VÖZ
VERBAND ÖSTERREICHISCHER ZEITUNGEN

An das Bundeskanzleramt - Verfassungsdienst

z.H. Sektionschef: Mag. Dr. Gerhard Hesse

Wien, am 22.06.2017

Stellungnahme: Datenschutz-Anpassungsgesetz 2018

Sehr geehrter Herr SC Dr. Hesse!

Wir bedanken uns für die Möglichkeit zur Stellungnahme zum oben bezeichneten Gesetzesentwurf und nehmen hierzu Stellung wie folgt:

1. Einleitende Anmerkungen zur Datenschutz-Grundverordnung

Vorweg müssen wir anmerken, dass wir die EU-Datenschutzgrundverordnung (nachfolgend: DSGVO), zu welcher der vorgelegte Begutachtungsentwurf in unmittelbarem Bezug steht, insgesamt als rechtsstaatlich besorgniserregend beurteilen. Die DSGVO wurde von manchen Experten als *eines der schlechtesten Gesetze des 21. Jahrhunderts*[1] bezeichnet – wesentlicher Kritikpunkt: Sie enthält zahlreiche Regelungen, denen es derart an Bestimmtheit fehlt, dass für den Rechtsunterworfenen unmöglich erkennbar ist, wo die Grenze zwischen gesetzeskonformem und gesetzwidrigem Verhalten verläuft.

Besonders krass lässt sich die rechtsstaatliche Bedenklichkeit der DSGVO am Zusammenspiel von Art. 25 DSGVO und Art. 83 DSGVO illustrieren: Art. 25 DSGVO verpflichtet im Wesentlichen zu „Datenschutz durch Technikgestaltung" und zu

[1] Vgl. https://www.heise.de/newsticker/meldung/Rechtsexperte-Datenschutz-Grundverordnung-als-groesste-Katastrophe-des-21-Jahrhunderts-3190299.html, abgerufen am 10.06.2017.

1013 Wien, Schottenring 12/Top 5 • Tel. +43 1 533 79 79-0 • E-Mail office@voez.at • ZVR-Zl 872763352
PRIVAT BANK der Raiffeisenlandesbank OÖ • IBAN AT50 3400 0000 0721 9660 • BIC RZOOAT2L • UID-Nr ATU38643802

‚datenschutzfreundlichen Voreinstellungen". Welche konkreten Maßnahmen dies im Einzelnen umfasst, ist jedoch nicht geregelt – offenbar konnte man sich im demokratischen Prozess nicht auf konkrete Pflichten und Verbote einigen. Stattdessen wird lediglich abstrakt und kryptisch auf ‚geeignete technische und organisatorische Maßnahmen" verwiesen und als (einziges) Beispiel Pseudonymisierung genannt. Welche Maßnahmen also konkret *geeignet* und damit rechtlich erforderlich sind, hat der Rechtsunterworfene somit selbst herauszufinden. Dabei muss er folgende, jeweils nicht quantifizierte Faktoren berücksichtigen:

- Stand der Technik;
- Implementierungskosten;
- Art, Umfang, Umstände und Zwecke der Verarbeitung;
- Eintrittswahrscheinlichkeit;
- Schwere der mit der Verarbeitung verbundenen Risiken.

Es ist offenkundig, dass es unmöglich ist, anhand einer solchen Regelung abschließend zu beurteilen, wann man sich rechtskonform verhält und wann rechtswidrig. Mit dieser Beurteilung wird der Rechtsunterworfene letztlich an nichtstaatliche Einrichtungen verwiesen: Ein genehmigtes Zertifizierungsverfahren, dem man sich unterziehen kann, soll als ‚Faktor" herangezogen werden können, um die Erfüllung der Pflichten nach Art. 25 DSGVO zu beurteilen. Die letztgenannte Regelung lässt erahnen, dass den Verordnungsgebern die fehlende Determiniertheit der von ihnen geschaffenen Regelungen durchaus bewusst war.

Ein Verstoß gegen die undeterminierte Anordnung des Art. 25 Abs. 1 wird sodann in Art. 83 DSGVO mit Geldbußen von bis zu zehn Millionen Euro oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs bedroht, und zwar *je nachdem, welcher der Beträge höher ist*. Mit anderen Worten: Rechtlich möglich ist künftig, dass selbst über ein Kleinstunternehmen, sogar über ein EPU, für die Verletzung des Art. 25 Abs. 1 DSGVO Geldbußen in der Höhe von bis zu zehn Millionen Euro verhängt werden; selbst wenn dieser Betrag ein Vielfaches des weltweiten Jahresumsatzes des bestraften Unternehmens darstellt.

Mit dieser Konstruktion wird jedenfalls für kleine und mittelständische Unternehmen eine potenziell existenzbedrohende Sanktion in der Rechtsordnung der Europäischen Union verankert: Eine Geldbuße von zehn Millionen Euro beträgt für KMUs regelmäßig nicht 2 %, sondern ein Vielfaches des Jahresumsatzes und würde für kleine oder mittelständische Unternehmen regelmäßig in die Insolvenz führen – für den höheren Strafrahmen (20 Millionen Euro bzw. 4% des Umsatzes, höhere Betrag ist Obergrenze) gilt dies umso mehr. Zugleich wird der von bloßer Verwarnung bis zur Verhängung

solcher Höchststrafen reichende Sanktionsradius in das Ermessen einer Verwaltungsbehörde gestellt. Jedes Unternehmen wird sich hüten, einer Anordnung einer mit derartiger Sanktionskompetenz für derart unbestimmte Verhaltensanordnungen ausgestatteten Verwaltungsbehörde zu widersprechen, selbst wenn solche Anordnungen im Einzelfall als unverhältnismäßig, willkürhaft oder sonst rechtswidrig erlebt werden.

Dass diese Sanktionskonstruktion der DSGVO letztlich auch von denselben politischen Kräften vollinhaltlich mitgetragen wurde, die in Richtung einzelner EU-Mitglieder und Drittstaaten oft zu Recht ihre Sorgen über die Aushöhlung des Rechtsstaats geäußert haben, hinterlässt uns als Unternehmer-Interessenvertretung der österreichischen Zeitungsmedienunternehmen in großer Ratlosigkeit. Zu den kleinen und mittelständischen Unternehmen, denen hier die rechtliche Möglichkeit einer Insolvenzherbeiführung als Sanktion für Verstöße gegen das zukünftige Datenschutzrecht in Aussicht gestellt wird, zählen nämlich auch praktisch alle Mitglieder des Verbands Österreichischer Zeitungen. Dass das beschriebene Regelungskonstrukt damit auch ein grundsätzlich geeignetes Instrument ist, eine kritische freie Presse zu erheblicher Zurückhaltung bei personenbezogener Berichterstattung zu veranlassen, und damit drastisch in die Kommunikations- und Pressefreiheit einzugreifen, muss nicht gesondert erwähnt werden.

Wir gehen davon aus, dass jedenfalls die genannten Bestimmungen der DSGVO einer Überprüfung auf Verhältnismäßigkeit nach Art. 49 GRC bzw. auf Determiniertheit nach Art. 7 EMRK nicht standhalten werden. Bis zur absehbaren Aufhebung dieser Bestimmungen sehen wir die **Aufgabe des österreichischen Gesetzebers darin, die Öffnungsklauseln zur maximalen Schadensbegrenzung für die österreichische Medienwirtschaft und zum Schutz des österreichischen Rechtsstaats vor der Aushöhlung wesentlicher Prinzipien zu nützen**:

- Determinierungsgebot,
- Verhältnismäßigkeitsgrundsatz,
- Legalitätsprinzip,
- Kommunikationsfreiheit.

2. Meinungsäußerungs- und Informationsfreiheit der Medien: Art. 85 DSGVO und § 27 des vorgelegten Begutachtungsentwurfes

Die durch die DSGVO bewirkte Beeinträchtigung der Meinungsäußerungs- und Informationsfreiheit war dem Verordnungsgeber bewusst: In Art. 85 Abs. 1 DSGVO wurde daher geregelt, dass die Mitgliedstaaten durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß der DSGVO mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang zu bringen haben.

Insbesondere sollen die Mitgliedstaaten auch für Datenverarbeitung zu journalistischen Zwecken weitreichende Abweichungen oder Ausnahmen vorsehen, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen. Es ist hervorzuheben, dass Art. 85 Abs. 1 und 2 nicht als Kann-Bestimmungen formuliert sind und daher Pflicht eines jeden Mitgliedstaates sind. In Bezug auf das den österreichischen Gesetzgeber bindende Determinierungsgebot bedeutet dies insbesondere auch: Der Gesetzgeber hat das Kriterium „wenn dies erforderlich ist" durch klare Aussagen zur Abgrenzung der Anwendbarkeit bzw. Nichtanwendbarkeit der DSGVO auf journalistische Tätigkeit auszugestalten.

Diesem Erfordernis wird der vorgelegte Begutachtungsentwurf nicht gerecht. Art. 2 § 27 des vorgelegten Entwurfes lautet:

> ***Soweit dies erforderlich ist**, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen, finden von der DSGVO die Kapitel II (Grundsätze), mit Ausnahme des Art. 5, Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), mit Ausnahme der Art. 28, 29 und 32, Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehörden), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besondere Verarbeitungssituationen) auf die Verarbeitung, die **zu journalistischen Zwecken** oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, **keine Anwendung**. Von den Bestimmungen dieses Bundesgesetzes ist in solchen Fällen nur § 6 (Datengeheimnis) anzuwenden.*

In den Erläuterungen ist dazu ausgeführt:

> *... Inhaltlich sollen damit weitgehend die von § 48 DSG 2000 (Anm.: weitgehende Ausnahme für publizistische Tätigkeiten) vorgesehenen Ausnahmen für derartige Verarbeitungen erhalten bleiben. Von den Bestimmungen dieses Bundesgesetzes ist nur § 6 (Datengeheimnis) anzuwenden; davon unberührt bleibt die Anwendung des verfassungsrechtlich verankerten Grundrechts auf Datenschutz gemäß § 1. Für Verarbeitungen, die dem Mediengesetz (MedienG), BGBl. Nr. 314/1981, unterliegen, gelten die Vorschriften des MedienG auch ohne ausdrückliche Anordnung.*

Nun ist es zwar richtig, dass für Verarbeitungen, die dem Mediengesetz unterliegen, dessen Vorschriften auch ohne ausdrückliche Anordnung gelten; allerdings wird damit nicht die durch § 48 DSG 2000 vorgenommene Systematik erhalten, wonach das Mediengesetz für diese Verarbeitungen die Anwendbarkeit des Datenschutzrechts weitgehend verdrängt. § 48 DSG 2000 sieht nämlich bisher vor,

- dass für publizistische Tätigkeit im Sinne des Mediengesetzes ohne Wenn und Aber nur §§ 4 bis 6, 10, 11, 14 und 15 des DSG 2000 anzuwenden sind – **alle übrigen Bestimmungen des DSG 2000 auf publizistische Tätigkeiten im Sinne des Mediengesetzes also ausdrücklich und ausnahmslos unanwendbar sind**; und

- dass die Verwendung von Daten für publizistische Tätigkeiten im Sinne des Mediengesetzes insoweit explizit zulässig ist, als dies zur Erfüllung der Informationsaufgabe der Medienunternehmer, Mediendienste und ihrer Mitarbeiter in Ausübung des Grundrechtes auf freie Meinungsäußerung gemäß Art. 10 Abs. 1 EMRK erforderlich ist.

Beide dieser sehr klaren und wesentlichen Aussagen zum Verhältnis von Datenschutz und Medienrecht, sind in Art. II § 27 des vorgelegten Entwurfes verlorengegangen. Es wird lediglich die für den Rechtsunterworfenen wenig Klarheit bringende Formel aus Art. 85 Abs. 2 DSGVO übernommen, und normiert, dass bestimmte Kapitel der DSGVO unanwendbar sind, *„soweit dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen"*. Was dies für die Abgrenzung zwischen Datenschutzrecht und Medienrecht konkret bedeuten soll, bleibt – ganz im Stil der DSGVO – offen.

Eine Anwendbarkeit der in Art. 85 Abs. 2 DSGVO genannten Kapitel der DSGVO auf journalistische Tätigkeit und Medienberichterstattung hätte insbesondere folgenden Konsequenzen:

- Es würde grundsätzlich eine **Parallelzuständigkeit der Datenschutzbehörde** für Sachverhalte begründet, die bisher ausschließlich in die Zuständigkeit der Mediengerichtsbarkeit fallen;

- Medienberichterstattung und journalistische Recherche könnten grundsätzlich zum Gegenstand der **Geldbußen** werden, welche Art. 83 DSGVO in existenzvernichtender Höhe androht;

- Die klar abgegrenzten **Tatbestände für medienrechtliche Entschädigungen** für erlittene Kränkungen würden durch den allgemeinen Anspruch auf Ersatz immaterieller Schäden nach Art. 82 Abs. 1 DSGVO verwässert, die **Höchstbetragsgrenzen** nach Mediengesetz obsolet.

Zur Vermeidung dieser nachteiligen Folgen für eine freie Presse empfehlen wir dringend folgende Neufassung des vorgeschlagenen Art. II § 27:

Freiheit der Meinungsäußerung und Informationsfreiheit

§ 27. (1) Die Verarbeitung von Daten zum Zwecke der Veröffentlichung von Inhalten in periodischen Medien von Medienunternehmen, Mediendiensten oder Medieninhabern im Sinne des Mediengesetzes ist insoweit zulässig, als dies zur Erfüllung der Informationsaufgabe der Medienunternehmer, Mediendienste und ihrer Mitarbeiter in Ausübung des Grundrechtes auf freie Meinungsäußerung gemäß Art. 10 Abs. 1 EMRK erforderlich ist.

(2) Um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen finden Kapitel II (Grundsätze), mit Ausnahme des Art. 5, Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), mit Ausnahme der Art. 28, 29 und 32, Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehörden), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besondere Verarbeitungssituationen) auf Veröffentlichungen in dem Mediengesetz unterliegenden periodischen Medien keine Anwendung.

(3) Um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen finden die in Abs. 2 genannten Kapitel der DSGVO weiters keine Anwendung auf die Verarbeitung personenbezogener Daten zu durch Art. 10 Abs. 1 EMRK gerechtfertigten literarischen sowie durch § 17a StGG gerechtfertigten künstlerischen Zwecken.

3. Verarbeitung personenbezogener Daten im Beschäftigungskontext

In § 29 des vorgelegten Entwurfes ist normiert, dass das Arbeitsverfassungsgesetz (ArbVG) eine Vorschrift im Sinne des Art. 88 DSGVO ist – also die dortigen datenschutzrechtlichen Regelungen betreffend Arbeitnehmer die Anwendung der DSGVO verdrängende speziellere Regelungen sind.

Vor diesem Hintergrund wäre es zur Vermeidung von Zersplitterung und Redundanz empfehlenswert, auf parallele arbeitsrechtliche Regelungen im vorgeschlagenen DSG 2018 zu verzichten und diese Regelungen ausschließlich in arbeitsrechtlichen Gesetzen, insbes. im ArbVG zu verankern.

4. Bildverarbeitung

Das DSG 2000 enthält Vorschriften betreffend Video*überwachung*, also systematische und fortlaufende Feststellung von Ereignissen, betreffend ein überwachtes Objekt oder eine überwachte Person, durch technische Bildaufnahme- oder Bildübertragungsgeräte.

Mit dem vorgelegten Entwurf soll ein Regelungskomplex für jede Art von Bildaufnahme, einschließlich begleitender Tonaufzeichnung, geschaffen werden, wobei jede Bildaufnahme außerhalb des privaten Bereichs ungeachtet der Frage ihrer (Nicht)Veröffentlichung einer spezifischen

- Rechtfertigung,
- Protokollierung und
- Ersichtlichmachung des Verantwortlichen in der Bildaufnahme durch Kennzeichnung

bedarf. Gemäß dem Wortlaut des § 30 Abs. 1 des Entwurfes gilt das Rechtfertigungserfordernis selbst für Bildaufnahmen, auf welchen keine Person

ersichtlich ist (wobei Voraussetzung unter Berücksichtigung des in Art. II § 2 definierten Anwendungsbereiches wohl ein dennoch bestehender Personenbezug sein muss).

Die Regelungen erscheinen überschießend, erhebliche Rechtsunsicherheit und übertriebenen Verwaltungsaufwand in Bezug auf die Anfertigung von Bildaufnahmen im öffentlichen Raum ist zu befürchten. Auch diese Regelung zeigt deutlich auf, dass eine klare Abgrenzungsregelung im Hinblick auf journalistische Tätigkeit erforderlich ist. Die Anwendung der vorgeschlagenen Regelung auf Fotojournalismus würde eine erhebliche und unverhältnismäßige Beeinträchtigung der Kommunikations- und Pressefreiheit mit sich bringen.

Der vorgeschlagene Art. II § 30 muss auf Fotojournalismus (Anfertigung von Abbildungen für publizistische Tätigkeit bzw. mediale Berichterstattung) im Rahmen einer klaren generellen Regelung (vgl. Punkt 2.) im selben Maße für unanwendbar erklärt werden, wie dies für sonstige Verarbeitungsvorgänge für Veröffentlichungen in periodischen Medien im Sinne des Mediengesetzes erforderlich ist.

5. Befugnisse der Datenschutzbehörde

Der Datenschutzbehörde werden durch die DSGVO und durch § 11 des vorgelegten Entwurfes erhebliche, das Hausrecht beeinträchtigende und polizeiartige Kompetenzen eingeräumt, darunter das Recht zur Betretung von Räumen, Inbetriebsetzung von Datenverarbeitungsanlagen und zur Anfertigung von Kopien von Datenträgern.

Die Untersuchungs- und Betretungsrechte der Datenschutzbehörde sind mit dem durch Art 10 EMRK garantierten Schutz journalistischer Quellen und dem in § 31 Mediengesetz verankerten Redaktionsgeheimnis-Umgehungsschutz unvereinbar. Auch diese Regelung zeigt deutlich auf, dass die in Punkt 2. näher behandelte Regelung betreffend die Beziehung zwischen dem neuen Datenschutzrecht und dem Medienrecht dringend im dort beschriebenen Sinne präzisiert werden muss. Mindestgebot ist unseres Erachtens ein klarer Verweis auf die Beschränkung der Befugnisse der Datenschutzbehörde durch das Redaktionsgeheimnis.

6. Rückwirkung

Gemäß § 76 Abs. 4 DSG 2018 sind zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes bei der Datenschutzbehörde oder bei den ordentlichen Gerichten zum DSG 2000 *anhängige Verfahren nach den Bestimmungen des DSG 2018 und der*

DSGVO fortzuführen, mit der Maßgabe, dass die Zuständigkeit der ordentlichen Gerichte aufrecht bleibt. Gemäß Art. 2 § 76 Abs. 5 des vorgelegten Entwurfes sind *Verletzungen des DSG 2000, die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes noch nicht anhängig gemacht wurden, sind nach der Rechtslage nach Inkrafttreten dieses Bundesgesetzes zu beurteilen.* Mit diesen Bestimmungen wird normativ die Rückwirkung der Datenschutzgrundverordnung und des DSG 2018 angeordnet: Wird eine Verletzung erst nach Inkrafttreten des DSG 2018 anhängig gemacht, so wäre das zugrundeliegende Verhalten gemäß dem vorgeschlagenen § 76 Abs. 5 DSG 2018 selbst dann nach der neuen Rechtslage zu beurteilen, wenn es vor deren Inkrafttreten gesetzt wurde. Damit könnten Verhaltensweisen nachträglich pönalisiert werden, welche nach der alten Rechtslage überhaupt nicht tatbestandsmäßig waren. Eine solche Regelung ist rechtsstaatlich höchst bedenklich.

In diesem Zusammenhang ist auch darauf hinzuweisen, dass die Erläuterungen zu Art. II § 76 im Widerspruch zum klaren Wortlaut des Art. II § 76 Abs. 4 und 5 stehen. In den Erläuterungen heißt es: Ein strafbarer Tatbestand, der vor dem Inkrafttreten dieses Bundesgesetzes verwirklicht wurde, ist *nach jener Rechtslage zu beurteilen, die für den Täter in ihrer Gesamtauswirkung günstiger ist.* Eine solche Regelung wäre wünschenswert, ist dem normativen Text des vorgelegten Entwurfes aber tatsächlich nicht zu entnehmen.

Wir empfehlen Art. II § 76 Abs. 4 und 5 durch folgende Regelung zu ersetzen: Sachverhalte, die vor dem Inkrafttreten dieses Bundesgesetzes verwirklicht wurden, sind nach jener Rechtslage zu beurteilen, die für Verantwortlichen und Auftragsverarbeiter in ihrer Gesamtauswirkung günstiger ist.

7. Weitergeltung von Zustimmungserklärungen

Was die Frage der Weitergeltung bereits vor Geltung der DSGVO erteilter Einwilligungserklärungen anbelangt, droht erhebliche Rechtsunsicherheit, der durch diesen Passus in den Erläuterungen nicht adäquat entgegengewirkt wird. So wird der Aspekt der Weitergeltung erteilter Einwilligungserklärungen nur in einem Erwägungsgrund der DSGVO adressiert (ErwGr 171). Darin wird zwar grundsätzlich deren Weitergeltung zugesagt, wobei darauf abgestellt wird, dass "*die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht*". Die Bestimmungen im normativen Teil der DSGVO zur Einwilligungserklärung (Art. 4 Z 11, Art. 7 Abs. 2 und Abs. 4) sind großteils vage formuliert und daher auslegungsbedürftig.

Was die Weitergeltung bereits erteilter Einwilligungserklärungen betrifft, hat der nationale Gesetzgeber daher insbesondere aus verfassungsrechtlichen Gründen (siehe

dazu nachstehend) für eine Klarstellung im Sinne der Rechtssicherheit für die Normunterworfenen zu sorgen. Durch den Verweis auf ErwGr 171 DSGVO in den Erläuterungen zu § 76 wird dieser Notwendigkeit aus unserer Sicht nicht Genüge getan. Vielmehr sollte der Gesetzgeber auf die bisherige Rechtslage und die von den Höchstgerichten in ständiger langjähriger Rechtsprechung entwickelten inhaltlichen Anforderungen bei der Einholung von Einwilligungserklärungen abstellen. Diese sind im Wesentlichen eine leicht zugängliche, klare und transparente Information, welche Datenarten zu welchem Zweck verarbeitet werden, an wen allenfalls Daten übermittelt werden und welche Daten der Übermittlungsempfänger zu welchen Zwecken verarbeitet, sowie ein leicht zugänglicher, klarer und transparenter Hinweis, dass die Einwilligung jederzeit widerrufen werden kann, wie dieser Widerruf erfolgen kann und dass er sich nicht auf die Vertragserfüllung auswirkt.

Notwendig ist daher eine Bestimmung in § 76, wonach Einwilligungserklärungen, die der Rechtslage und der höchstgerichtlichen Judikatur unter dem DSG 2000 entsprachen, weitergelten.

Dies aus folgenden Gründen:

- Aus dem verfassungsrechtlichen Gleichbehandlungsgrundsatz ergibt sich ein Vertrauensschutz, demzufolge bei "*plötzlich eintretenden Eingriffen in erworbene Rechtspositionen, auf deren Bestand der Normunterworfene mit guten Gründen vertrauen konnte*"[1] die Gravität des Eingriffs sowie das Gewicht der für diesen Eingriff sprechenden Gründe zu beachten sind, damit dieser zulässig ist[2]. Auch das Unionsrecht enthält einen Gleichbehandlungsgrundsatz in Art 20 der Grundrechtecharta. Das bisherige Datenschutzrecht hatte nun fast zwei Jahrzehnte Bestand und es hat sich eine ständige höchstgerichtliche Rechtsprechung insbes. zur Wirksamkeit von Einwilligungserklärungen entwickelt. Im Vertrauen auf diesen Bestand haben Unternehmen durch Einholung von dieser Rechtsprechung entsprechenden Einwilligungserklärungen "Investitionen" getätigt. Auf wohlerworbene Rechte ist entsprechend Rücksicht zu nehmen.

- Hierfür spricht ferner das verfassungsrechtlich geschützte Prinzip der Privatautonomie[3], welches auch in der freiwilligen Erteilung von Einwilligungen und damit der Verfügung über das persönliche "Dateneigentum" Ausdruck findet. Würden diese Einwilligungen kraft gesetzgeberischer Anordnung plötzlich ihre

[1] VfGH 05.10.1989, G 228/89 = VfSlg. 12.186/1989.
[2] Vgl VfGH 25.06.1998, G 384/96 = VfSlg. 15.231/1998.
[3] Art 5 StGG; Art 1 1. ZP ERMK.

Gültigkeit verlieren, so würde damit auch die Privatautonomie unverhältnismäßig eingeschränkt werden.[4]

- Die Weitergeltung bereits erteilter Einwilligungen hat auch für die betroffenen Personen positive Auswirkungen. Zum einen werden sie so nicht durch eine erneute Bitte um Einwilligung belästigt;[5] der Schutz vor Belästigungen ist seit längerem schon ein wichtiges Anliegen des Gesetzgebers.[6] Zum anderen würde sich ihre Situation nicht ändern, weil ihnen nach wie vor das Recht zukommt, ihre Einwilligung jederzeit zu widerrufen. Der Widerruf der Einwilligung und die erneute Erteilung sind hier also funktional äquivalent, weil ohnehin bereits eine Datenverarbeitung stattgefunden hat. Dies z.T. sogar über einen recht langen Zeitraum, währenddessen die Datenverarbeitung unwidersprochen geblieben ist.

  So sind etwa in Art 6 Abs 4 DSGVO "*die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen*" (lit d leg cit) zu berücksichtigen. Die Bestimmung gilt zwar nur für den Fall, dass sich der Zweck einer Datenverarbeitung ändert. Wenn geringe Folgen für die betroffenen Personen sogar eine Zweckänderung ermöglichen, dann muss umso mehr die bloße Weitergeltung der Einwilligungserklärung angenommen werden.

- Durch die derzeit geltende Rechtslage und höchstgerichtliche Judikatur wurden schon bisher hohe datenschutzrechtliche Anforderungen an eine wirksame Einwilligungserklärung gestellt. So wurde etwa die Freiwilligkeit der Einwilligung, die in Art 7 Abs 4 DSGVO gefordert wird, schon bisher in Österreich sowohl datenschutzrechtlich (§ 4 Z 14 DSG 2000) als auch verbraucherrechtlich durch das in § 6 Abs 3 KSchG geregelte Transparenzgebot sichergestellt. Auch dass die Datenverarbeitung – wie bereits erwähnt – in vielen Fällen lange unwidersprochen geblieben ist, indiziert Freiwilligkeit zum Zeitpunkt der erstmaligen Erteilung und weiterhin bestehende Einwilligung in die Datenverarbeitung.

- Letztlich ist auch darauf hinzuweisen, dass der nationale Gesetzgeber in Art 2 § 3 DSAG eine Durchführungsbestimmung vorgesehen hat, welche von der DSGVO nicht vorgesehen ist.[7] Demnach muss eine Berichtigung oder Löschung personenbezogener Daten nicht unverzüglich erfolgen, wenn dies aus Gründen der Wirtschaftlichkeit nicht möglich ist. Die Regelung ist sinnvoll und sachgerecht. Ihre

[4] Ähnl bereits die Stellungnahme von A1 (9/SN-322/ME), Seite 7.
[5] In diesem Sinne auch die Stellungnahmen von A1 (9/SN-322/ME), Seite 1 und von Oesterreichs Energie (18/SN-322/ME), Seite 7.
[6] Vgl. etwa § 107 Abs 2 TKG.
[7] Vgl dazu Seite 4 der EB.

ratio ist jedoch noch weitergehender anzuwenden und insb. auf den hier angesprochenen Fall der Weitergeltung von Einwilligungserklärungen zu übertragen: So wie es nicht erwartet werden kann, dass verteilt gespeicherte Daten unverzüglich gelöscht werden,[8] kann auch nicht erwartet werden, dass jahrelang unbeanstandet und rechtmäßig verarbeitete Daten von einem Tag auf den anderen gar nicht mehr verarbeitet werden (oder eine solche Verarbeitung mit Rechtsunsicherheit behaftet ist). Dem steht die Harmonisierungswirkung durch die DSGVO ebensowenig entgegen wie im Zusammenhang mit Art 2 § 3 DSAG.

Abschließend darf noch angemerkt werden, dass eine Klarstellung bezüglich der Weitergeltung bereits erteilter Einwilligungen schon mehrfach im Rahmen des Begutachtungsprozesses angeregt wurde.[9] Hinsichtlich der konkreten Fomulierung erlauben wir uns aus den oben genannten Gründen die Einfügung folgenden Absatzes in Art 2 § 76 DSAG vorzuschlagen:

(x) Vor dem Zeitpunkt des Inkrafttretens dieses Bundesgesetzes rechtswirksam erteilte Einwilligungen in Datenverarbeitungen behalten ihre Gültigkeit.

Wir ersuchen dringend um Berücksichtigung unserer Anmerkungen und stehen zu deren Erörterung jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

Mag. Gerald Grünberger
(Verbandsgeschäftsführer)

[8] Siehe dazu das Bsp. auf Seite 4 der EB: "*Insbesondere bei einer etwa aus Sicherheitsgründen weit verteilten Speicherung von personenbezogenen Daten kann es sich im Einzelfall als schwierig erweisen, einzelne Datensätze sofort aus sämtlichen Kopien zu entfernen*".

[9] Siehe die Stellungnahmen von A1 (9/SN-322/ME), Seite 1, 6 ff und von Oesterreichs Energie (18/SN-322/ME), Seite 7.