersplitterung des Datenschutzrechts führen. Zudem würde diese Vorgehensweise einen laufenden Anpassungsbedarf in der Praxis hervorrufen. Ob dieses Vorgehen der Rechtssicherheit dient und dem Ziel des Verordnungsgebers, einen einheitlichen europäischen Rechtsrahmen zu schaffen, gerecht wird, wird sich erst, insbesondere durch die Rechtsprechung des Europäischen Gerichtshofs (EuGH), in den nächsten Jahren zeigen.

2 Ende der Begutachtungsfrist am 23.06.2017, Zuweisung an den Verfassungsausschuss am 26.06.2017 und voraussichtliche Beschlussfassung im Nationalrat am 27. oder 28.06.2017.

3 Siehe EB 1664 dB, 1.

Eine gesetzliche Neuregelung im Umfang des Datenschutz-Anpassungsgesetzes 2018 (DS-AnpG) weist naturgemäß viele offene und zu diskutierende Fragen auf. Angesichts dessen sowie der besonderen gesellschaftlichen und wirtschaftlichen Bedeutung dieses Gesetzes **ist die Begutachtungsfrist von sechs Wochen als zu knapp bemessen zu kritisieren**, weshalb epicenter.works sich in der vorliegenden Stellungnahme nur auf die unseres Erachtens besonders problematischen Bestimmungen bezieht.

Insbesondere bezieht sich unsere Kritik auf folgende Punkte:

- Das Vorgehen der Bundesregierung im Gesetzgebungsprozess (Beschluss des Entwurfs als Regierungsvorlage während offener Begutachtungsfrist und überhastete Beschlussfassung im Plenum) ist demokratiepolitisch äußerst bedenklich und abzulehnen, da diversen Stakeholdern die Möglichkeit der Partizipation genommen wird.
- Die Nichtinanspruchnahme der Möglichkeit, eine abstrakte Beschwerdebefugnis bzw. Verbandsklage zu schaffen, bewirkt das Fehlen eines wichtigen Instruments der objektiven Rechtmäßigkeitskontrolle und somit zur Durchsetzung des materiellen Datenschutzrechts, verhindert ein effektives Vorgehen österreichischer Organisationen gegen nichtösterreichische Verantwortliche und erhöht die Wahrscheinlichkeit, dass sich österreichische Verantwortliche vor ausländischen Gerichten/Behörden verantworten müssen.
- Die Befugnis der Datenschutzbehörde zu Datenschutzüberprüfungen wird auf Fälle "begründeten Verdachts" eingeschränkt - dies ist im Sinne der Effektivierung des Datenschutzrechts nicht geboten und zudem unionsrechtswidrig.
- Zahlreiche Bestimmungen des Entwurfs sind nicht klar genug formuliert, vor allem im Lichte des Spannungsverhältnisses der DSGVO mit dem österreichischen Verfassungsrecht und Verwaltungsstrafrecht. Dies betrifft insbesondere die Bestimmungen für die Verhängung von Geldbußen, was im Hinblick auf das strafrechtliche Bestimmtheitsgebot besonders problematisch ist.

- Das Beschwerderecht des Betroffenen wird durch Beschwerdefristen von einem Jahr nach Kenntnis und von drei Jahren nach Stattfinden des beschwerenden Ereignisses unsachgemäß und wohl auch unionsrechtswidrig eingeschänkt.
- Die generalpräventive Wirkung des Datenschutzrechts wird dadurch erheblich beschnitten, dass die Datenschutzbehörde Verfahren formlos einstellen kann, wenn der Beschwerdegegner währen des laufenden Verfahrens die behauptete Rechtsverletzung nachträglich beseitigt.
- Der räumliche Anwendungsbereich ist im DSG (2018) nicht definiert.

II. Zu den einzelnen Bestimmungen des Artikel 2 Datenschutz-Anpassungsgesetz 2018

§§ ohne Bezeichnung der Norm beziehen sich auf das DSG (2018)

zu § 1 (Grundrecht auf Datenschutz):

Wir begrüßen die **Neufassung des Grundrechts auf Datenschutz** und die damit einhergehende Eingrenzung auf natürliche Personen, weil dadurch die Bedeutung des Grundrechts als Persönlichkeits- und Freiheitsrecht wesentlich deutlicher zur Geltung kommt. Know-How, Betriebs- und Geschäftsgeheimnisse werden zukünftig insbesondere durch die noch umzusetzende EU-Geheimnisschutz-RL (RL 2016/943/EU) geschützt. Auch dass die früheren Begleitrechte auf Auskunft, Richtigstellung und Löschung nun im Basisgrundrecht ihren Niederschlag finden ist richtig, da diese nun nicht mehr einem Ausführungsvorbehalt[4] unterliegen.

zu § 2 (Anwendungsbereich):

Im DSG (2018) fehlt eine Regelung über den räumlichen Anwendungsbereich. Insoweit grenzüberschreitende Datenverarbeitungen innerhalb der EU oder des EWR erfolgen wäre es im Hinblick auf die anzuwendenden nationalen Anpassungs- bzw. Umsetzungsgesetze erforderlich, Kollisionsnormen zu schaffen, die festlegen, welches nationale Recht im Falle eines Normenkonflikts anzuwenden ist. **Durch das fehlen solcher Normen entsteht eine erhebliche Rechtsunsicherheit für alle Verantwortlichen und Betroffenen.**

zu § 11 Abs 1:

Hinsichtlich der Überprüfungsbefugnis der Datenschutzbehörde (DSB) im Fall "eines begründeten Verdachtes" auf Verletzung der in der DSGVO genannten Rechte und Pflichten ist anzumerken, dass in Art 58 Abs 1 lit b DSGVO, der unmittelbar anwendbar ist, eine Beschränkung der Befugnis der Aufsichtsbehörde auf "begründete Verdachtsfälle" nicht vorgesehen ist. Eine solche wäre auch nicht sachgerecht, da viele Arten von Verletzungen des Datenschutzrechts von außen nicht wahrnehmbar sind und daher keinen solchen Verdacht

4 § 1 Abs 3 DSG 2000.

auslösen. **Vielmehr kann die DSB eine Datenschutzüberprüfung durchführen, wann immer sie diese für notwendig erachtet.** Eine Öffnungsklausel diesbezüglich gibt es nicht, weshalb der nationale Gesetzgeber die Prüfungsbefugnis der DSB bei Rechtsverletzungen nicht einschränken kann und durch Einführung einer solchen Bestimmung europarechtswidrig handelt.

zu § 11 Abs 5:

Hinsichtlich der Strafbefugnis der DSB ist darauf hinzuweisen, dass diese als Verwaltungsbehörde zu qualifizieren ist und es verfassungsrechtlich äußerst fraglich ist, dass eine solche Behörde, Strafen in der Höhe, wie sie Art 83 DSGVO zulässt, überhaupt aussprechen kann (siehe dazu insbesondere das zu § 99d BWG vor dem VfGH anhängige Verfahren zu den Strafbefugnissen der FMA). Zu überlegen wäre hier die Konstruktion eines (Straf)Antragsrechts der DSB und eine Entscheidungsbefugnis des Bundesverwaltungsgerichts bei Strafen ab einer gewissen Höhe, die die Bagatellgrenze überschreiten.

zu den §§ 13 ff:

Die Beschwerdefrist von einem Jahr nach Kenntnis und insbesondere jene von drei Jahren nach Stattfinden des beschwerenden Ereignisses ist aus praktischer Sicht deutlich zu kurz. Die Regelung ist unsachgemäß, da Datenschutzverletzungen dem Betroffenen – wenn überhaupt – in vielen Fällen erst Jahre später bekannt werden, und es ist zudem nicht ersichtlich, dass die DSGVO dem nationalen Gesetzgeber das Recht einräumt, das Beschwerderecht des Betroffenen auf diese Art zu beschränken.

Es ist nicht ersichtlich, warum gemäß § 13 Abs 5 hinsichtlich einer (berechtigten) Beschwerde an die DSB, diese nur Verantwortlichen aus dem privaten und nicht auch aus dem öffentlichen Bereich auftragen kann (argumentum e contrario), den Anträgen des Beschwerdeführers auf Auskunft, Berichtigung, Löschung und Einschränkung zu entsprechen.

Wie nach bisheriger Rechtslage kann die Datenschutzbehörde nach § 13 Abs 6 Verfahren formlos einstellen, wenn der Beschwerdegegner währen des laufenden Verfahrens die behauptete Rechtsverletzung nachträglich beseitigt. Diese Regelung beschneidet die generalpräventive Wirkung des Datenschutzrechts erheblich, da sie für Verantwortliche einen

Anreiz schafft, so lange gegen das Datenschutzrecht zu verstoßen, bis es zu einem Verfahren kommt.

In den Erläuterungen[5] zu den Übergangsbestimmungen des § 76 heißt es, dass im Falle von Verletzungen von Rechten aus der DSGVO neue Klagen bei den ordentlichen Gerichten ab dem 25. Mai 2018 generell *nicht* mehr eingebracht werden können und stattdessen der Antrag an die DSB zu richten sei. Diese Erklärung ist insoweit irreführend und fragwürdig, als Art 79 DSGVO unmittelbar anwendbar ist und dem Betroffenen nach dieser Bestimmung eine Klagemöglichkeit (gerichtlicher Rechtsbehelf) "unbeschadet" einer Beschwerde bei einer Aufsichtsbehörde eingeräumt wird. Eine Bestimmung im 3. Abschnitt des 2. Hauptstücks (§§ 13 ff) ähnlich § 5 Abs 4 DSG 2000 hinsichtlich einer Klagestellung des Betroffenen für den Rechtsschutz ist dringend erforderlich, und zwar nicht nur für Klagen gegen Verantwortliche aus dem privaten, sondern auch gegen Verantwortliche aus dem öffentlichen Bereich. Art 79 Abs 1 DSGVO macht nämlich deutlich, dass die Mitgliedstaaten ein umfassendes gerichtliches Rechtsschutzsystem für datenschutzrechtliche Rechtsverstöße bereithalten müssen. Nach dem Konzept des Art 79 DSGVO soll ein Betroffener auf zweierlei voneinander unabhängigen Wegen Rechtsschutz suchen können. Einerseits kann er Beschwerde bei der Aufsichtsbehörde (in Österreich die DSB) erheben und diesen Weg gegebenenfalls gerichtlich weiterverfolgen (Art 77 und 78 DSGVO), andererseits kann er sich unabhängig davon *unmittelbar* gerichtlich gegen den Verantwortlichen wenden. **Der Betroffene hat nach der DSGVO ein Recht auf eine Entscheidung in der Sache durch ein staatliches Gericht.** Diese Entkoppelung der Rechtsbehelfe verdeutlicht die herausgehobene Bedeutung, die der Verordnungsgeber dem gerichtlichen Rechtsschutz für die Einhaltung des materiellen Datenschutzrechts beimisst[6]. Die Schlechterstellung aller Betroffenen hinsichtlich des Rechtsschutzes in dieser europarechtswidrigen Art sollte im vorliegenden Entwurf unbedingt noch behoben werden.

5 EB 1664 dB S.29.

6 Vgl. auch Paal/Pauly, Datenschutz-Grundverordnung, 716.

zu § 17 (fehlende abstrakte Bechwerde- bzw. Klagefugnis für bestimmte, nicht auf Gewinnerzielungsabsicht gerichtete Einrichtungen, Organisationen oder Vereinigungen):

Wir begrüßen die Regelung in § 17 des Entwurfs, in dem Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht das Vertretungsrecht eingeräumt wird, regen allerdings dringend die Schaffung einer ergänzenden „abstrakten" Beschwerde- bzw. Klagemöglichkeit durch Inanspruchnahme der Öffnungsklausel des Ar 80 Abs 2 DSGVO aus den nachstehenden Gründen an:

Eine "abstrakte" Beschwerdemöglichkeit bzw. Verbandsklage als Instrument der objektiven Rechtmäßigkeitskontrolle und somit zur Durchsetzung des materiellen Datenschutzrechts würde das angestrebte Ziel der Effektivierung des Datenschutzes besser erreichbar machen. Viele Menschen haben aus diversen Gründen Hemmungen, sich auf behördliche oder gerichtliche Verfahren einzulassen, sei es auch nur als "verletzte Vertretene" im Hintergrund. Durch die Inanspruchnahme der Öffnungsklausel könnten Rechtsverletzungen, insbesondere wenn durch Datenverarbeitungen drittschützende Normen verletzt werden, so z.B. im Falle unvollständiger Datenschutzerklärungen auf Websites oder in Fällen, in denen die Betroffenen ihre Rechte nicht verfolgen (wollen), trotzdem einer Überprüfung unterzogen werden. In den letztgenannten Fällen läge die Hemmschwelle bei Betroffenen zur Rechtsdurchsetzung wesentlich niedriger, wenn diese nicht – vertreten durch die in § 17 genannten Organisationen – ein Verfahren anstrengen müssten, sondern zur Einleitung eines Verfahrens diese Organisationen bloß über Rechtsverletzungen benachrichtigen müssten. Man begibt sich durch Nichtinanspruchnahme der Öffnungsklausel eines effektiven Instruments der Durchsetzung des Datenschutzrechts und läuft Gefahr, die derzeitige Situation der mangelnden Durchsetzung des Datenschutzrechts zu prolongieren.

Zudem würde es ohne eine Inanspruchnahme der Öffnungsklausel zu der Situation kommen, dass z.B. deutsche Verbraucherschutzorganisationen[7] gegen rechtsverletzende österreichische Unternehmen durch eine Klage vor deutschen Gerichten vorgehen können, österreichische Verbraucherschutzorganisationen vor

7 Siehe § 3 deutsches Unterlassungsklagengesetz (UKlaG).

österreichischen Gerichten jedoch nicht. Die sich so ergebende höhere Wahrscheinlichkeit eines ausländischen Gerichtsstandes kann zudem nicht im Interesse der beklagten österreichischen Unternehmen sein.

Eine österreichische Organisation würde in der Praxis auch viel eher, nicht zuletzt aufgrund des wohl bestehenden Informationsvorsprungs, gegen Rechtsverletzungen vorgehen und so zur Effektivierung des Datenschutzes und Sensibilisierung der Unternehmen beitragen.

Die Absurdität der Situation wird besonders deutlich, wenn man sich vor Augen führt, dass ohne eine Inanspruchnahme der Öffnungsklausel nichtösterreichische Organisationen zwar österreichische Unternehmen vor ausländischen Gerichten klagen können, österreichische Organisationen vor österreichischen Gerichten nichtösterreichische Unternehmen (insbesondere internationale Konzerne) jedoch nicht klagen können. **Dies ist besonders unverständlich, wenn man bedenkt, dass die Missachtung des Datenschutzrechts durch nichtösterreichische Konzerne einer der treibenden Kräfte hinter der EU-Datenschutzreform war.**

Der Erfolg der Verbandsklagebefugnis lässt sich insbesondere im Bereich des Konsumentenschutzrechts erkennen. Durch zahlreiche vom Verein für Konsumenteninformation (VKI) oder der Arbeiterkammer (AK) erfolgreich geführte Verfahren wurden diverse Konzerne, insbesondere aus dem Telekommunikations- oder Bankensektor dazu gebracht, bereits im Vorfeld ihre AGBs auf mögliche Rechtsverletzungen zu überprüfen, und Übervorteilungen der Kunden hintangehalten. Wohl kaum jemand in Österreich hält das Erfolgsmodell der Verbandsklage im Konsumentenschutzrecht für überflüssig.

Ein rechtliches Vorgehen gegen Unternehmen, die datenschutzrechtliche Bestimmungen verletzen, sollte auch nicht davon abhängig sein, ob man (zufällig) bereits Geschädigte findet.

Zudem bedarf es auch in § 17 einer Klarstellung, dass den genannten Organisationen auch im Falle einer Vertretung eines verletzten Betroffenen nicht bloß eine Beschwerdebefugnis bei der Datenschutzbehörde, sondern auch ein unmittelbares gerichtliches Klagerecht eingeräumt wird (siehe dazu die Ausführungen zu §§ 13 ff oben).

Vorschlag einer Formulierung des § 17 DSG (2018):

§ 17 (1) Die betroffene Person hat das Recht, eine Einrichtung, Organisation~~en~~[8] oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen, in ihrem Namen die in den §§ 13 bis 16 und Art. 79 DSGVO genannten Rechte wahrzunehmen und das Recht auf Schadenersatz gemäß § 18 in Anspruch zu nehmen.

"§17 (2) Jede der in Absatz 1 genannten Einrichtungen, Organisationen oder Vereinigungen hat unabhängig von einem Auftrag der betroffenen Person das Recht, bei der Datenschutzbehörde eine Beschwerde zu erheben sowie die in den Artikeln 78 und 79 DSGVO aufgeführten Rechte in Anspruch zu nehmen, wenn ihres Erachtens die Rechte einer betroffenen Person gemäß der Datenschutz-Grundverordnung oder des 1. oder 2. Hauptstücks dieses Bundesgesetzes infolge einer Datenverarbeitung verletzt worden sind."

zu § 19:

Es wird dringend angeregt, § 19 des Entwurfs klarer und verständlicher zu formulieren. Dies erscheint nicht zuletzt im Lichte des Bestimmtheitsgebots des Art 18 Abs 1 B-VG geboten. Laut Erkenntnis des VwGH vom 26.3.2004, 2003/02/0202 verlangt „das Bestimmtheitsgebot des Art 18 Abs 1 B-VG für Strafbestimmungen - aus dem Gesichtspunkt des Rechtsschutzbedürfnisses - eine besonders genaue gesetzliche Determinierung des unter Strafe gestellten Verhaltens (vgl hiezu VfSlg 13785/1994). Ferner ist für Strafbestimmungen auf dem Boden des § 1 Abs 1 VStG und des Art 7 MRK der Grundsatz zu beachten, dass eine Tat nur bestraft werden darf, wenn sie gesetzlich vor ihrer Begehung mit Strafe bedroht war, und strafgesetzliche Vorschriften das strafbare Verhalten unmissverständlich und klar erkennen lassen."

Nicht nachvollziehbar ist auch, dass Abs 1 (Rechtsverletzungen durch Handeln von entscheidungsbefugten Personen) immer anwendbar ist, aber Abs 2 (Rechtsverletzungen aufgrund mangelnder Überwachung und Kontrolle) nur subsidiär[9] anwendbar ist.

8 Richtig muss es lauten "Organisation" (Redaktionsversehen im Entwurf).

9 "..., sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet."

Im Sinne der Rechtssicherheit bedarf es einer Klarstellung, dass Datenschutzbeauftragte nicht als Verantwortliche gem. § 9 VStG gelten und dass diese nicht den Strafbestimmungen der DSGVO bzw. des DSG (2018) unterliegen, da dies angesichts des in der DSGVO für den Datenschutzbeauftragten vorgesehenen Rollenverständnisses nicht sachgerecht wäre.

Zudem wäre im Sinne der Rechtssicherheit eine Legaldefinition des Begriffs "öffentlichen Stellen" erforderlich.

zu § 29:

Im Hinblick auf das verfassungsrechtliche Determinierungsgebot gem Art 18 B-VG erscheint ein bloß pauschaler Verweis auf das Arbeitsverfassungsgesetz (ArbVG) mehr als bedenklich.

zu §§ 30 ff (Bildverarbeitung):

Zunächst ist darauf hinzuweisen, dass es höchst fraglich ist, ob und wenn ja auf welcher Grundlage in der DSGVO die Bildverarbeitung im privaten Bereich einer nationalstaatlichen Regelung überhaupt zugänglich ist. Eine Öffnungsklausel, die dem nationalen Gesetzgeber erlaubt, zusätzliche Bedingungen und Beschränkungen der Verarbeitung personenbezogener Daten zu normieren, findet sich allenfalls in Art 9 Abs 4 DSGVO für den Bereich der Verarbeitung bestimmter besonderer Kategorien personenbezogener Daten ("sensible Daten"), und zwar für genetische, biometrische und Gesundheitsdaten. Dazu müsste man aber personenbezogene Bilddaten per se als "sensible" Daten einordnen (hier: biometrische oder Gesundheitsdaten). Diese Frage ist aber nicht abschließend geklärt[10]. In diesem Fall müssten sich zudem die Zulässigkeitskriterien der Verarbeitung dieser Daten (siehe § 30 Abs 2) am wesentlich strengeren Maßstab des Art 9 DSGVO orientieren.

§ 30 Abs 3 Z 1 ist zu eng gefasst. Die Regelung, dass die Bildverarbeitung in diesem Fall nur zulässig ist, wenn die private Liegenschaft *ausschließlich* vom Verantwortlichen genutzt wird, ist praxisfern und sollte auf dessen Familienangehörige oder Mitbewohner ausgedehnt werden. Allerdings ist zu bezweifeln, dass die genannte Bestimmung überhaupt erforderlich ist, da gem. Art 2 Abs 2 lit c DSGVO die Verarbeitung personenbezogener Daten durch

10 Siehe dazu ausführlich *Knyrim*, Bilddaten: immer sensibel?, jusIT2016/102, 235 und *Bergauer*, Die Einordnung von Bilddaten erkennbarer Personen im Datenschutzrecht. Eine Replik auf Knyrim, Bilddaten: immer sensibel?, jusIT2016/102, 235, jusIT2016/103.

natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vom Anwendungsbereich der Datenschutz-Grundverordnung überhaupt ausgenommen ist.

Die in § 31 normierte Ermächtigung, personenbezogene Bilddaten "im erfoderlichen Ausmaß" zu übermitteln erscheint im Hinblick auf das Bestimmtheitsgebot des Art 18 B-VG und die verfassungsgerichtliche Judikatur zu Eingriffen in das Grundrecht auf Datenschutz äußerst problematisch.

Die Ausnahme der Kennzeichnungspflicht von Bildaufnahmen für Zwecke der privaten verdeckten Ermittlung und somit die Ermöglichung derselben ist aufgrund des hohen Missbrauchspotentials, vor allem in Zeiten der starken Nutzung von Social Media und den schnellen Verbreitungsmöglichkeiten digitaler Inhalte, strikt abzulehnen.

zum 3. Hauptstück (§§ 34 ff):

Das 3. Hauptstück dieses Bundesgesetzes setzt die RL (EU)2016/680 um und regelt die Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei, des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs. Die einschlägigen materienspezifischen Regelungen zu Datenverarbeitungen (insb im SPG, PStSG, MBG und der StPO) gehen den allgemeinen Regelungen dieses Hauptstück als leges speciales vor. Diesbezüglich ist darauf hinzuweisen, dass derzeit hinsichtlich der Verfassungskonformität bestimmter Regelungen zur Datenverarbeitung in der SPG-Novelle 2008 ein Verfahren beim EGMR sowie hinsichtlich zahlreicher Bestimmungen im PStSG beim VfGH anhängig ist[11].

zu § 34:

Der sachliche Anwendungsbereich wurde gegenüber der RL (EU)2016/680 insofern erweitert, als die (Umsetzungs)Bestimmungen des 3. Hauptstücks auch für die Verarbeitung personenbezogener Daten durch die "zuständige Behörde" für Zwecke der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung gelten. Insofern ist es nicht ersichtlich, warum die Definition der "zuständigen Behörde" in § 35 Z 7 wortgleich aus der Richtlinie übernommen wurde und nicht um die genannten Tatbestandselemente erweitert wurde. Sofern keine materienspezifischen Regelungen bestehen, **kommt es somit**

11 In beiden Verfahren ist mit einer Entscheidung noch im Jahr 2017 zu rechnen (EGMR Nr. 3599/10 und VfGH G223/2016).

zu der Situation, dass es gar keine "zuständige Behörde" für die Verarbeitung personenbezogener Daten zu Zwecken der nationalen Sicherheit, des Nachrichtendienstes oder der militärischen Eigensicherung gibt und die tatsächlich datenverarbeitende Behörde personenbezogene Daten ohne Rechtsgrundlage verarbeitet.

Auch wenn es sich im Falle des § 34 um eine Umsetzungsbestimmung der RL (EU)2016/680 handelt, wären im Hinblick auf das verfassungsrechtliche Determinierungsgebot gem Art 18 B-VG Legaldefinitionen der Begriffe "öffentliche Sicherheit" und "nationale Sicherheit" vorzunehmen. Die Problematik solcher unscharfen und weiten Begriffe wird insbesondere bei der Versagung oder Aufschiebung der Informationspflichten nach dem PStSG (§ 26 Abs 2 DSG 2000) sichtbar.

zu § 37:

In § 37 werden die Art 6 und 7 der RL (EU)2016/680 umgesetzt. Im Hinblick auf das verfassungsrechtliche Determinierungsgebot und die verfassungsgerichtliche Judikatur zu eingriffsnahen Gesetzen sollte jedoch die Wendung "soweit möglich", auch wenn sie in der Richtlinie vorkommt, im österreichischen Umsetzungsgesetz überhaupt nicht verwendet werden. Insbesondere in § 37 Abs 1 ist die Wendung entbehrlich, da eine Einordnung in die Kategorie "sonstige Personen" gem. Z 5 leg cit aufgrund des demonstrativen Charakters der Norm immer möglich ist, sollte eine Einordnung in die Kategorien der Z 1 bis 4 nicht möglich sein.

zu § 43:

Wie oben schon zu § 34 erwähnt handelt es sich bei dem Begriff der "nationalen Sicherheit" um einen äußerst weiten und unbestimmten Begriff, der einer Legaldefinition bedarf. Durch Berufung auf den Schutz der nationalen Sicherheit kann - nach dem vorliegenden Entwurf - eine Information der betroffenen Person über die Verarbeitung personenbezogener Daten wohl immer unterbleiben (insbesondere im Fall einer Verarbeitung personenbezogener Daten aufgrund geheimer Ermittlungsmaßnahmen).

III. Conclusio

A. Rechtspolitische Überlegungen

Insgesamt ist zu erkennen, dass im Entwurf des Datenschutz-Anpassungsgesetzes 2018 viele Bestimmungen unklar geregelt sind und Fragen offen lassen sowie zahlreiche Interpretationsspielräume zulassen. Dieser Umstand ist der Rechtssicherheit nicht zuträglich. **Wir empfehlen eine eingehende Überarbeitung des vorliegenden Entwurfs, insbesondere im Hinblick darauf, dass hier eine äußerst grundrechtssensible Materie normiert wird.**

Die Beschlussfassung als Regierungsvorlage während offener Begutachtungsfrist ist demokratiepolitisch höchst bedenklich. Eine solche Vorgehensweise ist abzulehnen und keinesfalls zu wiederholen. Zudem hatte die Bundesregierung seit Verabschiedung der Datenschutz-Grundverordnung ausreichend Zeit, ein Anpassungsgesetz vorzulegen.

Sollte die Öffnungsklausel des Art 80 Abs 2 DSGVO (Möglichkeit einer abstrakten Beschwerdebefugnis bzw. Verbandsklage (siehe oben zu § 17 DS-AnpG 2018) zum jetzigen Zeitpunkt nicht in Anspruch genommen werden, wäre die nachträgliche Einführung jedenfalls auch im Zuge einer verpflichtenden Evaluierung des DSG (2018) gem § 1 Abs 5 Deregulierungsgrundsätzegesetz[12] zu prüfen.

B. Fehlende Wirkungsfolgenabschätzung

Auf den ersten Blick erscheint es erfreulich, dass dem Gesetzesvorschlag eine „wirkungsorientierte Folgenabschätzung“ (WFA) zugrunde liegt. Bei Betrachtung des Inhalts der WFA zeigt sich jedoch, dass sich diese darauf beschränkt, die Folgen für den Bundeshaushalt zu beschreiben. Eine Folgenabschätzung im Hinblick auf die erwarteten Auswirkungen auf das Grundrecht des Schutzes personenbezogener Daten der in Österreich lebenden Menschen fehlt ebenso wie eine gesellschafts- und demokratiepolitische Diskussion obwohl es sich um eine grundrechtssensible Materie handelt.

12 Bundesgesetz über die Grundsätze der Deregulierung.