WIRTSCHAFTSKAMMER ÖSTERREICH

Bundeskanzleramt
Verfassungsdienst
Ballhausplatz 2
1014 Wien

e-mail: v@bka.gv.at

Wiedner Hauptstrasse 63 | Postfach 195
1045 Wien
T +43 (0)5 90 900-DW | F +43 (0)5 90 900-243
E rp@wko.at
W http://news.wko.at/rp

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sachbearbeiter	Durchwahl	Datum
	Rp 1759/17/Ro/MH	3215	22.06.2017

Entwurf eines Bundesgesetzes, mit dem das Bundes-Verfassungsgesetz geändert, das Datenschutzgesetz erlassen und das Datenschutzgesetz 2000 aufgehoben wird (Datenschutz-Anpassungsgesetz 2018); Stellungnahme

Sehr geehrte Damen und Herren!

Die Wirtschaftskammer Österreich teilt zu dem im Betreff genannten Entwurf Folgendes mit:

I. Allgemeine Bemerkungen

Die EU-Datenschutz-Grundverordnung (DSGVO), die am 25.5.2018 in Geltung tritt, ist zwar als EU-Verordnung grundsätzlich unmittelbar anwendbar, enthält jedoch etliche Regelungsspielräume und Öffnungsklauseln, die fakultativ von den Mitgliedstaaten genutzt werden können. Die Durchführung der DSGVO soll in Österreich hinsichtlich der allgemeinen Angelegenheiten des Datenschutzes durch das gegenständliche „Datenschutz-Anpassungsgesetz 2018“, speziell durch das erste, zweite, vierte und fünfte Hauptstück des darin enthaltenen neuen Datenschutzgesetzes (DSG) erfolgen.

Gleichzeitig mit der DSGVO wurde auch die Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung beschlossen. Diese Richtlinie muss in innerstaatliches Recht umgesetzt werden, was durch das dritte Hauptstück des neuen DSG erfolgen soll.

Die Datenschutz-Grundverordnung (DSGVO) ist ab 25. Mai 2018 in Geltung, die Anpassungsfrist ist somit sehr kurz und eine Herausforderung für die österreichischen Unternehmen.
Eine möglichst rasche, zeitnahe Beschlussfassung ist daher unbedingt erforderlich um Rechtssicherheit zu schaffen, damit die österreichischen Betriebe neben den unmittelbar anwendbaren Regeln der DSGVO auch die österreichischen Ausführungs- und Durchführungsbestimmungen mit ausreichender Vorbereitungszeit implementieren können. Dies gilt auch für die Erlassung von Verordnungen nach dem neuen DSG, insbesondere die Kundmachung der Listen betreffend die Datenschutz-Folgenabschätzung („Black-“ und „Whitelists“).

Die folgenden Ausführungen konzentrieren sich auf das erste, zweite, vierte und fünfte Hauptstück des neuen DSG (Artikel 2).
Im dritten Hauptstück sind zumindest zwei Dinge positiv anzumerken, einerseits § 35 Z 8 („8. *„Verantwortlicher" die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;*") bzw Z 9 („*9. „Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;*") welche eine eindeutige Definition von Verantwortlichen und Auftragsverarbeitern enthalten und andererseits § 43 Abs 4, nach welchem die die Unterrichtung der betroffenen Person unterbleiben kann, soweit und solange dies im Einzelfall unbedingt erforderlich und verhältnismäßig ist.

II. Zu den einzelnen Bestimmungen in Artikel 2 (Datenschutzgesetz-DSG)

Zu § 1 (Grundrecht auf Datenschutz):

Zu Abs 1:
§ 1 DSG enthält wie der bisherige § 1 DSG 2000 eine Verfassungsbestimmung zur konkreteren Ausgestaltung des Grundrechts auf Datenschutz. Art 8 der Europäischen Grundrechtecharta (Charta), Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) sowie Art 8 der Menschenrechtskonvention (EMRK) geben hier im Wesentlichen die Marschrichtung vor. Die nun vorliegende Formulierung des § 1 DSG enthält allerdings einige Widersprüche, auch zur DSGVO. § 1 Abs 1 DSG besagt, dass jede natürliche Person Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten, auf Auskunft über die Verarbeitung solcher Daten sowie auf Richtigstellung unrichtiger Daten und auf Löschung unzulässigerweise verarbeiteter Daten hat. Das Recht auf Löschung stellt ein Betroffenenrecht nach der DSGVO dar, hat jedoch keine grundrechtliche Rechtfertigung in den oben genannten Grundlagen. Hier wurde offenbar lediglich der Text des bisherigen § 1 Abs 3 DSG 2000 übernommen, was allerdings im neuen System einen Widerspruch (gold plating) darstellen würde und daher abzulehnen ist.

Zu Abs 2:
Gem Art 6 Abs. 1 lit f DSGVO ist ein Grund für die Rechtmäßigkeit der Verarbeitung: „die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eine Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen...".
Die Grundrechtsbestimmung des § 1 sieht - wie bisher - vor, dass Beschränkungen u.a. „im überwiegenden berechtigten Interesse eines anderen" zulässig sind. Damit müsste nach wie vor der Verantwortliche sein überwiegendes berechtigtes Interesse darlegen - und nicht, wie nach DSGVO, die betroffene Person, dass ihre Interessen überwiegen. Insofern widerspricht diese Regelung der DSGVO.

Weiters werden nicht sämtliche Erlaubnistatbestände des Art 6 Abs 1 DSGVO genannt; etwa wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen.

Für eine generelle „*Vorhersehbarkeit*" der Beschränkungen, wie sie in § 1 Abs 2 definiert ist („*Diese Beschränkungen müssen notwendig und verhältnismäßig und, insbesondere im Hinblick auf den Zweck, die verarbeiteten Daten und die Art der Verarbeitung, für die betroffene Person vorhersehbar sein.")*, besteht ebenso wenig eine Grundlage in der DSGVO wie in der Grundrechtecharta.

Von der Unvereinbarkeit mit der DSGVO abgesehen, wären mit einer derartigen Regelung sämtliche Möglichkeiten der Verarbeitung von „big data" obsolet. Eine (abschließende)

Definition des Grundrechts auf Datenschutz ist bereits in der DSGVO enthalten (EG 1), welcher direkt auf Art 8 Abs 1 der Charta der Grundrechte der Europäischen Union und Art 16 Abs 1 des Vertrags über die Arbeitsweise der Europäischen Union verweist. Es besteht daher auch objektiv keine Notwendigkeit für eine weitere (abweichende) Regelung im DSG. Wir sprechen uns daher für eine ersatzlose Streichung des § 1 DSG aus.

Beschränkungen des Grundrechts auf Datenschutz sind nach der vorliegenden Fassung des § 1 unter anderem aufgrund einer gesetzlichen Grundlage zulässig. In den Erläuterungen sollte klargestellt werden, ob/inwieweit darunter auch Verordnungen, Bescheide etc. zu subsumieren sind oder tatsächlich nur Gesetze im formellen Sinn erfasst werden sollen.

Nach § 1 Abs 3 DSG gilt das Grundrecht auf Datenschutz auch gegenüber *„Privaten"*. Weder dem Gesetzestext des DSG noch den Erläuterungen ist eine Definition des Begriffs des „Privaten" zu entnehmen.

Die Aufzählung der Beschränkungen des Grundrechts auf Datenschutz ist, wie oben ausgeführt, insofern irreführend, da einerseits Art. 6 Abs. 1 lit b der DSGVO - im Konkreten die Durchführung vorvertraglicher Maßnahmen bzw. Vertragserfüllung - nicht erwähnt wird. Andererseits wird im vorliegenden Fall die Wahrnehmung einer Aufgabe, welche im öffentlichen Interesse liegt, an das Bestehen einer gesetzlichen Grundlage gekoppelt. Im Ergebnis stellt dies eine kumulative Voraussetzung dar, welche im Vergleich zur DSGVO überschießend ist. Es wäre daher - sollte § 1 beibehalten werden - geboten, die Gründe für eine rechtmäßige Verarbeitung taxativ - entsprechend der DSGVO - anzuführen.

Als Beispiel für die Wahrnehmung einer Aufgabe, welche dem öffentlichen Interesse dient, wird die Datenverarbeitung in Pharmakovigilanzprozessen herangezogen, welche der Sicherstellung und Überwachung der Gesundheit dient. Durch bereits bestehende spezifische Arzneimittel Vorgaben sind pharmazeutische Unternehmer dazu verpflichtet, ihre am Markt befindlichen pharmazeutischen Produkte genau zu überwachen und im Falle des Auftretens von Nebenwirkungen diese zu dokumentieren sowie die entsprechenden Meldungen an die zuständigen Behörden weiterzuleiten (Pharmakovigilanz). Grundlage dieser Nebenwirkungsmeldung sind personenbezogene Daten der betroffenen Patienten und der meldenden Personen (z.B. Ärzte oder Apotheker). Auf Grundlage des noch geltenden Datenschutzrechts kann häufig allein über eine Einwilligungserklärung der betroffenen Personen die Verarbeitung datenschutzkonform durchgeführt werden. Dies ist praxisfern, da in diesem Fall das Patientenwohl und die Arzneimittelsicherheit in erster Linie im Fokus stehen müssen. Die Erhebung von personenbezogenen Daten könnte jedoch als Widerspruch zu dem in den Erläuterungen erwähnten Grundsatz der Datenminimierung gesehen werden und führte bereits in der Vergangenheit zu Rechtsunsicherheiten.

Es wäre daher zielführend in den Erläuterungen sowie in den entsprechenden Materiengesetzen klarzustellen, dass eben diese Datenverarbeitung als Eingriff im öffentlichen Interesse - zur Gewähr einer qualitativ hohen Arzneimittelsicherheit und zur Vermeidung von Mehrfachmeldungen ein und desselben Nebenwirkungsfalles - gerechtfertigt werden kann.

Aus dem Blickpunkt der wissenschaftlichen Forschung wird auf Folgendes hingewiesen:
Der Datenschutz ist für die forschenden Firmen vor allem hinsichtlich der Zusammenarbeit mit Forschungseinrichtungen von besonderer Bedeutung.
Da der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten oft nicht vollständig angegeben werden kann, sollte es betroffenen Personen entsprechend dem Erwägungsgrund 33 der DSGVO erlaubt sein, ihre Einwilligung für bestimmte Bereiche oder Teile von Forschungsprojekten wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung

geschieht. Speziell auch in diesem Zusammenhang ist die, oben angesprochene, in § 1 Abs. 2 normierte „Vorhersehbarkeit" für die betroffene Person abzulehnen.

Zur Zweckangabe in der Einwilligung im Forschungskontext („broad consent"):
Nach der derzeitigen Rechtslage liegt eine rechtsgültige Zustimmungserklärung in die Datenverwendung ua nur dann vor, wenn darin (im Vorhinein) der konkrete Verwendungszweck angegeben wird.[1] *„Oft lässt sich jedoch bei neuen Forschungsprojekten die genaue Zielsetzung nicht von vornherein festlegen und/oder Daten werden in großem Umfang, etwa in Biobanken, gesammelt, um diese für künftige Studien vorzuhalten."*[2] Der in EG 33[3] der DSGVO im Kontext der wissenschaftlichen Forschung erwähnte sog „broad consent" (breit formulierte Einwilligungserklärung) ist daher in der Praxis von großer Bedeutung und sollte angesichts der in Österreich bislang vorherrschenden Judikatur jedenfalls in das neue DSG ausdrücklich aufgenommen werden, wobei in zukünftigen Einwilligungserklärungen natürlich nicht auf ein gewisses Maß an Zweckbestimmtheit verzichtet werden kann.

Wie diesbezüglich die Wendung zur „Vorhersehbarkeit" in § 1 Abs 2 zweiter Satz DSG (Verfassungsbestimmung) zu verstehen ist, bleibt offen. Insbesondere vor dem Hintergrund, dass bereits in Art 5 Abs 1 DSGVO die Grundsätze für die Verarbeitung personenbezogener Daten ausreichend prädeterminiert sind, handelt es sich nicht um eine „unbedingt erforderliche Regelung im innerstaatlichen Recht" im Sinne der Erläuterungen - Allgemeiner Teil. Zumindest sollte jedoch die Zulässigkeit eines „broad consent" für die Datenverarbeitung in der wissenschaftlichen Forschung ausdrücklich (zB in die Erläuterungen) aufgenommen werden.[4]

Zu § 3 (Durchführungsbestimmungen):

Im deutschen BDSG-Neu idF des Datenschutz-Anpassungs- und -Umsetzungsgesetzes-EU (DSAnpUG-EU) wurden die Öffnungsklauseln der DSGVO dazu genutzt, um Datenschutzbestimmungen sinnvoll und angemessen einzuschränken.

Dies ist insbesondere zu den Betroffenenrechten anzumerken, zu denen §§ 32 ff BDSG-neu beispielsweise folgende Beschränkungen vorgesehen, deren Verankerung auch im DSG umgesetzt werden sollte:

- Das Informationsrecht ist u.a. eingeschränkt, wenn dadurch die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen beeinträchtigt oder die vertrauliche Mitteilung an öffentliche Stellen gefährdet wäre.
- Das Auskunftsrecht ist eingeschränkt, wenn die Datenspeicherung nur zur Erfüllung von Aufbewahrungsvorschriften oder zur Datensicherung oder Datenschutzkontrolle erfolgt.
- Die Löschungspflicht ist eingeschränkt, wenn die Löschung nur mit unverhältnismäßigem Aufwand möglich wäre und das Interesse des Betroffenen als gering anzusehen ist.

---

[1] Vgl die ständige Judikatur des OGH, RIS-Justiz RS RS0115216: *„Eine wirksame Zustimmung zur Verwendung nichtsensibler Daten liegt nur vor, wenn der Betroffene weiß, welche seiner Daten zu welchem Zweck verwendet werden."*
[2] So zutreffend *Buchner/Kühling* in *Kühling/Buchner* (Hrsg), Datenschutz-Grundverordnung (2017) Art 7 Rz 64.
[3] *„Oftmals kann der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden. Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen."*
[4] *„Diese Beschränkungen müssen notwendig und verhältnismäßig und, insbesondere im Hinblick auf den Zweck, die verarbeiteten Daten und die Art der Verarbeitung, für die betroffene Person vorhersehbar sein."*

Hinsichtlich der Berichtigungs- und Löschungspflichten sollte in § 3 - angelehnt an § 35 Abs 1 des deutschen BDSG-Neu – folgende *"Durchführungsregelung"* ergänzt werden:

"Ist eine Löschung im Falle nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten gemäß Artikel 17 Absatz 1 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679. Die Sätze 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden."

Zumindest wird in Nutzung der Öffnungsklausel nach Art 23 DSGVO vorgeschlagen, die bisher schon ausdrücklich genannten Ausnahmen in das DSG aufzunehmen, sofern nicht bereits durch die DSGVO selbst abgedeckt:
Das wäre für das **Auskunftsrecht** (Art 15 DSGVO) der Text des § 26 Abs 2 DSG 2000. Der Verantwortliche hätte sonst etwa im Falle eines anhängigen Rechtsstreits keine Möglichkeit, den Auskunftsantrag der betroffenen Person abzulehnen (wie etwa in BVwG 22. 2. 2017, W214 2132040-1).
Für die Rechte auf **Berichtigung** (Art 16 DSGVO) und **Löschungsrecht** (Art 17 DSGVO) würde sich die Übernahme von § 27 Abs 3 DSG 2000 anbieten.

Zu § 4 (Gemeinsame Bestimmungen zu den Datenschutzbeauftragten):

Nach den Erläuterungen zu § 4 DSG (letzter Satz) soll die Verschwiegenheitspflicht des Datenschutzbeauftragten nicht gegenüber der Datenschutzbehörde gelten. Dessen ungeachtet gilt trotzdem das **Bankgeheimnis**, das nicht durch einen Satz in den Erläuterungen aufgehoben werden kann. Die Geltung des Bankgeheimnisses gegenüber der Datenschutzbehörde sollte in den Erläuterungen zu § 4 klargestellt werden.

Begrüßt wird die Bestimmung, dass der Datenschutzbeauftragte ein Aussageverweigerungsrecht gem § 4 Abs 2 besitzt.
Allerdings wird in § 4 Abs 2 festgehalten, dass dem Datenschutzbeauftragen nur dann ein Aussageverweigerungsrecht zustehen soll, wenn Personen der Stelle, für die er tätig ist, ein solches bereits in Anspruch genommen haben. Das ist insofern nicht praxisgerecht, weil dem Datenschutzbeauftragten in der Praxis der Umfang dieses Rechtes nicht genau bekannt sein wird und dem Datenschutzbeauftragten aus Anlass seiner Befragung auch die Information, ob eine solche Inanspruchnahme bereits erfolgt ist (oder möglicherweise erst erfolgen wird), nicht bekannt sein wird.
Es wird daher empfohlen, über den Rahmen der Inanspruchnahme den eigentlichen Geheimnisträger entscheiden zu lassen und den zweiten Satz wie folgt zu formulieren:
Erhält ein Datenschutzbeauftragter bei seiner Tätigkeit Kenntnis von Daten, für die einer der Kontrolle des Datenschutzbeauftragten unterliegenden Stelle beschäftigten Person ein gesetzliches Aussageverweigerungsrecht zusteht, steht dieses Recht auch dem Datenschutzbeauftragten und den für ihn tätigen Personen insoweit zu, als die Person, der das gesetzliche Aussageverweigerungsrecht zusteht, den Datenschutzbeauftragten nicht von seiner Geheimhaltungsverpflichtung entbunden hat.

Zu § 5 (Datenschutzbeauftragter im öffentlichen Bereich):

Die Erläuterungen erklären die Sonderbestimmungen nur auf Verantwortliche des öffentlichen Bereichs iSd § 15 Abs 1 Z 1 DSG anwendbar. Das wäre in § 5 Abs 1 ausdrücklich zu regeln.

Begrüßt wird die Klarstellung, dass der Datenschutzbeauftragte im öffentlichen Bereich hinsichtlich der Ausübung seiner Aufgaben weisungsfrei ist.
Es sollte ausdrücklich klargestellt werden, dass diese Weisungsfreiheit im Umfang des Art 38 Abs 3 DSGVO auch für Datenschutzbeauftragte des privaten Bereiches gilt.

Datenschutzbeauftragte im öffentlichen Bereich müssen nach der Bestimmung des § 5 Abs 2 DSG auch diesem Bereich angehören. Die Zuziehung externer Datenschutzbeauftragte ist in den Erläuterungen zu § 5 Abs 2 ausdrücklich ausgeschlossen. Das ist uE nicht zu akzeptieren und widerspricht klar der DSGVO.

Zu § 9 (Leiter der Datenschutzbehörde):

§ 9 Abs 2 Z 1 DSG ist uE zu kurzsichtig gefasst, da es mittlerweile auch andere gleichwertige juristische Ausbildungen gibt (zB Wirtschaftsrechtsstudien an der WU Wien).

Z 1 ist daher zu ergänzen um: *„oder vergleichbare Studienrichtungen, die den hierfür erforderlichen Ansprüchen genügen"*.

Zu § 10 (Aufgaben der Datenschutzbehörde):

Zu Abs 2:
Gemäß Art 35 Abs 4 DSGVO erstellt die Aufsichtsbehörde eine Liste der Verarbeitungsvorgänge für die eine Datenschutzfolgenabschätzung durchzuführen ist und veröffentlicht diese. Gemäß Art 35 Abs 5 DSGVO kann die Aufsichtsbehörde eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für welche keine Datenschutz-Folgenabschätzung notwendig ist. Diesbezüglich legt § 10 Abs 2 DSG folgendes fest: *„Die Datenschutzbehörde hat die Listen nach Art 35 Abs 4 und 5 DSGVO im Wege einer Verordnung kundzumachen."*
Es wird begrüßt, dass diese Listen in Form einer Verordnung zu erlassen sind.

In Anbetracht der Tatsache, dass etwa bezüglich des gerade nicht unter Art 22 DSGVO fallenden „Profilings" für Marketingzwecke/ Direktwerbung/ Einordnung in Marketing-Zielgruppen, offenbar Unklarheiten bestehen, ist die Erlassung und Kundmachung einer White-List aus Gründen der Rechtssicherheit dringend erforderlich und sollte nicht im Ermessen der Datenschutzbehörde liegen.

Bereits bisher konnten nur jene Typen von Datenanwendungen und Übermittlungen aus diesen zu Standardanwendungen erklärt werden, bei denen angesichts des Verwendungszwecks und der verarbeiteten Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich war. Die Datenschutzbehörde sollte daher jedenfalls unter Heranziehung der Standard- und Musterverordnung die bisherigen Standardanwendungen von der Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung ausnehmen.

Die genannten Listen sind für die korrekte Umsetzung der DSGVO durch die Verantwortlichen von enormer Bedeutung, weswegen die Kundmachung des Datenschutz-Anpassungsgesetzes 2018 und in weiterer Folge der Erlass der oben erwähnten Verordnungen so rasch wie möglich erfolgen sollten, damit diese Verordnungen rechtzeitig Berücksichtigung finden können.

Zu Abs 3:
In Abs 3 wird ausgewiesen, dass die Datenschutzbehörde gleichzeitig auch als einzige nationale Akkreditierungsstelle gem Art 43 Abs 1 lit a DSGVO fungieren soll. Nach Ansicht der WKÖ sollte weiterhin auch die Akkreditierungsstelle des BMWFW als solche agieren können.

Weiters sollte die Behörde zur Stärkung der Rechtsicherheit und Hintanhaltung existenzgefährdender Strafverfahren auch einer Verpflichtung zur Beratung von Unternehmen und Bürgern unterliegen, dies entsprechend dem Forderungsmodell „Beraten statt Strafen". Auch Art 57 Abs 1 lit v DSGVO besagt, dass die Aufsichtsbehörde *„jede sonstige Aufgabe im Zusammenhang mit dem Schutz personenbezogener Daten erfüllen muss".*

Zu § 11 (Befugnisse der Datenschutzbehörde):

Zu Abs 4:
Grundsätzlich sollte die Untersagung der Weiterführung von Datenverarbeitungen (wie in § 11 Abs 4 DSG vorgesehen) die ultima ratio darstellen. Der Verantwortliche und ein allfälliger Auftragsverarbeiter, gegen den sich die nachteilige Maßnahme richtet, sind entsprechend EG 129 der DSGVO vorher zu hören. So kann sichergestellt werden, dass die Interessen der Beteiligten abgewogen werden und im Ergebnis die beabsichtigte Maßnahme verhältnismäßig ist. Es ist auch erforderlich sicherzustellen, dass solche Maßnahmen nur bei einem **offenkundigen wesentlichen unmittelbaren Risiko** für die Rechte und Freiheiten der betroffenen Personen erfolgen. Diese Forderungen sollten zum Schutze der Verantwortlichen und allfälliger Auftragsverarbeiter berücksichtigt werden und könnten wie untenstehend statuiert werden:

*„(4) Liegt durch den Betrieb einer Datenverarbeitung ein **offenkundiges** wesentliches unmittelbares **Risiko für die Rechte und Freiheiten** der betroffenen Personen (Gefahr im Verzug) vor, so kann die Datenschutzbehörde die Weiterführung der Datenverarbeitung mit Bescheid gemäß § 57 Abs. 1 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 - AVG, BGBl. Nr. 51/1991, untersagen. **Dabei dürfen nur die unter Berücksichtigung der Umstände des jeweiligen Einzelfalls und unter Abwägung der berührten Interessen erforderlichen und verhältnismäßigen Maßnahmen ergriffen werden; außerdem ist der Verantwortliche und ein allfälliger Auftragsverarbeiter, gegen den sich die nachteilige Maßnahme richtet, vorher zu hören und sind ihm gegenüber überflüssige Kosten und übermäßige Unannehmlichkeiten zu vermeiden.** Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenverarbeitung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Ebenso kann die Datenschutzbehörde auf Antrag einer betroffenen Person eine Einschränkung der Verarbeitung nach Art. 18 DSGVO mit Bescheid gemäß § 57 Abs. 1 AVG anordnen, wenn der Verantwortliche einer diesbezüglichen Verpflichtung nicht fristgerecht nachkommt. Wird einer Untersagung nicht unverzüglich Folge geleistet, hat die Datenschutzbehörde nach Art. 83 Abs. 5 DSGVO vorzugehen.*

Erläuterungen zu § 11 Abs 4:
*Ebenfalls aus dem DSG 2000 (§ 30 Abs. 6a) übernommen werden soll in Abs. 4 die Möglichkeit bei Gefahr im Verzug, die Weiterführung der Datenverarbeitung mit Bescheid gemäß § 57 Abs. 1 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 - AVG, BGBl. Nr. 51, untersagen zu können. **Durch das Wort offenkundig und das Vorliegen von Gefahr in Verzug nur bei einem Risiko für die Rechte und Freiheiten der betroffenen Person wird klargestellt, dass solche Maßnahmen wegen Gefahr in Verzug nur dann in Betracht kommen, wenn im Sinne der Definition gemäß dem 75. Erwägungsgrund der DSGVO tatsächlich ein Schaden droht, und nicht schon dann zulässig sind, wenn lediglich eine unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen der betroffenen Personen als Ergebnis einer Interessenabwägung angenommen wird. Im Hinblick auf den 129. Erwägungsgrund der DSGVO sollen nur geeignete, erforderliche und verhältnismäßige Maßnahmen getroffen werden dürfen, welche keine überflüssigen Kosten und übermäßigen Unannehmlichkeiten für die durch solche Maßnahmen Verpflichteten verursachen sollen; außerdem ist im Sinne des 129. Erwägungsgrundes***

die vorherige Anhörung des Betroffenen vorgesehen. Das Gebot, in diesem Zusammenhang auch die berührten Interessen abzuwägen, ist Ausfluss des Verhältnismäßigkeitsprinzips (im engeren Sinn). Hierdurch wird nochmals bekräftigt, was sich bereits aus dem Einleitungssatz der Bestimmung, wonach nur eine offenkundige wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen zu vorläufigen Maßnahmen berechtigt ergibt: Je weniger intensiv der Eingriff in die schutzwürdigen Geheimhaltungsinteressen der betroffenen Personen ist, umso weniger schwerwiegend dürfen die Auswirkungen der vorläufigen Maßnahme für den hierdurch Verpflichteten sein. Diese Maßnahme sollte nur iSd DSGVO nach einer vorangegangenen Interessensabwägung und als ultima ratio erfolgen. […]"

Zu Abs 5:
§ 11 Abs 5, der die Datenschutzbehörde zur Verhängung von Geldbußen ermächtigt, die nach Art 83 Abs 5 und 6 DSGVO bis zu 4% des weltweiten Jahresumsatzes bzw EUR 20 Mio betragen können, ist uE verfassungsrechtlich bedenklich, weil nach der bisherigen Judikatur des Verfassungsgerichtshofs die Verhängung von besonders hohen Geldstrafen Gerichten vorbehalten ist.
Derzeit ist genau zu dieser Frage ein Verfahren zu § 99d BWG vor dem Verfassungsgerichtshof anhängig. Kurz zusammengefasst ergeben sich die Überlegungen zur Verfassungswidrigkeit einerseits aus der Spruchpraxis des Verfassungsgerichtshofes, der zufolge die Verhängung hoher Geldstrafen der ordentlichen Gerichtsbarkeit vorbehalten ist, andererseits aus dem Grundsatz, dass, soweit das Unionsrecht den Mitgliedstaaten bei seiner Vollziehung einen Spielraum einräumt, der Gesetzgeber nach der Judikatur des VfGH nicht nur an die Vorgaben des Unionsrechts, sondern auch an jene der österreichischen Verfassung gebunden ist, was in der Lehre als "doppelte Bindung" des Gesetzgebers bezeichnet wird (vgl dazu z.B. den Gesetzesprüfungsantrag des BVwG zu W210 - 213108). Sollte sohin der Verfassungsgerichtshof den § 99d BWG als verfassungswidrig befinden, so wären auch die Bestimmungen zur Geldbuße im neuen DSG, die daran angelehnt sind, voraussichtlich als verfassungswidrig zu qualifizieren und daher wohl nur von kurzer Lebensdauer.

Dieses Ergebnis wird entsprechend einem Rechtsgutachten von **Potacs/Raschauer**[5] durch folgende Überlegungen gestützt:

Art 83 Abs 9 DSGVO enthält eine Öffnungsklausel für Mitgliedstaaten, deren Rechtsordnung keine Geldbußen vorsehen. In solchen Rechtsordnungen kann gemäß Art 83 Abs 9 DSGVO so vorgegangen werden, ***„dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von den Aufsichtsbehörden verhängten Geldbußen haben"***.
In Erwägungsgrund 151 wird zu dieser Bestimmung auf die Rechtsordnungen Dänemarks und Estland hingewiesen, in denen *„die in dieser Verordnung vorgesehenen Geldbußen nicht zulässig"* sind. Nach Ansicht der Gutachter ist diese Reglung des Art 83 Abs 9 DSGVO allerdings nicht nur in Bezug auf Dänemark und Estland anwendbar.[6] Vielmehr sollten diese Bestimmung nach den *„Besonderheiten mitgliedstaatlicher Rechtsordnungen"*[7] im allgemeinen Rechnung tragen, weshalb sich auch im Text von Art 83 Abs 9 DSGVO keine Einschränkung auf Dänemark und Estland finden lässt. Dementsprechend formuliert auch Erwägungsgrund 151 sehr allgemein, wonach die *„zuständigen nationalen Gerichte die Empfehlung der Aufsichtsbehörde, die die Geldbuße in die Wege geleitet hat, berücksichtigen"* sollten.

---

[5] *Potacs/Raschauer*, Rechtsgutachten zum Anpassungsbedarf im Verwaltungsstrafverfahren auf Grund exzessiver Strafdrohung - dargestellt am Beispiel der Datenschutzgrundverordnung.
[6] Siehe aber *Feiler/Forgó*, EU-DSGVO, 352, Rz 21.
[7] *Frenzel*, Art 83, Rz 30.

Art 83 Abs 9 DSGVO müsste daher auch dann anwendbar sein, wenn die in Art 83 DSGVO vorgesehenen administrativen Geldbußen in den Rechtsordnungen der Mitgliedstaaten auch nur teilweise unzulässig sind. In solchen Fällen dürfen die Mitgliedstaaten ein System einrichten, **nach dem die Aufsichtsbehörden ein Verfahren in die Wege leiten, in dem dann die Geldbußen von staatlichen Gerichten verhängt werden.**

Ein Lösungsansatz bestünde daher darin, ein Verfahren festzulegen, in welchem die Datenschutzbehörde ein Verfahren beim Bundesverwaltungsgericht (oder allenfalls einem ordentlichen Zivilgericht) einleitet und dieses dann die Geldbuße verhängt. Die Datenschutzbehörde würde demnach den „Ankläger" darstellen und das Gericht den „Richter". Im Hinblick auf die Judikatur des VfGH könnte auch eine Lösung gefunden werden, wonach die Datenschutzbehörde geringere Geldbußen selbst verhängt und erst ab einer bestimmten Höhe einen Antrag auf Verhängung der Geldbuße durch ein Gericht stellen muss.

Abgesehen von der kritischen Judikatur des VfGH über die Verhängung hoher Strafen durch Verwaltungsbehörden untermauert auch das **nemo-tenetur-Prinzip** unsere Ansicht, dass Ankläger, Ermittler und Richter getrennt sein müssen. Arbeitet ein Unternehmen nicht mit der Aufsichtsbehörde gemäß Art 31 DSGVO zusammen, weil es sich nicht selbst belasten möchte, dann könnte die ermittelnde Behörde das Strafverfahren einleiten und selbst über die Strafhöhe entscheiden. Das Unternehmen wäre somit gezwungen mitzuarbeiten und sich selbst zu belasten ohne dass es einer übergeordneten Überprüfung durch eine andere Instanz, ob die Verweigerung zu Recht erfolgt ist, bedürfte.

Jedenfalls wäre aber eine Ahndung durch ordentliche Gerichte im Rahmen der Strafgerichtsbarkeit unter Anwendung der Strafprozessordnung und des Verbandverantwortlichkeitsgesetztes völlig unangemessen, denn unabhängig von der Höhe der Geldbuße ist der Unwertgehalt von Verletzungen der DSGVO zwar keine Bagatelle, aber dennoch niemals einer Kriminalisierung angemessen. Außerdem muss das Verfahren durch eine Aufsichtsbehörde in die Wege geleitet werden, was eine Anklagebefugnis durch die Staatsanwaltschaft ausschließt und was gegen eine Ahndung durch ein ordentliches Gericht im Rahmen der Strafgerichtsbarkeit spricht.

Potacs/Raschauer halten weiters folgendes fest: *„Gemäß Art 83 Abs 2 lit b DSGVO hat die Behörde Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes gebührend zu berücksichtigen. Die Verhängung von Geldbußen ist demnach verschuldensabhängig, wobei die Unschuldsvermutung gilt. Dies ist ersichtlich von Amts wegen zu ermitteln. Damit ist die in § 5 VStG verankerte Verschuldensvermutung nicht zu vereinbaren. Ganz allgemein ist darauf hinzuweisen, dass die Verschuldensvermutung des § 5 Abs 1 VStG bei hohen Strafen mit Art 6 MRK und Art 48 GRC nicht im Einklang steht."*
Aufgrund der dazu ergangenen Judikatur und des Gutachtens von Potacs/Raschauer, darf und kann § 5 VStG nicht Grundlage einer Bestrafung sein. Es ist daher gesetzlich klarzustellen, dass die Verschuldensvermutung des § 5 VStG im Bereich der Umsetzung der DSGVO nicht zur Anwendung kommt. Sollte dennoch § 5 VStG zur Anwendung kommen, dann wird vorgeschlagen, ab einer bestimmten Strafdrohung die Bescheinigungslast entfallen zu lassen.

In den Erläuterungen wird ausdrücklich auf die Regelung zum Kumulationsverbot in Art 83 Abs 3 DSGVO hingewiesen. Dies wird begrüßt; allerdings wäre eine Regelung, die das Kumulationsprinzip für unanwendbar erklärt, im Gesetzestext selbst vorzuziehen.

Weiters wird dringendst auf die Notwendigkeit der **„Verwarnung"** hingewiesen, da nicht jeder datenschutzrechtliche Verstoß ausschließlich durch die Verhängung einer Geldbuße geahndet werden kann. In einigen Fällen, insbesondere in den Fällen der Fahrlässigkeit, kann es durchaus genügen, den Verantwortlichen zu verwarnen, damit sich ein Verstoß

nicht wiederholt. Wir begrüßen hier die Erläuterungen zu § 11 und zu § 69 DSG, welche vorsehen, dass unter den von der DSGVO vorgesehenen Voraussetzungen (Art 83 iVm Erwägungsgrund 148) bzw nach dem VStG eine Verwarnung erteilt bzw eine Ermahnung ausgesprochen werden kann. Noch begrüßenswerter wäre jedoch eine entsprechende ausdrückliche und verpflichtende Regelung im Gesetzestext.

Zu § 12 (Tätigkeitsbericht und Veröffentlichung von Entscheidungen):

Gerade im Hinblick auf die neue Rechtslage und das Fehlen von diesbezüglichen Entscheidungen wäre es sinnvoll, sämtliche Entscheidungen der Datenschutzbehörde zu veröffentlichen.

Zu § 14 (Begleitende Maßnahmen):

Im Sinne der obenstehenden Erwägungen zu § 11 Abs 4 muss der Wortlaut des § 14 Abs 1 dem § 11 Abs 4 gleichgezogen werden. Aus diesem Grund wird eine Änderung wie folgt angeregt.

*„§ 14. (1) **Liegt durch den Betrieb einer Datenverarbeitung ein offenkundiges wesentliches unmittelbares Risiko für die Rechte und Freiheiten der betroffenen Person (Gefahr in Verzug) vor, so** kann die Datenschutzbehörde nach § 11 Abs 4 vorgehen."*

§ 14 Abs. 4 des Gesetzesentwurfs sieht vor, dass Bescheide, die eine Übermittlung von Daten ins EU-Ausland genehmigen, bis auf weiteres weiter gelten, aber im Falle dessen, dass die rechtlichen Voraussetzungen nicht mehr bestehen, zu widerrufen sind.
Diese Rechtswirkungen sollten auf alle Bescheide der Datenschutzbehörde anwendbar sein, soweit diese einer Verfahrenspartei eine bestimmte Datenverwendung gestatten; dies auch, um den Bescheidadressaten hinsichtlich ihrer bis dato bescheidmäßig gestatteten Datenverwendung Rechtssicherheit zu gewähren.

Zu § 17 (Vertretung von betroffenen Personen):

Generell sollten derart vertretungsbefugte Verbände speziell akkreditiert oder ähnlich dem § 19 Konsumentenschutzgesetz vorab gesetzlich ermächtigt werden müssen. Gewisse Kriterien sind unabhängig davon unabdingbar einzuhalten bzw gesetzlich zu definieren, beispielsweise die Sicherstellung etwaiger Prozesskosten bzw die ausreichende Kapitalausstattung, prozessgebundene Rücklage, etc. Auch darf und sollte die Rechtsanwaltspflicht nicht durch Betrauung eines solchen Verbands umgangen werden. Angedacht werden könnte auch eine Verordnungsermächtigung für das Bundeskanzleramt im Einvernehmen mit BMWFW (ebenfalls unter Einhaltung spezieller Kriterien) zur Bestimmung solcher Verbände.

Ausgeschlossen werden sollte, dass sich auch **ausländische Verbände** auf Abmahnungen in Österreich konzentrieren können, so zB deutsche Verbände. Der Vertretungsrecht sollte sich daher ausschließlich auf inländische Einrichtungen beschränken.

Zu § 18 (Haftung und Recht auf Schadenersatz):

Zum ausgeführten Gerichtsstand nach § 18 Abs 2 möchten wir eindringlich darauf hinweisen, dass datenschutzrechtliche Materien keine konsumentenschutzrechtlichen Angelegenheiten darstellen, weshalb auch eine Begründung des Gerichtsstands des gewöhnlichen Aufenthalts des Klägers nicht gerechtfertigt werden kann. Dieser kann natürlich nur eine Option darstellen, nicht jedoch die Regel. Die Regel sollte wie allgemein üblich der Gerichtsstand des gewöhnlichen Aufenthalts des Beklagten sein.

Zu § 19 (Allgemeine Bedingungen für die Verhängung von Geldbußen):

In Abs 2 ist geregelt, dass juristische Personen auch für das Fehlverhalten der ihnen zurechenbaren Personen nach Abs 1 (zB Geschäftsführer) verantwortlich gemacht werden können, Abs 3 verweist auf das Absehen einer Strafe gegen den Verantwortlichen nach § 9 VStG, wenn für dieselbe Strafe bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wurde. Wir begrüßen, dass die Haftung juristischer Personen in den Vordergrund getreten ist. Diese sollte aufgrund des Doppelbestrafungsverbots jedoch alleinig zur Haftung herangezogen werden können.

Zwar hat die Datenschutzbehörde gemäß § 19 Abs 3 DSG von der Bestrafung eines Verantwortlichen gemäß § 9 VStG abzusehen, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wird. Das hindert die Behörde allerdings nicht zuerst gegen die natürliche Person und im Anschluss gegen die juristische Person vorzugehen. Darüber hinaus sieht § 9 Abs 7 VStG eine Solidarhaftung vor: Während juristische Personen im Kriminalstrafrecht ausschließlich im Rahmen des Verbandsverantwortlichkeitsrecht belangt werden können, haften sie gemäß § 9 Abs 7 VStG (zusätzlich) zu den § 9 Beauftragten (bzw Vertretungsbefugten) für die verhängte Geldstrafe.

Diese Problematik wäre dadurch aufzulösen, wenn ausschließlich die juristische Person zur Verantwortung gezogen würde. Die Verordnung berücksichtigt in EG 149 ausdrücklich den Grundsatz „ne bis in idem" insofern, als in der Verhängung von strafrechtlichen und verwaltungsstrafrechtlichen Sanktionen darauf Rücksicht zu nehmen ist.

Es muss daher sichergestellt werden, dass es **nicht zu einer Doppelbestrafung** der juristischen Person und einer natürlichen Person kommen kann. Ist der Verantwortliche eine juristische Person, so sollte ausschließlich diese bestraft werden können. Eine entsprechende Klarstellung ist dringend erforderlich.
In Abs 3 sollte der letzte Halbsatz „und keine besonderen Umstände vorliegen, die einem Absehen von der Bestrafung entgegenstehen" gestrichen werden. Sollte das nicht möglich sein, müssten zumindest die „besonderen Umstände" näher definiert werden. Jedenfalls dürfen darunter nur äußerste Extremfälle verstanden werden.

Um das richtige Augenmaß für die Verantwortung natürlicher Personen zu wahren[8], regen wir an, teilweise den Erwägungsgrund 150 DSGVO in die Erläuterungen zu § 19 Abs 3 aufzunehmen:

„[…] Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der Erwägung des angemessenen Betrags für die Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen."

Damit würde klargestellt, dass existenzgefährdende Geldbußen für natürliche Personen nicht im Sinne der DSGVO wären.

Weiters muss bei der Bemessung der Geldstrafen auf die Unternehmensstruktur, insbesondere auf KMU, Rücksicht genommen werden.

Aus Rechtssicherheitsgründen sollte zumindest in den Erläuterungen klargestellt werden, dass für die Einhaltung der datenschutzrechtlichen Bestimmungen ein verantwortlicher

[8] Das durchschnittliche Jahresnettoeinkommen eines nach § 9 VStG zum verantwortlichen Beauftragten bestellten Mitarbeiters z.B. einer Bank oder eines Versicherungsunternehmens ist im Regelfall bei weitem nicht ausreichend, derartige Geldstrafen auch nur annähernd zu begleichen. Gäbe es die Begrenzung der Ersatzfreiheitstrafe mit höchstens 6 Wochen gemäß § 16 Abs 2 VStG nicht, so käme man hier auf mehrfach lebenslange Ersatzfreiheitsstrafen.

Beauftragter iSd § 9 Abs 2 VStG rechtskräftig bestellt werden kann. Es gibt zu diesem Thema bis dato in der Praxis die unterschiedlichsten Rechtsansichten.

Letztlich sollte klargestellt werden, dass der Datenschutzbeauftrage niemals Verantwortlicher gemäß § 9 VStG sein kann.

Zu Abs 5:
§ 19 Abs. 5 des Entwurfs sieht vor, dass gegen Behörden und „öffentliche Stellen" keine Geldbußen verhängt werden können. Diese Bestimmung hat ihren Ursprung in Art 83 Abs 7 DSGVO, welcher normiert, dass jeder Mitgliedstaat Vorschriften dafür festlegen *kann, ob und in welchem Umfang* gegen Behörden und öffentliche Stellen im betreffenden Mitgliedstaat, Geldbußen verhängt werden können. Der Entwurf enthält keine Definition des Begriffes „öffentliche Stelle".
Der Begriff der „öffentlichen Stelle" ist nach Ansicht der Art 29-Datenschutzgruppe durch nationale Rechtsordnungen festzulegen[9]. Erforderlich wäre daher eine Definition der „öffentlichen Stelle" im DSG. Jedenfalls gehen wir davon aus, dass sämtliche Körperschaften öffentlichen Rechts gemäß WKG als „öffentliche Stellen" im Sinne dieser Bestimmung anzusehen sind.

Bei einer Definition des Begriffs der „öffentlichen Stelle" fordern die Bundessparten Information und Consulting sowie Tourismus und Freizeitwirtschaft auch eine Klarstellung dahingehend, dass bei unternehmerischer Tätigkeit auch über „öffentliche Stellen" Geldbußen verhängt werden können um eine Gleichbehandlung mit privaten Unternehmen zu gewährleisten. Derartige Klarstellungen sind auch im Einklang mit der DSGVO, die es in ihrem Art 83 Abs 7 den Mitgliedstaaten freistellt, auch festzulegen „in welchem Umfang" über öffentliche Stellen Geldbußen verhängt werden können.

Weiters wäre eine Klarstellung erforderlich, dass die datenschutzrechtlichen Vorgaben der DSGVO auch für Behörden und öffentliche Stellen einzuhalten sind.

Zu § 21 (Datenschutzrat):

In den Datenschutzrat sollten auch private Unternehmen Vertreter entsenden können.

Zu §§ 25 ff (Datenverarbeitungen zu spezifischen Zwecken):

Zu den Ausführungen in den Erläuterungen zu § 25 des Entwurfs, „Flexibilisierungsklausel":

Die „Erstreckung" dieser Flexibilisierungsklausel des Art 6 Abs 2 DSGVO auch auf den privaten Bereich ist mehr als hinterfragenswert. Die Ausführungen in den Erläuterungen zum Entwurf lassen den Schluss zu, dass die DSGVO anscheinend in einigen Punkte Art 8 EMRK widersprechen würde und daher die Mitgliedstaaten sich über den Wortlaut hinwegsetzen können. Auch der Verweis auf eine Aussage des Juristischen Dienstes des Rates in einer Sitzung am 26.11.2014 ist irritierend, zumal bei der großen Anzahl an Sitzungen im Rahmen der Verhandlungen zur DSGVO wohl die unterschiedlichsten Aussagen getätigt wurden und hier auch nicht auf die letztgültige Textversion Bezug genommen wird. Sollte entgegen unserer Ansicht die Erstreckung dieser Flexibilisierungsklausel auch auf den privaten Bereich tatsächlich möglich sein, so bedarf es aus unserer Sicht einer ordnungsgemäßen und nachvollziehbaren Begründung, warum vom ausdrücklichen Wortlaut

[9] Siehe dazu WP 243 in der revidierten Fassung vom 5.4.2017: *The WP29 considers that such a notion is to be determined under national law. Accordingly, public authorities and bodies include national, regional and local authorities, but the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law.*

der DSGVO abgewichen wird. Dies wäre aus Rechtssicherheits- und Nachvollziehbarkeitsgründen jedenfalls erforderlich.

Zu § 25 (Verarbeitung zum Zweck der wissenschaftlichen Forschung und Statistik):

Wie bereits die Richtlinie 95/46/EG weist auch die DSGVO der Verwendung personenbezogener Daten zu Zwecken der **wissenschaftlichen Forschung und Statistik** eine privilegierte Stellung zu. Dies ist Ausdruck des Spannungsverhältnisses, in dem das in Art 8 der Charta der Grundrechte der Europäischen Union normierte Recht auf den Schutz personenbezogener Daten einerseits und die in Art 13 der EU-Grundrechtecharta normierte Freiheit der Wissenschaft (Forschung) andererseits zu einander stehen. Dieses **grundrechtliche Spannungsverhältnis** besteht auch in Österreichs innerstaatlichem Recht zwischen der Wissenschaftsfreiheit nach Art 17 StGG und dem Grundrecht auf Datenschutz gemäß § 1 des derzeit geltenden DSG 2000, das nach § 1 des DSG verfassungsrechtlich verankert bleiben soll.

Diese privilegierte Stellung der Datenverwendung zu Zwecken der wissenschaftlichen Forschung und Statistik kommt in der DSGVO etwa in Art 5 Abs 1 lit b), Art 9 Abs 2 lit j) sowie Art 89 Abs 2 zum Ausdruck. Die beiden letztgenannten Bestimmungen ermächtigen sowohl den europäischen als auch den nationalen Gesetzgeber, Regelungen vorzusehen, die einerseits die Verwendung besonderer Kategorien personenbezogener Daten (Art 9 Abs 1 DSGVO) zu den genannten Zwecken unter bestimmten Voraussetzungen auch ohne die Zustimmung der betroffenen Person ermöglichen (Art 9 Abs 2 lit j), und andererseits die Einschränkung von Rechten betroffener Personen bei der Verwendung personenbezogener Daten zu diesen Zwecken vorsehen können (Art 89 Abs 2).

Der Öffnungsklausel des Art 9 Abs 2 lit j) DSGVO trägt das DSG insofern Rechnung, als der den § 46 DSG 2000 weitestgehend übernehmende § 25 des DSG vorsieht, dass bei Vorliegen einer der in § 25 Abs 1 Z 1 bis 3 des DSG genannten Voraussetzungen alle personenbezogenen Daten, also auch besondere Kategorien personenbezogener Daten im Sinne des Art 9 DSGVO, für Zwecke wissenschaftlicher (statistischer) Untersuchungen verarbeitet werden dürfen, sofern solche Untersuchungen keine personenbezogenen Ergebnisse zum Ziel haben.

Demgegenüber legt § 25 Abs 2 des DSG (wie auch schon bisher § 46 Abs 2 DSG 2000) fest, dass in den nicht von Abs 1 Z 1-3 erfassten Fällen, die Verwendung personenbezogener Daten (sowohl der besonderen als auch der nicht-besonderen Datenkategorien) zu Zwecken wissenschaftlicher Forschung und Statistik nur auf sondergesetzlicher Grundlage (Abs 2 Z 1), mit Zustimmung des Betroffenen (Abs 2 Z 2) oder mit Genehmigung der Datenschutzbehörde (Abs 2 Z 3) zulässig ist.

In diesem Zusammenhang wäre es aus unserer Sicht wünschenswert, in den Erläuterungen zum Gesetzesentwurf festzuhalten, dass die Zulässigkeit der Verwendung nicht-besonderer Kategorien personenbezogener Daten (sohin „schlichter" personenbezogener Daten) zu Zwecken wissenschaftlicher Forschung und Statistik auf der Grundlage berechtigter Interessen des Verantwortlichen gemäß Art 6 Abs 1 lit f) DSGVO durch § 25 des DSG in keiner Weise eingeschränkt wird. Diese Klarstellung, die übrigens auch in der Begründung zu § 27 des deutschen Datenschutz-Anpassungs- und -Umsetzungsgesetzes-EU (dDSAnpUG-EU) enthalten ist, würde nicht zuletzt eine DSGVO- und somit europarechtskonforme Auslegung des § 25 des DSG sicherstellen.

Ferner plädieren wir für die Einführung einer weiteren Bestimmung, die vergleichbar zu § 27 des deutschen BDSG-neu idF des dDSAnpUG-EU (beispielsweise als § 25a des DSG) Folgendes vorsieht:

„§ 25a
Verarbeitung besonderer Kategorien personenbezogener Daten zum Zweck der wissenschaftlichen Forschung und Statistik
(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke wissenschaftlicher Forschung und Statistik ist auch ohne Einwilligung der betroffenen Person zulässig, wenn dies zur Erreichung dieser Zwecke erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person am Ausschluss der Verarbeitung deutlich überwiegen. Der Verantwortliche ist in diesem Fall verpflichtet, angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen zu ergreifen.
(2) Die in Abs. 1 angeführten Bestimmungen entbinden den Verantwortlichen nicht von seiner Verpflichtung, angemessene technische und organisatorische Maßnahmen zum Schutz der Rechte sowie der Wahrung der Interessen betroffener Personen zu ergreifen, zu denen insbesondere die frühestmögliche Pseudonymisierung und Anonymisierung in Einklang mit § 25 Absatz 5 sowie Artikel 89 Absatz 1 der Verordnung (EU) 2016/679 gehören.“

Eine derartige Regelung wäre wünschenswert, weil zur Umsetzung wissenschaftlicher Forschungsvorhaben oder statistischer Untersuchungen vielfach besondere Kategorien personenbezogener Daten verarbeitet werden müssen, bevor es überhaupt möglich ist, die Zustimmung betroffener Personen einzuholen. Dies ist etwa stets dann der Fall, wenn das konkrete Forschungsziel (bzw das Erkenntnisinteresse einer statistischen Untersuchung) eine Vorauswahl von Probanden anhand besonderer Kategorien personenbezogener Daten notwendig macht. So kommen beispielsweise für viele medizinische Untersuchungen nur Personen mit einem bestimmten Krankheitsbild als Probanden in Frage oder für Meinungsumfragen innerhalb eines spezifischen Bevölkerungssegments nur die Angehörigen einer bestimmten Bevölkerungsgruppe.

Die in derartigen Situationen verwendeten Daten stammen häufig nicht (oder zumindest nicht ausschließlich) vom Verantwortlichen der Untersuchung selbst, sodass bei der Verarbeitung dieser Daten die in § 25 des DSG vorgesehene Privilegierung in aller Regel nicht in Anspruch genommen werden kann. Bei Annahme des DSG in seiner derzeitigen Form droht deshalb eine Gesetzeslücke, die durch die hier vorgeschlagene Regelung geschlossen werden sollte.

Aus unserer Sicht wäre es schließlich wünschenswert, in den Erläuterungen zum DSG ausdrücklich klarzustellen, dass auch die mit wissenschaftlichen Methoden (etwa in Einklang mit den ICC/ESOMAR-Richtlinien) betriebene **Markt- und Meinungsforschung** vom Begriff der wissenschaftlichen Forschung und Statistik im Sinne des § 25 des DSG erfasst ist.

Pseudonymisieren ist in der DSGVO allgemein definiert als die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzufügen zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Voraussetzung ist, dass 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 können.

§ 25 Abs. 1 Z 3 legt fest, dass Verantwortliche der Untersuchung alle personenbezogenen Daten verarbeiten dürfen, sofern diese für ihn pseudonymisert sind. Im Sinne der Rechtsklarheit sollte in diesem Zusammenhang auf die Verhaltensregeln verwiesen werden, durch welche nach Art. 40 Abs. 2 lit d DSGVO Verbände und anderen Vereinigungen eine Präzisierung von Pseudonymisierung vornehmen können.

Zu Missverständnissen könnte nun die Formulierung des § 25 Abs. 5 führen, welche ein „Verschlüsseln" der Daten vorsieht. Es wird angeregt die Terminologie der DSGVO einzuhalten und den Begriff der „Pseudonymisierung" zu verwenden.

Den Erläuterungen zu § 25 ist zu entnehmen, dass die Sonderregelungen für wissenschaftliche Forschung „Verantwortliche des öffentlichen oder privaten Bereichs" umfasst. Dies wird begrüßt und es wird zur Erhöhung der Rechtssicherheit in dieser Frage angeregt, auch im Gesetzestext festzuhalten, dass diese Regelung „für die öffentliche und private Forschung durch öffentliche und nicht-öffentliche Stellen gilt".

Entsprechend dem Erwägungsgrund 50 der DSGVO können im Recht der Mitgliedstaaten die Aufgaben und Zwecke bestimmt und konkretisiert werden, für die eine Weiterverarbeitung als vereinbar und rechtmäßig erachtet wird. In vielen Forschungsprojekten der pharmazeutischen Industrie kann es notwendig sein, dass bereits erhobene Gesundheitsdaten zu einem wissenschaftlichen Forschungszweck verarbeitet werden sollen, der vom dem ursprünglichen Zweck der Verarbeitung nicht umfasst ist. Dies würde Kosten sparen, unnötige Doppeluntersuchungen und das aufwendige nachträgliche Einholen von Einwilligungserklärungen vermeiden. Im Lichte dieses Erwägungsgrundes sollte in den Erläuterungen dargelegt werden, dass die Weiterverarbeitung für im öffentlichen Interesse liegende wissenschaftliche Forschungszwecke als vereinbarer und rechtmäßiger Verarbeitungsvorgang angesehen wird.

Weiters ist darauf hinzuwiesen, dass die Formulierung in den Erläuterungen in eindeutigem Widerspruch zum Gesetzestext bzw. der Praxis steht. Pseudonymiserung ist seit vielen Jahren in der Praxis ein umfassend etabliertes Standardinstrument im Umgang mit Forschungs- und Gesundheitsdaten. Bei Anwendung des § 25 Abs. 1 Z 3 des vorliegenden Entwurfes stellt sich im Falle von pseudonymisierten Daten daher die Frage, wie der Verantwortliche der Untersuchung (meist Sponsor einer klinischen Prüfung nach dem Arzneimittelgesetz) den in § 1 des Entwurfes erwähnten Grundrechten (insbesondere auf Auskunft, Richtigstellung und Löschung) nachkommen kann, wenn diesem de facto kein direkter Personenbezug vorliegt.

Schließlich ist daran zu erinnern, dass bei klinischen Prüfung, um die Integrität einer wissenschaftlichen Studie zu bewahren, aber auch um alle Sicherheitsaspekte einer Studie miteinzubeziehen, es essentiell ist, dass bereits erhobene Daten nicht wieder gelöscht werden und dem Recht auf Löschung nicht nachgekommen werden kann. Aber auch die angeführten Gründe in Art. 89 Abs. 2 DSGVO „wenn das Recht auf Löschung die Verwirklichung der spezifischen Zwecke unmöglich macht oder ernsthaft beeinträchtigt" zeigt wie im Bereich der klinischen Forschung z.B. ein Widerruf der Einwilligung interpretiert werden sollte: Daten, die bis zum Zeitpunkt des Widerrufs erhoben wurden, können für die Zwecke der Studie beibehalten und verwendet werden. Eine weitere Verarbeitung soll nicht möglich sein.

Es sollte daher dringend zumindest von der Ausnahme in Art. 89 Abs. 2 DSGVO Gebrauch gemacht werden und sollten die Rechte des Betroffenen insbesondere bei pseudonymisierten Daten keine Anwendung finden.

Zu § 27 (Freiheit der Meinungsäußerung und Informationsfreiheit):

Die DSGVO bietet den Mitgliedstaaten im Art 86 die Möglichkeit, den **Zugang der Öffentlichkeit zu amtlichen Dokumenten** auf einzelstaatlicher Ebene zu regeln. Gemäß der Richtlinie 2003/98/EG und Erwägungsgrund 154 ist davon auch die Weiterverarbeitung dieser Dokumente durch Weiterverwender umfasst, da die Weiterverwendung von Daten, die ohne Einschränkung öffentlich zugänglich sind, auf Grundlage der EU-PSI Richtlinie und des heimischen IWG erlaubt ist.

Sowohl der Zugang zu den Daten, als auch die Weiterverwendung von öffentlichen Daten stellen ein **öffentliches Interesse** dar. Bezüglich des Zugangs ist dieses Interesse in Erwägungsgrund 154 festgehalten: *„Der Zugang der Öffentlichkeit zu amtlichen Dokumenten kann als öffentliches Interesse betrachtet werden."* Umfassendere Möglichkeiten für die Weiterverwendung von Informationen des öffentlichen Sektors sollten u.a. die europäischen Unternehmen in die Lage versetzen, deren Potenzial zu nutzen, sowie zu Wirtschaftswachstum und Schaffung von Arbeitsplätzen beitragen (EG 5 der Richtlinie 2003/98/EG). Die Möglichkeiten der PSI Richtlinie werden vor allem von innovativen Startups wahrgenommen.

Jeder Widerspruch von Betroffenen gemäß Artikel 21 DSGVO gegen die weitere Verarbeitung derartiger veröffentlichter Daten richtet sich daher auch gegen das öffentliche Interesse an der Transparenz. Im Falle von Artikel 21 Abs 1 hat der Verantwortliche zwingende schutzwürdige Gründe für die Verarbeitung nachzuweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, falls er die Daten trotz Widerspruch weiterverarbeiten will. Für die Abwägung dieser Gründe gegen das Interesse der Betroffenen ist im Falle von IWG-Daten klarzustellen, dass

- Betroffene jedenfalls mit der Weiterverwendung ihrer Daten gemäß PSI Richtlinie im Sinne des Erwägungsgrundes 47 DSGVO rechnen müssen, wenn sie in öffentlich zugängliche Register eingetragen werden,
- das Geheimhaltungsinteresse praktisch nicht gegeben ist, wenn die Daten in öffentlichen Registern frei zugänglich sind,
- das öffentliche Interesse an der Transparenz gegeben ist,
- die Verarbeitung personenbezogener Daten für die Verhinderung von Betrug gemäß Erwägungsgrund 47 DSGVO ein berechtigtes Interesse darstellt,
- die Vollständigkeit und Richtigkeit von Datenbanken laut Artikel 9 der Richtlinie 2008/48/EG ebenfalls ein wichtiges öffentliches Interesse darstellt.

Zu § 29 (Verarbeitung personenbezogener Daten im Beschäftigungskontext):

§ 29 erster Satz sieht vor, dass „das Arbeitsverfassungsgesetz (ArbVG), BGBl. Nr. 22/1974, eine Vorschrift im Sinne des Art. 88 DSGVO [ist]".

Es bedarf hier der Klarstellung, dass Verstöße gegen das ArbVG nicht dem Sanktionsregime der DSGVO unterliegen.
Wir sprechen uns daher für eine ersatzlose Streichung des § 29 DSG aus.
Sollte eine gänzliche Streichung nicht möglich sein, könnte alternativ ausschließlich der 2. Satz („Die dem Betriebsrat zustehenden Befugnisse bleiben unberührt.") erhalten bleiben.

Es sollte in diesem Zusammenhang zudem klargestellt werden, dass Strafregisterauszüge von Mitarbeitern verarbeitet werden dürfen (elektronisch oder analoge Ablage).

Zu §§ 30 bis 33 (Bildverarbeitung):

Die DSGVO enthält keine speziellen Regelungen zu Videoüberwachungen und Bildverarbeitung. Nach den Erläuterungen stützt sich der österreichische Gesetzgeber als unionsrechtliche Grundlage für die Bestimmungen der §§ 30 ff jedoch auf folgende Regelungen der DSGVO:

- Art 6 Abs 2 und 3 (danach können aber nur in Bezug auf die Rechtmäßigkeitsgründe Erfüllung rechtlicher Verpflichtungen und öffentlicher Aufgaben Sonderregeln vorgesehen werden);

- Erwägungsgrund 10 (bei diesem handelt sich nur um einen bloßen Erwägungsgrund, dem nicht die normative Bedeutung des VO-Texts zukommt. Zudem geht aus EG 10 nicht zweifelsfrei hervor, dass auf dessen Grundlage eine Verschärfung der Datenschutzbestimmungen gestützt werden kann).

Die Regelungen für die Bildverarbeitung im DSG sind somit erheblich restriktiver als die allgemeinen Regeln der DSGVO. Insbesondere die Zulässigkeitsvoraussetzungen des § 30 Abs 2 sind strenger ausgestaltet als jene in Art 6 DSGVO. Konkret wird in § 30 Abs 2 etwa eine „vertragliche Verpflichtung" und das „öffentliche Interesse" nicht als Zulässigkeitsvoraussetzung genannt.
Auch findet sich in § 30 Abs 2 Z 4 wieder das Zulässigkeitserfordernis des „überwiegenden berechtigten Interesse des Verantwortlichen", was wiederum dem Wortlaut des Art 6 Abs 1 lit f DSGVO widerspricht (siehe Ausführungen zu § 1).

Darüber hinaus sind die in § 30 Abs 4 normierten Fälle einer absoluten Unzulässigkeit (Kontrolle der Arbeitnehmer, automationsunterstützter Abgleich, Auswertung anhand sensibler Daten) einer Bildaufnahme überaus streng ausgestaltet. Aufgrund ihrer generellen Geltung erlauben sie - anders als Art 6 DSGVO - keine Rechtfertigung, wie zB durch Einwilligung, Interessenabwägung oder in Form der Erfüllung rechtlicher Verpflichtungen.

Insgesamt ist eine entsprechende Grundlage in der DSGVO für diese restriktiveren Regeln nicht gegeben. Die Regelungen sind daher uE europarechtswidrig.

Inhaltlich wird Folgendes angemerkt:

Mit der neuen Regelung werden jegliche Bildaufnahmen umfasst, was unserem Erachten nach definitiv als überschießend zu betrachten ist. Es sollte jedenfalls auf den Zweck der Bildaufnahme abgestellt werden.

Ein Eingriff in Rechte von Betroffenen ist mit Sicherheit als schwerwiegender anzusehen, wenn eine systematische Überwachung erfolgt, als bei rein privaten Aufnahmen ohne einen Überwachungszweck.

Der neue § 30 Abs. 3 Z 3 erscheint nicht ausreichend, um zulässige Privataufnahmen zu machen. Dies vor allem in Zusammenschau mit Abs. 4, der aussagt, dass Bildaufnahmen ohne ausdrückliche Einwilligung der betroffenen Person in deren höchstpersönlichen Lebensbereich immer unzulässig sind. Abgesehen vom Kernbereich der Privatsphäre soll auch ein Eingriff in deren Vorfeld unzulässig sein, wie etwa die Kontrolle von Zugängen zu Sakralgebäuden. Dies ist verständlich, wenn es um eine Überwachung bzw., wie auch in den Erläuterungen festgehalten, um die Kontrolle von solchen Zugängen geht. Da aber der Gesetzestext keinen Unterschied zwischen einer Überwachung/Kontrolle und bloßen privaten Aufnahmen ohne einen Überwachungszweck macht, hätte diese Regelung zur Folge, dass alle Bildaufnahmen u. ä. - ob ein privates Dokumentationsinteresse besteht oder nicht - rechtswidrig wären.

Es soll daher jedenfalls eine Differenzierung zwischen Bildaufnahmen zu Überwachungszwecken und Privataufnahmen ohne diesen Zweck erfolgen.

Es muss klargestellt werden, dass die Voraussetzung „bereits erfolgter Rechtsverletzungen" allgemein und nicht standortspezifisch zu verstehen ist.

Zu § 30 Abs 4 Z 2 ist anzumerken, dass unserer Ansicht nach jedenfalls sichergestellt werden muss, dass diese Bestimmung nicht enger ausgelegt wird als der derzeitige Status Quo. D.h. dass die gezielte Arbeitnehmerkontrolle durch Videoüberwachung zwar unzulässig ist, aber die Überwachung von Objekten an Arbeitsstätten (zB Schank/Kassa-

Bereich) weiterhin zulässig sein muss, wenn der primäre Zweck der Überwachung nicht auf die Arbeitsleistung gerichtet ist.

Grundsätzlich werden zB Bilder von Arbeitnehmern, die bspw. unternehmensintern verwendet werden sollen sowie Bilder, die im Rahmen von Veranstaltungen aufgenommen werden, wohl in den Anwendungsbereich des § 30 Abs 3 Z 3 fallen und somit nicht unbedingt eine Zustimmungserklärung benötigen. Zur Klarstellung wäre hier aber eine Feststellung (zumindest in den Erläuterungen) wünschenswert, dass „Dokumentationsinteresse" weit auszulegen ist.

Vor dem Hintergrund, dass in vielen Fällen die konkrete Verwendung von Bildern (zB Verwendung in unternehmensinternem Telefonbuch, Veröffentlichung von Veranstaltungsbildern auf einer Website oder in einer Unternehmenszeitung) bereits aufgrund des Bildnisschutzes bestimmten Voraussetzungen unterworfen ist (insb der Zustimmung der abgebildeten Personen), sollte zumindest für derartige Fallgruppen die Dokumentationspflicht entfallen.

Eine lange Aufbewahrungszeit kann schon aufgrund eines bloßen „Dokumentationsinteresses" erfolgen. Daher sollte die Aufbewahrungsfrist für Bilder zu Gänze gestrichen oder zumindest erheblich verlängert werden.

Ferner sollte in die Erläuterungen aufgenommen werden, dass bei Fällen mit längerer Speicherdauer, wo das rechtliche Interesse daran von der Behörde festgestellt wurde, diese Speicherdauer auch nach In-Kraft-treten des neuen Gesetzes zulässig bleibt.

Die weitgehende Ausdehnung dieser Bestimmungen gegenüber jenen zur Videoüberwachung gem §§ 50a ff DSG 2000 ist offensichtlich. Es muss dennoch sichergestellt sein, dass die Regelung lediglich bei **Identifizierbarkeit einer natürlichen Person** zur Anwendung kommt, wenn demnach personenbezogene Daten nach Art 4 Z 1 DSGVO verarbeitet werden würden, widrigenfalls auch Infrarotaufnahmen und auch selbstfahrende Autos mit Radarmessungen darunter zu subsumieren wären (was allerdings nicht die Intention des Gesetzgebers sein kann).

Weiters sollte klargestellt werden, dass die **Beschilderungspflicht** mit dem Namen des Verantwortlichen bei der Bilddatenverarbeitung für bereits vor dem 25.5.2018 montierte Hinweisschilder nicht gelten sollte, hier demnach eine eigene Übergangsbestimmung notwendig wäre.

Gemäß § 32 Abs 3 sind die aufgenommenen personenbezogenen Daten vom Verantwortlichen zu löschen, wenn sie für den Zweck, für den Sie ermittelt wurden, nicht mehr benötigt werden und keine andere gesetzlich vorgesehene Aufbewahrungspflicht besteht. Zur Klarstellung wäre aus unserer Sicht noch auf die Regelung des § 3 des Entwurfes zum DSG zu verweisen, wonach die Löschung der personenbezogenen Daten nicht unverzüglich zu erfolgen hat, wenn die Löschung aus wirtschaftlichen und technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann und die Verarbeitung dieser personenbezogenen Daten bis zu diesem Zeitpunkt einzuschränken ist.

Zu einzelnen betroffenen Branchen:
Leider wird die Standard- und Musterverordnung mit der Standardanwendung „Videoüberwachung" außer Kraft treten. Jedoch gehen wir davon aus, dass mit der Bestimmung § 30 Abs 3 Z 2 DSG die Videoüberwachung im bisherigen Sinn und Umfang zulässig ist. Die Aufbewahrungsdauer gem § 32 Abs 3 DSG (72 Stunden) bleibt erhalten.

Dies ist jedenfalls weiterhin essentiell für die Branche der **Tankstellen und Garagen**.

Speziell zur **Garagenwirtschaft:**
Es besteht ein besonderes Interesse, die Kraftfahrzeug - Kennzeichenerfassung weitestgehend rechtlich abzusichern.
Aus den Erläuterungen ist zu entnehmen, dass unter dem Begriff „Objekten" in § 30 Abs. 3 Z 3 etwa Kraftfahrzeugkennzeichen oder Fahrzeugaufschriften zu verstehen sind.
In der Praxis wird beispielsweise zur Überwachung der zulässigen Parkdauer (Einkaufszentrum gestattet z.B. kostenloses Parken bis zu zwei Stunden) an der Einfahrt eine Videoaufnahme mit Bild und Kennzeichen des PKW aufgenommen; daraus wird die Zeichenkette des Kennzeichens in einer Datenbank eingetragen (dadurch kann die tatsächliche Verweildauer gemessen werden).
Dieses System ist etwa mit der bekannten „Section-Control" vergleichbar und hat den Zweck, Missbrauch durch zweckwidrige Nutzung zu verhindern (Fahrzeuglenker nutzt den Parkplatz im Einkaufszentrum um andere Erledigungen durchzuführen bzw. als Dauerparkplatz für die Dauer des Arbeitstages).

Wird nun der Parkvorgang während der erlaubten Parkdauer abgeschlossen, werden die Daten nicht weiterbearbeitet und wieder gelöscht. Erst bei einem Verstoß gegen die Abstell- oder Nutzungsbedingungen (in aller Regel Zeitüberschreitung) werden die Daten herangezogen um dem Zulassungsbesitzer eine Zusatzgebühr/Strafgebühr zu verrechnen.

Diese Anwendung sollte zulässig sein und wir ersuchen daher um eine Klarstellung bzw. um Aufnahme in den Erläuterungen (als Beispiel für den Anwendungsfall des § 30 Abs. 3 Z 3).

Wir gehen bei diesem Anwendungsfall davon aus, dass das PKW-Kennzeichen keine personenbezogenen Inhalte zum Fahrer des Wagens aufweist.
Davon zu unterscheiden ist die Erfassung des Kennzeichens als „Zufahrtsmedium". Dauerparker oder sonstige registrierte Kunden stimmen bei Abschluss ihres Vertrages zu, dass das Kennzeichen als Zufahrts- und Ausfahrtsmedium bzw. zur Abrechnung der Parkzeit verwendet werden kann. Sinn dieser Zustimmungserklärung ist, dem Kunden mehr „Convenience beim Parken" zu bieten. Der Kunde braucht beim Schranken nicht mehr anhalten, sondern das System erkennt automatisch, dass dieses Fahrzeug ein „Kundenfahrzeug ist" und öffnet und schließt automatisch den Schranken. Diese vertragliche Nutzung der „Kennzeichen-Daten" sollte datenschutzrechtlich unbedenklich sein.

Beförderungsgewerbe mit **Pkw:**
Es gilt die Videoüberwachung in Taxis weiterhin zu ermöglichen (zum Schutz und Prävention von Taxiüberfällen). Taxis mit Videoüberwachung sind von außen gekennzeichnet und würden unter die Ausnahmebestimmung des § 30 Abs. 2 Z 2 fallen. Konsumenten erkennen von außen deutlich den Aufkleber der Videoüberwachung und stimmen somit einer Aufzeichnung zu. Die Voraussetzung „bereits erfolgter Rechtsverletzungen" muss allgemein und nicht standortspezifisch interpretiert werden.

In vielen moderneren KFZ und auch in Taxis gibt es eine Videoaufzeichnung der übrigen Verkehrsteilnehmer, um im Falle eines Verkehrsunfalles einen Beweis betreffend eines Fehlverhaltens gem. StVO zu haben und auch das Verschulden bei einem Verkehrsunfall mit Sachschaden oder Personenschaden leichter und eindeutiger nachzuweisen. In wie weit diese Aufzeichnungen unter die Ausnahmebestimmung gem. § 30 Abs. 2 Z. 4 fallen, erscheint fragwürdig und sollte noch näher und besser ausformuliert werden. Diese Unfallaufzeichnungssysteme erscheinen sinnvoll und scheinen für den einzelnen KFZ Lenker im Einzelfall vertretbar zu sein.

Seilbahnen:
Die Datenschutzbehörde hat die Bildüberwachung bei Zutrittsstellen von österreichischen Seilbahnen im Sommer 2015 rechtlich neu beurteilt und wertet sie seitdem als „Zutrittskontrolle mit Bildvergleich" und nicht mehr als Videoüberwachung.

In den dazugehörigen Rahmenbedingungen der Datenschutzbehörde ist mit dem automationsunterstützten Bilddatenabgleich ein Bereich, der für die österreichischen Seilbahnunternehmen von großer Bedeutung ist, nach wie vor streng geregelt. Im Punkt „Auswertungsvorgang" heißt es dort nämlich „... diese Überprüfung nimmt der nächst dem Drehkreuz in einem abgeschlossenen Raum befindliche Mitarbeiter (Liftangestellter) des Auftraggebers durch persönliche Wahrnehmung am Bildschirm vor. *Ein automationsunterstützter Bilddatenabgleich erfolgt nicht, da ein solcher unzulässig wäre.*"

Diese Anforderungen führen den Einsatz der Bildüberwachung bei der Zutrittskontrolle nahezu ad absurdum, da unserer Meinung nach der Mitarbeiter genauso gut einen direkten Vergleich zwischen dem Referenzfoto und den das Drehkreuz passierenden Personen vornehmen könnte. Die Aufnahme des Vergleichsfotos bringt keinen Vorteil und bindet noch dazu einen Mitarbeiter pro Zutrittsstelle zur Gänze. Ein wirklicher Vorteil wäre zum Beispiel der Einsatz eines Programmes, das basierend auf einem Prüf-Algorithmus (automatischer Vergleich von Geschlecht, Alter, etc.) Verdachtsfälle erkennt und bei Vorliegen eines solchen anschlägt.

Der Entwurf des Datenschutz-Anpassungsgesetzes behandelt den Bereich der Bildverarbeitung im 6. Abschnitt. In § 30 Abs 4 Z 3 soll der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten mit anderen personenbezogenen Daten als generell unzulässig verankert werden.

Wir sehen diese Bestimmung als zu streng, da ein automationsunterstützter Bilddatenabgleich bei Zutritts-Systemen von Seilbahnen nach unseren Vorstellungen ausschließlich Verdachtsfälle der Verletzung des Beförderungsvertrages identifizieren, und nicht nach anderen Kriterien suchen soll, die den Persönlichkeitsschutz der Betroffenen beeinträchtigen könnten (kein Filter nach absoluten Kriterien). Nicht die Identität der Personen soll festgestellt werden, sondern die Übereinstimmung der das Drehkreuz passierenden Person mit der laut Berechtigungsseriennummer auf der Liftkarte berechtigten Person. Der Konnex zu Name, Geburtsdatum oder anderen sensiblen Daten ist, außer bei ohnehin personalisierten Karten, bei diesem System auch bei Ausschöpfung aller Auswertungsmöglichkeiten nicht möglich.

Wir fordern daher eine Abschwächung der Bestimmung in § 30 Abs 4 Z 3, in der Form, dass so wie auch in § 30 Abs 4 Z 1 der Zusatz „ohne ausdrückliche Einwilligung der betroffenen Person" eingefügt werden soll.
Ziffer 4 würde dann wie folgt lauten: „der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten mit anderen personenbezogenen Daten ohne ausdrückliche Einwilligung der betroffenen Person".

Geschäfte:
Die Grundlage für die Videoüberwachung in Geschäften ist der § 30 Abs. 3 Z. 2 des Entwurfes, der die Videoüberwachung in öffentlich zugänglichen Orten regelt. Hier gab es bisher das Problem, dass die Außenseite eines Geschäftslokales nicht in die Überwachung einbezogen werden durfte, da dies in der Standard- und Musterverordnung nicht vorgesehen war. Das ist etwa bei Trafiken wegen der außen angebrachten Zigarettenautomaten und auch bei Juwelieren unbedingt erforderlich.

Bei der Videoüberwachung von privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden, gibt es in § 30 Abs. 3 Z. 1 die Regelung, dass öffentliche Verkehrsflächen in die Überwachung einbezogen werden dürfen, wenn dies zu Zweckerreichung unvermeidbar ist. Eine vergleichbare Regelung wird dringend auch für die Z. 2 dieser Regelung gefordert.

Betreffend die Datensicherheitsmaßnahmen findet sich im Entwurf zum Datenschutz-Anpassungsgesetz 2018 - außer im Zusammenhang mit der Bildverarbeitung - keine Regelung. Art. 32 DSGVO sieht unter dem Titel „Sicherheit der Verarbeitung" die Pflicht des Verantwortlichen und Auftragsverarbeiters vor, durch technische und organisatorische Maßnahmen ein angemessenes Schutzniveau für die Rechte und Pflichten der Betroffenen bei der Verarbeitung von Daten zu gewährleisten. Art 32 DSGVO hält diese Anforderungen sehr allgemein.
Im Sinne der Rechtssicherheit sollten die nationalen Bestimmungen konkretere Anforderungen an die Maßnahmen zur Datensicherheit abbilden.

Weiters sollte für Krankenanstalten Sonderregelungen in Bezug auf Datensicherheitsmaßnahmen normiert werden.
Schon die derzeit gemäß Datenschutzgesetz 2000 geltenden Datensicherheitsmaßnahmen zeigen, dass diesen - ohne dabei letztlich eine potentielle Gefährdung der Patientensicherheit in Kauf zu nehmen - realistischer Weise kaum Rechnung zu tragen ist. Im Rahmen von Krankenbehandlungen und Gesundheitsmaßnahmen sind vielfach rasche Reaktionen von mehreren handelnden Personen gefordert. Genau dies macht die Einhaltung von Datensicherheitsmaßnahmen, wie sie etwa in Art 32 DSGVO vorgesehen sind, vielfach sehr schwierig bis unmöglich. Im Sinne der Sicherstellung reibungsloser Abläufe in Gesundheitseinrichtungen, insbesondere Krankenanstalten, und der damit einhergehenden Sicherstellung der Patientensicherheit, sehen wir es daher geboten, für Krankenanstalten spezielle Regelungen hinsichtlich Datensicherheitsmaßnahmen zu normieren.

Die in § 32 Abs. 1 im Entwurf zum Datenschutz - Anpassungsgesetz 2018 getroffene Formulierung, wonach durch Datensicherheitsmaßnahmen eine nachträgliche Veränderung „durch Unbefugte ausgeschlossen" werden soll, ist aus technischer Sicht dahingehend abzuschwächen, als dass nach erfolgter Risikobewertung (Datenschutz-Folgeabschätzung) eine Manipulation durch Unbefugte „soweit wie möglich hintanzuhalten ist".

Zu § 69 (Verwaltungsstrafbestimmung):

Die subsidiäre Verwaltungsstrafbestimmung ist insofern zu kritisieren, als auch hier der Strafrahmen erheblich erhöht wurde (nunmehr € 50.000,-).

Auf die Bemerkungen zu § 19 wird auch in diesem Zusammenhang hingewiesen.

§ 69 **Abs 4** ist unklar formuliert, was insbesondere bei modernen Speicherlösungen Fragen aufwirft (zB Cloudlösungen - Was passiert mit allfälligen Immaterialgüterrechten, die mit den entsprechenden Daten verknüpft sind?). Ein Verfall erscheint nur dann möglich, wenn ausschließlich inkriminierte Daten auf dem Datenträger enthalten sind. Bei unterschiedliche Daten sind nur die entsprechenden Daten zu löschen.

Nach § 69 Abs 2 ist bereits die versuchte Verwirklichung der in § 69 Abs 1 Z 1 - 5 genannten Delikte strafbar. Bei der Einschauverweigerung gegenüber der Datenschutzbehörde ist jedoch völlig unklar, worin der Versuch bestehen soll. Es bedarf der Klarstellung in den Erläuterungen, dass dieser Tatbestand nicht auch bei der Äußerung von bloßen Bedenken verwirklicht sein soll.

Zu § 70 (Datenverarbeitung in Gewinn- oder Schädigungsabsicht):

§ 70 führt zur absurden Konsequenz, im gerichtlichen Strafrecht milder bestraft zu werden, als im Verwaltungsstrafverfahren nach der DSGVO. Die gerichtliche Strafe erscheint hier vergleichsweise niedrig, weshalb sich die Frage nach der Sinnhaftigkeit dieser Regelung stellt.

Zu § 76 (Übergangs- und Schlussbestimmungen):

Zu Abs 2:
In Abs. 2 ist vorgesehen, dass das von der Datenschutzbehörde geführte Datenverarbeitungsregister von der Datenschutzbehörde bis 31. Dezember 2019 zu Archivzwecken fortzuführen ist. Aus Haftungsüberlegungen (z.B. Betroffene möchten Ansprüche aus einer etwaigen nicht genehmigten Datenanwendung ableiten) erscheint dieser Zeitraum zu kurz. Das Datenverarbeitungsregister sollte daher zumindest bis 31.Dezember 2022 fortgeführt werden.

Zu Abs 4 und 5:
In §§ 76 Abs 4 und 5 DSG wird festgelegt, dass Verletzungen des DSG 2000, die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes noch nicht anhängig gemacht wurden, nach der Rechtslage nach Inkrafttreten des DSG (und somit der DSGVO) zu beurteilen sind. Nach den Erläuterungen zu § 76 DSG ist ein strafbarer Tatbestand, der vor dem Inkrafttreten des Datenschutz-Anpassungsgesetzes verwirklicht wurde, nach jener Rechtslage zu beurteilen, die für den Täter in ihrer Gesamtauswirkung günstiger ist. Eine entsprechende Regelung findet sich jedoch nicht im Gesetzestext selbst, eine solche Regelung ist allerdings nach verwaltungsstrafrechtlichen Grundsätzen geboten. So legt § 1 Abs 2 VStG fest, dass sich Strafen grundsätzlich nach dem zur Zeit der Tat geltenden Recht richtet, es sei denn, dass das zur Zeit der Entscheidung geltende Recht in seiner Gesamtauswirkung für den Täter günstiger wäre. Da die Strafdrohungen der DSGVO als erheblich ungünstiger einzuschätzen sind, als jene des DSG 2000, würde die Beibehaltung des § 76 Abs 4 und 5 des Entwurfes dieses **Günstigkeitsprinzip** verletzen und wird daher abgelehnt.

Zu Abs 8:
Nach § 76 Abs. 8 sollen besondere Bestimmungen über die Verarbeitung von personenbezogenen Daten in anderen Bundes- oder Landesgesetzen unberührt bleiben. Die leges speciales sollen den allgemeinen Regelungen des neuen DSG vorgehen.

Hier bleibt unklar, ob auch Verordnungen dem DSG vorgehen:
Beispielsweise sind in der Verordnung der Finanzmarktaufsichtsbehörde über Inhalt und Gliederung der versicherungsmathematischen Grundlagen (BGBl. II Nr. 296/2015) gemäß § 2 personenbezogene Daten des Aktuars und des stellvertretenden Aktuars zu verarbeiten.

Ein weiteres Beispiel stellt die Verordnung des Bundesministers für Verkehr, Innovation und Technologie über die Rahmenbedingungen für automatisiertes Fahren (BGBl. II Nr. 402/2016) dar: gemäß § 1 Abs. 3 sind unter anderem Angaben zum Lenker des für Testfahrten zu verwendenden Fahrzeuges zu übermitteln

Dementsprechend sollte in den Erläuterungen präzisiert werden, dass auch (datenschutzrechtliche) Vorschriften von Verordnungen unberührt bleiben und den Regelungen des neuen DSG vorgehen.

Gemäß den Erläuterungen bleiben rechtskräftige Akte der Datenschutzbehörde in bestimmtem Umfang aufrecht. Nicht aufrecht bleiben Registrierungsakte im DVR. Es ist klar, dass die Registrierungsakte nicht gültig bleiben können, dass es das

Datenverarbeitungsregister nicht mehr geben wird. Gerade bei der Videoüberwachung und den IVS-Registrierungen sollte die Zulässigkeit der Datenanwendung auf Grundlage der rechtskräftigen Akte der Datenschutzbehörde dennoch bestehen bleiben. Statt der Registrierung muss der Verantwortliche die Verarbeitung ins Verfahrensverzeichnis aufnehmen. Das sollte in die Erläuterungen aufgenommen werden.

Weitere Anliegen zu § 76:
Es bedarf zusätzlich einer Übergangsregelung für bisherig vereinbarte Verschwiegenheitserklärungen der Dienstnehmer nach § 15 DSG 2000. Sollten diese lediglich einen Verweis auf § 15 DSG 2000 enthalten, jedoch keine weitere inhaltliche Ausgestaltung, sollten sie auch weiterhin rechtswirksam und gültig sein, da der bisherige Inhalt des § 15 DSG 2000 jenen des § 6 Abs 1 DSG entspricht.

Weiters stellt sich nach wie vor die Frage nach den **Genehmigungsverfahren im internationalen Datenverkehr**. Neue Standardvertragsklauseln sind schnellstmöglich zu veröffentlichen und eine Klarstellung hinsichtlich der bestehenden Standardvertragsklauseln muss raschest möglich erfolgen.

Weitere Übergangsbestimmungen sind aus unserer Sicht zum Thema **Einwilligung** notwendig. Die Erläuterungen zu § 76 führen aus: *„Beruhen die Verarbeitungen auf einer Zustimmung gemäß dem DSG 2000, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Zustimmung den Bedingungen der DSGVO entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der DSGVO fortsetzen kann. Dies entspricht den im Erwägungsgrund 171 der DSGVO enthaltenen Ausführungen zur „Einwilligung" nach der Richtlinie 95/46/EG."* Die Bedingungen für die Einwilligung werden in Art 7 DSGVO geregelt. Sollten diese Bedingungen für die Einwilligung bereits durch die Einwilligungserklärungen vor Anwendbarkeit der DSGVO erfüllt worden sein, bedarf es keiner neuerlichen Einwilligung durch die betroffene Person.

Vor diesem Hintergrund wäre auch eine Regelung im Datenschutz-Anpassungsgesetz 2018 wünschenswert, dass datenschutzrechtliche Einwilligungen, die vor der Geltung der DSGVO ab Mai 2018 rechtsgültig nach den bis dahin geltenden Datenschutzgesetzen eingeholt wurden, auch **weiterhin Gültigkeit** haben.

Art 7 Abs 4 DSGVO statuiert ein sog **„Koppelungsverbot"**. Allerdings wird durch die Wortfolge „[...] *Umstand in größtmöglichem Umfang Rechnung getragen werden...*" großzügig formuliert, dass es einer Verhältnismäßigkeitsprüfung im Einzelfall bedarf, ob die Erfüllung eines Vertrags von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Man könnte diese Regelung somit auch als ein abgeschwächtes Koppelungsverbot bezeichnen.

Demgegenüber schränkt der Erwägungsgrund 43 zu Art 7 der DSGVO den Spielraum des Art 7 Abs 4 DSGVO ein und eröffnet diesen gleichzeitig, indem er statuiert *„um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern. Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der*

Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist".

Der zweite Satz des Erwägungsgrunds 43 schränkt somit die pauschale Regelung des Art 7 Abs 4 DSGVO ein, da er die Freiwilligkeit verneint, wenn die Einwilligung für die Erfüllung des Vertrags nicht erforderlich ist (**klassisches strenges Koppelungsverbot**). Satz 1 des Erwägungsgrunds 43 öffnet jedoch die Möglichkeit einer Abwägung, ob zwischen der betroffenen Person und dem Verantwortlichen ein Ungleichgewicht besteht. In Kombination mit Art 7 Abs 4 DSGVO hat dies zur Folge, dass es einer Einzelfallprüfung bedarf, ob ein Ungleichgewicht besteht und ob im größtmöglichen Umfang Rechnung getragen wurde, dass die Einwilligung zur Vertragserfüllung erforderlich ist.

Des Weiteren ist es Ausdruck der **Privatautonomie**, dass Unternehmen die Bedingungen zur Gültigkeit und Zustandekommen von Verträgen selbst festlegen können. Die Privatautonomie steht in Österreich im Verfassungsrang (Art 5 StGG; Art 1 1. ZP EMRK). Eine Regelung, die diese einschränken würde, darf nicht unverhältnismäßig sein. Hier ist besonders zu berücksichtigen, dass bei einer auf dem Markt frei verfügbaren Leistung, kein Ungleichgewicht zwischen der betroffenen Person und dem Verantwortlichen besteht, da die betroffene Person die Leistung jederzeit von einem anderen Unternehmen beziehen könnte und somit die Privatautonomie unverhältnismäßig eingeschränkt wird. Somit kann von einer Freiwilligkeit der Einwilligung der betroffenen Person ausgegangen werden, denn sie entscheidet wissentlich und willentlich frei, dass sie unter den Bedingungen einen Vertrag mit dem Verantwortlichen abschließen möchte. Anderenfalls hätte sie nicht seine Einwilligung erteilt.

Es ist festzuhalten und zu fordern, dass bisher gültige Einwilligungserklärungen auch nach dem 25. Mai 2018 weiterhin gültig sind.

Berechtigtes Interesse an einer Datenverarbeitung (Art 6 Abs 1lit f) DSGVO):

Gemäß Art 6 Abs 1 lit f DSGVO ist eine Verarbeitung auch rechtmäßig, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Dieses berechtigte Interesse wird im Erwägungsgrund 47 bzw. 48 der DSGVO auch hinsichtlich Direktwerbung und für Verantwortliche, die Teil einer Unternehmensgruppe sind, konkretisiert.

Insbesondere für Konzerngesellschaften ist dieser Rechtsgrund zur Datenverarbeitung wesentlich, sodass eine nähere Ausgestaltung und Konkretisierung im Datenschutz-Anpassungsgesetz 2018 aus unserer Sicht wünschenswert wäre.

III. Weitere allgemeine Anmerkungen

Einwilligung von Kindern in Bezug auf Dienste der Informationsgesellschaft:

Art 8 Abs 1 DSGVO enthält eine besondere Regelung für das einwilligungsfähige Alter von Kindern in Bezug auf Online-Dienste/ Dienste der Informationsgesellschaft. Hier wurde das einwilligungsfähige Alter mit 16 festgesetzt. Auf Grund einer vorhandenen Öffnungsklausel, kann diese Altersgrenze jedoch mittels nationaler Regelungen auch auf bis zu 13 Jahren abgesenkt werden. In Fällen in denen der Online-Dienst einem noch nicht einwilligungsfähigen Kind (im Sinne der DSGVO) angeboten wird, ist der Dienstanbieter dazu verpflichtet, angemessene Anstrengungen zu unternehmen um sich zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung erteilt wurde.

Die Beibehaltung der Grenze von 16 Jahren würde der bisherigen österreichischen Rechtskultur widersprechen und die unterschiedlichen Altersgrenzen auch erhebliche praktische Schwierigkeiten herbeiführen. So können mündige Minderjährige nach §§ 170 ff ABGB über Sachen, die ihnen zur freien Verfügung überlassen worden sind, und über Einkommen aus eigenem Erwerb insoweit verfügen und sich verpflichten, als dadurch nicht die Befriedigung seiner Lebensbedürfnisse gefährdet wird. Sie können sich zudem selbständig durch Vertrag zu Dienstleistungen verpflichten. **Die Geschäftsfähigkeit ist somit bereits ab 14 Jahren umfangreich ausgestaltet und sollte das datenschutzrechtliche Regime dem zivilrechtlichen gleichgeschalten sein.**
Es ist daher erforderlich, dass der österreichische Gesetzgeber von der Öffnungsklausel des Art 8 Abs 1 DSGVO Gebrauch macht und die Altersgrenze für Einwilligungen nach Art 8 DSGVO auf das vollendet vierzehnte Lebensjahr senkt.

Dies ist insbesondere auch für die Bewerbungen für Lehrstellen und Praktika mittels Mail oder online-Bewerbungsplattformen wichtig.
Auch könnte beispielsweise ein mündiger Minderjähriger einen Kontovertrag für ein Schülerkonto abschließen, mit dem zwingend eine Datenverarbeitung einhergeht, jedoch keine Einwilligung zur Datenverarbeitung ohne seinen gesetzlichen Vertreter erteilen. Diesen Widerspruch sowie die damit einhergehenden Schwierigkeiten bei der Umsetzung und Handhabung unterschiedlicher Rechte und Pflichten in der Praxis gilt es dringend aufzulösen.

Profiling:

Bereits 2016 wurde im Zuge einer parlamentarischen Anfrage (8039/J XXV. GP) zur Umsetzung der DSGVO darauf hingewiesen, dass die Existenz bewährter Geschäftsmodelle wie **„Profiling“** sichergestellt werden muss. Durch den jetzigen Entwurf wird diesem Wunsch keine Rechnung getragen.

Art 4 Abs 4 der DSGVO versteht unter "*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.

Artikel 22 der DSGVO legt ein Verbot von automatisierten Entscheidungen im Einzelfall einschließlich Profiling fest, wenn diese automatisierten Einzelentscheidungen/Profiling dem Betroffenen gegenüber rechtliche Wirkungen entfalten oder sie in ähnlicher Weise erheblich beeinträchtigt werden. Die bloße Einordnung in eine Marketing-Zielgruppe fällt jedenfalls nicht darunter.

Profiling zu Zwecken der Direktwerbung entfaltet gegenüber der betroffenen Person weder rechtliche Wirkung noch wird diese in ähnlicher Weise erheblich beeinträchtigt. Über diese Tatsache scheint jedoch Unklarheit zu herrschen. So ist die Datenschutzbehörde in ihrem jüngst publizierten Leitfaden davon ausgegangen, dass auch die Einordnung in eine **Marketing-Zielgruppe** unter den Artikel 22 DSGVO zu subsumieren wäre (und somit folglich grundsätzlich verboten wäre, außer einer der Erlaubnistatbestände des Abs 2 käme zur Anwendung).

Es stellt sich bei dieser Auslegungsvariante die Frage, wie die bloße Einordnung in eine Marketing-Zielgruppe der Person gegenüber rechtliche Wirkungen entfalten soll bzw sie in sonst ähnlicher Weise erheblich beeinträchtigt wird. Man beachte diesbezüglich auch die aktuelle Einschätzung der Artikel 29 Gruppe, welche selbst lediglich die Erstellung von

„behavioural or marketing profiles based on usage or navigation on its website“ und nicht allgemein die Einordnung in Marketing-Zielgruppen als besonders risikobehaftet ansieht (Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is *"likely to result in a high risk"* for the purposes of Regulation 2016/679). Selbst diese Einschätzung kann in Zweifel gezogen werden.

Auch wird im Erwägungsgrund 47 der DSGVO klar festgehalten, dass die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden kann. Auf Basis der DSGVO (Art 21) kann gegen Datenverarbeitungen für Zwecke der Direktwerbung und damit verbundenes Profiling weiters ein jederzeitiger Widerspruch ohne Angabe von Gründen erhoben werden. Zudem werden durch flankierende, telekommunikationsrechtliche Regelungen zum Schutz der Privatsphäre ohnehin unerwünschte Kontaktaufnahmen untersagt, weshalb sich die Einschätzung als risikobehaftet nicht teilen lässt.

Auf Grundlage der DSGVO handelt es sich bei der bloßen Einordnung in Marketing Zielgruppen oder die Einteilung der Kunden in Sinus Milieus somit gerade nicht um Profiling im Sinne des Artikels 22. Da jedoch die Datenschutzbehörde (als künftige Ermittlungs- und uU sogar Strafverfolgungsbehörde) dies anders auszulegen scheint, ist eine innerstaatliche Zulässigkeitsregelung bzw Definition welche automatisierten (Einzel)Entscheidungen (einschließlich Profiling) iSd Artikel 22 Abs 2 lit b DSGVO zulässig sind, erforderlich. Dies ist aus Gründen der Rechtssicherheit dringend geboten.

Zur Öffnungsklausel des Art 10 DSGVO (Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten):

„Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.“

Banken sind etwa auf Basis des § 16 Finanzmarkt-Geldwäschegesetz (FM-GwG) iVm § 41 BWG zur Meldung von strafrechtlich relevanten Sachverhalten an die Geldwäschemeldestelle verpflichtet. Diese Regelungen erlauben die Verarbeitung durch Meldung des KI an die Geldwäschemeldestelle. Es ist aber unklar, ob entsprechende geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen in ausreichender Form vorgesehen sind (allenfalls käme § 22 FM-GwG in Betracht). Eine Klarstellung in den Erläuterungen wäre sinnvoll.

Zum Beispiel verlangen Kreditgenossenschaften für ihre Aufsichtsräte und ehrenamtliche Vorstände im Rahmen eines sog **Fit & Proper-Tests** Strafregisterauszüge. Sollte diese Tätigkeit eine Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten darstellen, sehen wir nur für Aufsichtsratsmitglieder in § 28a BWG (wobei hier fraglich ist, ob dieser geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht) eine gesetzliche Grundlage. Es fehlt eine entsprechende Grundlage iSd Art 10 DSGVO für ehrenamtliche Vorstände.

Es ist derzeit noch fraglich, ob von Art 10 DSGVO auch Daten über den Verdacht der Begehung einer Straftat erfasst werden (vgl. *Feiler/Forgò*, EU-Datenschutz-Grundverordnung Art 10 Rz 1). Dies würde bedeuten, das Whistleblowing-Systeme bei denen derartige Verdachtsfälle erfasst werden können, grundsätzlich im Privatbereich unzulässig wären, es sei denn es gäbe eine innerstaatliche Regelung, welche dies erlaubt. Der derzeit vorliegende Entwurf sieht eine solche Regelung nicht vor. Wir geben dabei

folgendes zu bedenken: Aufgrund des US-amerikanischen Sarbanes Oxley Act (SOX) haben in den USA börsennotierte Unternehmen und Tochterfirmen verpflichtend interne Kontrollmaßnahmen (Whistleblowing-Systeme) einzuführen. Die Nichtzulassung von Whistleblowing-Systemen im privaten Bereich würde Österreich für in den USA börsennotierte Unternehmen standortpolitisch vollkommen unattraktiv machen, da sie entweder US-amerikanisches Recht oder österreichisches/europäisches Recht verletzen würden, je nachdem ob sie Whistleblowing-Systeme betreiben oder nicht. Dies vollkommen zwanglos, da das bisherige Whistleblowing-Regime in Österreich (durch das Erfordernis der betrieblichen Mitbestimmung als Absicherung) anstandslos funktioniert. Es wird daher eine entsprechende innerstaatliche Regelung gefordert, um eine Rechtsunsicherheit im Rahmen des Art 10 DSGVO auszuschließen.

Art 8 Abs 4 des geltenden DSG 2000 sollte entsprechend angepasst auch in das neue DSG aufgenommen werden.

Die Stellungnahme wird auch dem Präsidium des Nationalrates im Wege elektronischer Post an die Adresse begutachtungsverfahren@parlament.gv.at übermittelt.

Mit freundlichen Grüßen

Dr. Richard Schenz
Vizepräsident

Mag. Anna Maria Hochhauser
Generalsekretärin