Erläuterungen

Allgemeiner Teil

Hauptgesichtspunkte des Entwurfs:

Die Verordnung (EU) 2021/784 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Bekämpfung der Verbreitung terroristischer Online-Inhalte (im Folgenden kurz: Verordnung) ist verbindlich und gilt ab dem 7. Juni 2022 unmittelbar in jedem Mitgliedstaat.

Durch diese Verordnung soll das reibungslose Funktionieren des digitalen Binnenmarkts in einer offenen und demokratischen Gesellschaft gewährleistet werden, indem der Missbrauch von Hostingdiensten für terroristische Zwecke bekämpft und ein Beitrag zur öffentlichen Sicherheit in der gesamten Union geleistet wird. Neben dem Schutz der öffentlichen Sicherheit sollen gleichzeitig angemessene und solide Vorkehrungen zum Schutz der Grundrechte (bspw. Recht auf Achtung des Privatlebens, auf den Schutz personenbezogener Daten, auf Meinungsfreiheit, auf unternehmerische Freiheit und auf wirksamen Rechtsbehelf) getroffen werden.

In Bezug auf EU-Verordnungen hat der EuGH festgestellt, dass ein prinzipielles unionsrechtliches Verbot der Änderung, Ergänzung oder Präzisierung durch verbindliches innerstaatliches Recht besteht (EuGH 18.2.1970, Rs. 40/69, *Bollmann*, Rz. 4; 31.1.1978, Rs. 94/77, *Zerbone*, Rz. 22/27). Der Umstand, dass eine Regelung in einem unmittelbar anwendbaren Unionsrechtsakt enthalten ist, bedeutet gleichwohl nicht notwendigerweise, dass jede nationale Maßnahme in diesem Bereich verboten wäre (EuGH 21.12.2011, Rs. C-316/10, *Danske Svineproducenter*, Rz. 42). Insb. dürfen nach der Rechtsprechung staatliche Vorschriften im Interesse ihres inneren Zusammenhangs und ihrer Verständlichkeit für die Adressaten bestimmte Punkte der EU-Verordnungen wiederholen (EuGH 28.3.1985, Rs. 272/83, *Kommission/Italien*, Rz. 27). Durchführungsmaßnahmen wie etwa im vorliegenden Fall betreffend Behördenzuständigkeit und Strafen sind zulässig und mitunter auch unionsrechtlich geboten. Die innerstaatliche Durchführung hat sich allerdings zwingend auf jene Bereiche zu beschränken, die durch die Verordnung nicht determiniert und zum innerstaatlichen Vollzug erforderlich sind. Jüngst wurden diese Grundsätze vom EuGH im Urteil vom 25.11.2021, Rs. C-372/20, *Finanzamt für den 8., 16. und 17. Bezirk in Wien*, Rz. 47 f in Erinnerung gerufen:

„*47 Insoweit erscheint es angebracht, darauf hinzuweisen, dass* […] *Verordnungen zwar aufgrund ihrer Rechtsnatur und ihrer Funktion im Rechtsquellensystem des Unionsrechts im Allgemeinen unmittelbare Wirkung in den nationalen Rechtsordnungen haben, ohne dass nationale Durchführungsmaßnahmen erforderlich wären, es jedoch vorkommen kann, dass manche Verordnungsbestimmungen* […] *des Erlasses von Durchführungsmaßnahmen durch die Mitgliedstaaten bedürfen* […]

48 Die Mitgliedstaaten können [solche] *Maßnahmen* […] *dann erlassen, wenn sie deren unmittelbare Anwendbarkeit nicht vereiteln, deren gemeinschaftliche Natur nicht verbergen und die Ausübung des durch die betreffende Verordnung verliehenen Ermessens innerhalb der Grenzen dieser Vorschriften konkretisieren* […].“

Nach Art. 12 der Verordnung sind die zuständigen Behörden zu benennen, die die Aufgaben nach den Art. 3, 4, 5 und 18 vollziehen werden. Wie einleitend erwähnt, ist die Verordnung am 7. Juni 2022 in Kraft getreten.

Näher betrachtet sieht die Verordnung im Wesentlichen Folgendes vor:

- Entfernungsanordnungen (Art. 3 und 4)

Behörden jedes Mitgliedstaates können Entfernungsanordnungen erlassen, wodurch die Hostingdiensteanbieter verpflichtet werden, in allen Mitgliedstaaten terroristische Inhalte innerhalb einer Stunde nach Erhalt der Entfernungsanordnung zu entfernen. Die Behörden des Herkunftslandes können Anordnungen aus anderen Mitgliedstaaten überprüfen.

- Spezifische Maßnahmen (Art. 5)

Wenn ein Anbieter terroristischen Inhalten ausgesetzt ist, hat er spezifische Maßnahmen zu ergreifen, wobei es ihm zunächst freisteht, welche Maßnahmen er ergreift, so zB:

- geeignete technische und operative Maßnahmen oder Kapazitäten, um terroristische Inhalte zu ermitteln und unverzüglich zu entfernen;
- Meldemechanismen für Nutzer;
- Mechanismen zur stärkeren Sensibilisierung für terroristische Inhalte;

- Beschwerdemechanismus für Inhalteanbieter, deren Inhalte aufgrund spezifischer Maßnahmen entfernt oder gesperrt wurden.

 Rechtsbehelfe (Art. 9)

Sowohl Hostingdiensteanbieter als auch Inhalteanbieter haben das Recht auf einen wirksamen Rechtsbehelf gegen Entscheidungen, die sie auf Grundlage dieser Verordnung erhalten haben. Dies beinhaltet das Recht, die Entscheidungen vor den Gerichten des für die Vollzugsbehörde zuständigen Mitgliedstaats, die die Entscheidung erlassen hat, anzufechten.

 Sanktionsvorschriften (Art. 18)

Die Verordnung gibt vor, dass für diverse – taxativ angeführte – Verstöße seitens der der Rechtshoheit des betreffenden Mitgliedstaates unterliegenden Diensteanbieter auf nationaler Ebene entsprechende Sanktionsbestimmungen erlassen werden und wirksame, verhältnismäßige und abschreckende Sanktionen zu verhängen sind sowie alle für die Anwendung der Sanktionen erforderlichen Maßnahmen getroffen werden.

Allfällige weitere Maßnahmen zur Bekämpfung der Verbreitung terroristischer Online-Inhalte – auf legislativer, nichtlegislativer und freiwilliger Basis – bleiben durch diesen Entwurf unberührt (siehe dazu die ErwG 2 und 3 der Verordnung)

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung dieses Bundesgesetzes gründet sich auf Art. 10 Abs. 1 Z 9 BVG („Post- und Fernmeldewesen“), auf Art. 10 Abs. 1 Z 6 B-VG („Pressewesen“), Art. 10 Abs. 1 Z 7 B-VG („Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“) und – soweit es die von Art. 12 iVm. Art. 13 Abs. 2 der Verordnung vorausgesetzte Betrauung einer unabhängigen Einrichtung betrifft – ergänzend auch auf Art. 20 Abs. 2 Z 8 BVG („nach Maßgabe des Rechts der Europäischen Union geboten“).

Zu Art. 1 (Terrorinhalte-Bekämpfungs-Gesetz)

Besonderer Teil

Zu § 1:

Die Bestimmung formuliert in der Art einer Zusammenfassung als grundsätzliche Orientierungslinie die Ziele des Gesetzesvorhabens. Die Formulierung in Abs. 2 orientiert sich an den Überlegungen in ErwG 1 bis 3 der Verordnung.

Definitionen:

Die mit diesem Gesetzesvorhaben durchgeführte Verordnung legt bei ihren Vorgaben folgende Begriffsbestimmungen (vgl. Art. 2 der Verordnung) zugrunde:

„*Hostingdiensteanbieter*“ bezeichnet einen Anbieter von Diensten der Informationsgesellschaft, dh. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellem Abruf eines Empfängers erbrachte Dienstleistung (die Verordnung verweist diesbezüglich auf Art. 1 lit. b der Richtlinie (EU) 2015/1535), wenn diese darin besteht, die durch einen „*Inhalteanbieter*“ bereitgestellten Informationen im Auftrag eines Inhalteanbieters zu speichern.

Unter dem Begriff „speichern“ ist nach ErwG 13 der Verordnung die Aufbewahrung von Daten im Speicher eines physischen oder virtuellen Servers zu verstehen. Anbieter von „reinen Durchleitungsdiensten“, von „Cachingdiensten“ oder von anderen Diensten, die auf anderen Ebenen der Internet-Infrastruktur geleistet werden, die keine Speicherung beinhalten, wie Register und Registrierungsstellen, sowie Anbieter von Domain-Namen-Systemen (DNS) oder von Zahlungsdiensten oder Anbieter von Schutzdiensten gegen DDoS (Distributed Denial of Service/verteilter Dienstverweigerungsangriff) sollten daher nicht in den Anwendungsbereich dieser Verordnung fallen.

Der aus Art. 1 lit. b der Richtlinie (EU) 2015/1535 stammende Begriff der „*Dienste der* Informationsgesellschaft“ findet sich in der österreichischen Rechtsordnung bereits in zahlreichen das Unionsrecht umsetzenden Vorschriften (vgl. im Zusammenhang mit den derzeitigen Aufgaben der KommAustria § 2 Z 2 KoPl-G).

Als „*Inhalteanbieter*“ ist gemäß Art. 2 Z 2 der Verordnung ein Nutzer zu verstehen, der Informationen bereitgestellt hat, die in seinem Auftrag von einem Hostingdiensteanbieter gespeichert und der Öffentlichkeit (dh. für einen potenziell unbegrenzten Personenkreis, vgl. Art. 2 Z 3 der Verordnung) zur Verfügung gestellt wurden oder werden.

Unter dem Begriff „*öffentliche Verbreitung*“ sollte nach ErwG 14 zu verstehen sein, dass Informationen den Nutzern im Allgemeinen leicht zugänglich gemacht werden, ohne dass weitere Maßnahmen des Inhalteanbieters erforderlich wären, unabhängig davon, ob die Personen tatsächlich auf die betreffenden Informationen zugreifen. Dementsprechend sollte in Fällen, in denen eine Registrierung oder die Aufnahme in eine Nutzergruppe erforderlich ist, um Zugang zu Informationen zu erlangen, nur dann von einer öffentlichen Verbreitung der Informationen ausgegangen werden, wenn die Nutzer, die auf die Informationen zugreifen möchten, automatisch registriert oder aufgenommen werden, ohne eine menschliche Entscheidung oder Auswahl, wem Zugang gewährt wird. Interpersonelle Kommunikationsdienste, wie beispielsweise E-Mail-Dienste oder Privatnachrichtenübermittlungsdienste, sollten nicht in den Anwendungsbereich der vorliegenden Verordnung fallen. Informationen sollten nur dann als im Sinne dieser Verordnung gespeichert und öffentlich verbreitet gelten, wenn dies auf direktes Verlangen des Inhalteanbieters hin geschieht. Folglich sollten Anbieter von Diensten wie Cloud-Infrastrukturen, die auf Verlangen von anderer Seite als von Seiten des Inhalteanbieters erbracht werden und Letzterem nur mittelbar zugutekommen, nicht unter die vorliegende Verordnung fallen. In den Anwendungsbereich der vorliegenden Verordnung sollten beispielsweise Anbieter von Dienstleistungen in sozialen Medien, von Video-, Bild- und Audio-Sharing-Diensten sowie von File-Sharing-Diensten und anderen Cloud-Diensten fallen, sofern diese Dienste dafür genutzt werden, um gespeicherte Informationen auf direktes Verlangen des Inhalteanbieters hin öffentlich zugänglich zu machen.

Aufgrund dieser Rollenverteilung zwischen Hostingdiensteanbieter und Inhalteanbieter wird deutlich, dass sich die Regulierungsmaßnahmen der mit diesem Gesetzesvorhaben zuständig gemachten KommAustria (vgl. dazu gleich nachfolgend die Ausführungen zu Abs. 1) auf den technischen „Bereitsteller“ oder „Transporteur“ des Inhalts, nicht aber auf den „Urheber“ (im Sinne eines inhaltlich Verantwortlichen) Inhalts beziehen. Die Regulierungstätigkeit der zuständigen Behörde betrifft ihrem weitaus überwiegenden Teil nach nicht den Medieninhaber, sondern etwa im Fall einer Entfernungsanordnung bloß indirekt.

Wie in Art. 16 Abs. 1 der Verordnung konkret angeführt ist die „zuständige Behörde“ (die KommAustria) im Fall der Beurteilung der spezifischen Maßnahmen (nach Art. 5) und bei der Verhängung von Strafsanktionen – mit Ausnahme von Strafsanktionen für Verstöße gegen die Pflicht, einen gesetzlichen Vertreter zu benennen (Art. 17) – nur für die ihrer Rechtshoheit unterliegenden Hostingdiensteanbieter zuständig. Das sind nach Art. 2 Z 9 der Verordnung jene Anbieter, mit Hauptverwaltung oder Sitz in Österreich, „*wo die wichtigsten Finanzfunktionen und die betriebliche Kontrolle ausgeübt werden*.“

Unter den vor allem im Zusammenhang mit der Ergreifung spezifischer Maßnahmen nach Art. 5 Abs. 1 der Verordnung und für die in Art. 7 geregelten Transparenzanforderungen (an den Anbieter) relevanten „*Nutzungsbedingungen*“ sind nach der Verordnung (vgl. Art. 2 Z 8) sämtliche Bestimmungen, Bedingungen und Klauseln, unabhängig von ihrer Bezeichnung oder Form, zur Regelung der vertraglichen Beziehungen zwischen einem Hostingdiensteanbieter und seinen Nutzern zu verstehen.

<u>Definition „terroristische Inhalte“:</u>

Dieser Terminus und sein Verständnis sind für den Zweck der Verordnung und damit auch des vorliegenden Gesetzesvorhabens grundlegend. Die Verordnung definiert den Begriff durch einen Verweis auf die Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates

1. Nach Art. 2 Z 7 der Verordnung sind nämlich „*terroristische Inhalte“ eines oder mehrere der folgenden Materialien, die Folgendes beinhalten oder bewirken:*

„a) die Anstiftung zur Begehung einer der in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten Straftaten, wenn durch solches Material direkt oder indirekt, z. B. durch die Verherrlichung terroristischer Handlungen, die Begehung terroristischer Straftaten befürwortet wird, mit der damit einhergehenden Gefahr, dass eine oder mehrere solche Taten begangen werden könnten;

b) die Bestimmung einer Person oder einer Gruppe von Personen zur Begehung einer der in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten Straftaten oder zum Beitragen an der Begehung;

c) die Bestimmung einer Person oder einer Gruppe von Personen zur Beteiligung an Handlungen einer terroristischen Vereinigung im Sinne des Artikels 4 Buchstabe b [der Richtlinie (EU) 2017/541, dh. einschließlich Bereitstellung von Informationen oder materiellen Mitteln oder durch jegliche Art der Finanzierung ihrer Tätigkeit in dem Wissen, dass diese Beteiligung zu den strafbaren Handlungen der terroristischen Vereinigung beiträgt];

d) die Unterweisung in der Herstellung oder im Gebrauch von Sprengstoffen, Schuss oder sonstigen Waffen oder schädlichen oder gefährlichen Stoffen beziehungsweise Unterweisung in anderen spezifischen Methoden oder Verfahren mit dem Ziel, eine der in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten terroristischen Straftaten zu begehen oder zu deren Begehung beizutragen;

e) eine Drohung, eine der in Artikel 3 Absatz 1 Buchstaben a bis i der Richtlinie (EU) 2017/541 aufgeführten Straftaten zu begehen;“

2. Die in allen vorstehenden literae als Verweis angegebenen „Buchstaben a bis i“ in Art. 3 Abs. 1 der Richtlinie (EU) 2017/541 lauten:

„a) Angriffe auf das Leben einer Person, die zum Tode führen können;

b) Angriffe auf die körperliche Unversehrtheit einer Person;

c) Entführung oder Geiselnahme;

d) schwerwiegende Zerstörungen an einer Regierungseinrichtung oder einer öffentlichen Einrichtung, einem Verkehrsmittel, einer Infrastruktur einschließlich eines Informatiksystems, an einer festen Plattform, die sich auf dem Festlandsockel befindet, einem allgemein zugänglichen Ort oder einem Privateigentum, die Menschenleben gefährden oder zu erheblichen wirtschaftlichen Verlusten führen können;

e) Kapern von Luft- und Wasserfahrzeugen oder von anderen öffentlichen Verkehrsmitteln oder Gütertransportmitteln;

f) Herstellung, Besitz, Erwerb, Beförderung, Bereitstellung oder Verwendung von Sprengstoffen oder Waffen, einschließlich chemischen, biologischen, radiologischen oder atomaren Waffen sowie die Forschung und Entwicklung im Zusammenhang mit chemischen, biologischen, radiologischen oder atomaren Waffen;

g) Freisetzung gefährlicher Stoffe oder Herbeiführen von Bränden, Überschwemmungen oder Explosionen, wenn dadurch das Leben von Menschen gefährdet wird;

h) Störung oder Unterbrechung der Versorgung mit Wasser, Strom oder anderen lebenswichtigen natürlichen Ressourcen, wenn dadurch das Leben von Menschen gefährdet wird;

i) *rechtswidrige Systemeingriffe im Sinne des Artikels 4 der Richtlinie 2013/40/EU* [dh. das vorsätzliche und unbefugte Löschen, Beschädigen, Beeinträchtigen, Verändern, Unterdrücken von Computerdaten eines Informationssystems und das Unzugänglichmachen solcher Daten] *in den Fällen, in denen Artikel 9 Absatz 3 oder Artikel 9 Absatz 4 Buchstaben b oder c der genannten Richtlinie Anwendung findet, und rechtswidrige Eingriffe in Daten im Sinne des Artikels 5 der genannten Richtlinie* [dh. das vorsätzliche und unbefugte, mit technischen Hilfsmitteln bewirkte Abfangen nichtöffentlicher Computerdatenübermittlungen an ein Informationssystem, aus einem Informationssystem oder innerhalb eines Informationssystems einschließlich elektromagnetischer Abstrahlungen aus einem Informationssystem, das Träger solcher Computerdaten ist] *in den Fällen, in denen Artikel 9 Absatz 4 Buchstabe c der genannten Richtlinie Anwendung findet;“*

ErwG 11 der Verordnung führt dazu aus, dass Materialien erfasst werden sollen, „*die jemanden zur Begehung terroristischer Straftaten oder zu einem Beitrag zur Begehung dieser Straftaten anstiften oder dazu bestimmten, jemanden zur Beteiligung an Handlungen einer terroristischen Vereinigung zu bestimmen, terroristische Aktivitäten verherrlichen, unter anderem auch durch die Verbreitung von Materialien, die Bilder von terroristischen Anschlägen zeigen. Unter die Definition sollten auch Materialien fallen, die zum Zweck der Begehung oder des Beitrags zur Begehung terroristischer Straftaten Anleitungen zur Herstellung oder Verwendung von Sprengstoffen, Schusswaffen oder anderen Waffen oder schädlichen oder gefährlichen Stoffen sowie chemischen, biologischen, radiologischen und nuklearen Stoffen (CBRN-Stoffen) oder zu anderen spezifischen Methoden oder Verfahren, einschließlich der Auswahl von Anschlagszielen, enthalten. Bei solchen Materialien kann es sich um Texte, Bilder, Tonaufzeichnungen und Videos sowie um Live-Übertragungen terroristischer Straftaten handeln, mit denen die Gefahr einhergeht, dass weitere solcher Taten begangen werden. Bei der Beurteilung, ob es sich bei Materialien um terroristische Inhalte im Sinne dieser Verordnung handelt, sollten die zuständigen Behörden und die Hostingdiensteanbieter Faktoren wie Art und Wortlaut der Aussagen, den Kontext, in dem die Aussagen getroffen wurden, und ihr Gefährdungspotenzial und somit ihr Potenzial zur Beeinträchtigung der Sicherheit von Personen berücksichtigen. Die Tatsache, dass das Material von einer Person, Vereinigung oder Organisation, die in der Liste der Union der an terroristischen Handlungen beteiligten Personen, Vereinigungen oder Organisationen aufgenommen wurde und*

restriktiven Maßnahmen unterliegt, hergestellt wurde, ihr zuzuschreiben ist oder in ihrem Namen verbreitet wird, sollte ein wichtiges Kriterium bei der Beurteilung darstellen.“

Materialien, „*die für Bildungs-, Presse- oder Forschungszwecke oder für künstlerische Zwecke oder zum Zweck der Sensibilisierung gegenüber terroristischen Aktivitäten verbreitet werden*,“ sollten nach ErwG 12 der Verordnung nicht als terroristische Inhalte gelten. Bei der Feststellung „*sollte insbesondere dem Recht auf Meinungs- und Informationsfreiheit, einschließlich der Medienfreiheit und des Medienpluralismus, und der Freiheit von Kunst und Wissenschaft Rechnung getragen werden. Insbesondere in Fällen, in denen der Inhalteanbieter eine redaktionelle Verantwortung trägt, sind Entscheidungen über die Entfernung verbreiteter Materialien unter Berücksichtigung der in einschlägigen Presse- und Medienvorschriften festgelegten journalistischen Standards, die im Einklang mit dem Unionsrecht einschließlich der Charta stehen, zu treffen. Ferner sollte die Formulierung radikaler, polemischer oder kontroverser Ansichten zu sensiblen politischen Fragen in der öffentlichen Debatte nicht als terroristischer Inhalt betrachtet werden*.“

Zu § 2:

Zu Abs. 1:

Die Regelung beinhaltet als wesentliche Grundlage für die Vollziehung der verfahrensrechtlichen und materiellen Bestimmungen der Verordnung die Festlegung der Zuständigkeit wie dies von Art. 12 Abs. 1 der Verordnung verlangt wird.

Schon nach der geltenden Rechtslage nach dem KoPl-G und dem 9b. Abschnitt des AMD-G sind der KommAustria regulatorische Vollzugsaufgaben zum Schutz vor verbotenen Inhalten (darunter auch terroristischen Inhalten) und die Beurteilung der Angemessenheit von Beschwerdemechanismen sowie der von Plattformbetreibern ergriffenen Maßnahmen aufgetragen. Es liegt daher nahe, diese Behörde mit den dem Grunde nach vergleichbaren Aufgaben im Hinblick auf die Bekämpfung terroristischer Inhalte zu betrauen. Schon mit der Zuständigkeit für Video-Sharing-Plattform-Anbieter nach dem AMD-G zählen seit dem 1.1.2021 zum Kreis der von der KommAustria regulierten Unternehmen nicht mehr nur die klassischen – auch als Medieninhaber oder Medienunternehmen verantwortlichen – Inhalteanbieter, sondern auch Plattformanbieter ohne eine redaktionelle Verantwortung für das von ihnen verbreitete Angebot. Mit den von den Inhalteanbietern klar zu unterscheidenden Hostingdiensteanbietern tritt nun eine weitere Sparte zu dem von der KommAustria Kreis der Regulierten hinzu. Abgesehen von den umfangreichen und verschiedenartigen regulatorischen Erfahrungen der KommAustria spricht auch ein zentraler weiterer Aspekt für die Zuweisung der Aufgabe an die KommAustria: Art. 13 der Verordnung verlangt, dass die Behörde bei der Wahrnehmung ihrer Aufgaben gemäß Art. 12 Abs. 1 „*weder Weisungen von anderen Stellen ein[holt], noch […] solche Weisungen entgegen[nimmt]*“. Dieser Anforderung ist durch die Betrauung der KommAustria (vgl. die die Unabhängigkeit absichernden Regelungen in den §§ 3 ff KOG), gestützt auf Art. 20 Abs. 2 Z 8 B-VG, eindeutig erfüllt. Aufgrund der Regelung in § 18 Abs. 1 KOG, wonach die RTR-GmbH im Rahmen ihrer Tätigkeit für die KommAustria ausschließlich an die Aufträge und fachlichen Weisungen des Vorsitzenden und der Mitglieder gebunden ist, ist auch sichergestellt, dass der für die KommAustria tätige Geschäftsapparat weder Weisungen von anderen Stellen einholt, noch solche Weisungen entgegennimmt. Die Verordnung anerkennt im zweiten Unterabsatz von Art. 13 Abs. 2 explizit, dass die Vorgabe der Weisungsfreiheit einer Aufsicht im Einklang mit dem nationalen Verfassungsrecht nicht entgegensteht. Auch vor diesem Hintergrund ist das sich aus Art. 20 Abs. 2 B-VG ergebende und in § 15 Abs. 1 KOG geregelte Recht des Bundeskanzlers, sich über alle Gegenstände der Geschäftsführung der weisungsfreien KommAustria zu unterrichten, unionsrechtlich unbedenklich.

Die KommAustria soll folglich zukünftig – wie in Art. 12 Abs. 1 der Verordnung ausdrücklich aufgelistet – für Folgendes zuständig sein:

- Entfernungsanordnungen (Art. 3)

Mit der Erlassung von Entfernungsanordnungen werden Hostingdiensteanbieter verpflichtet, in allen Mitgliedstaaten terroristische Inhalte innerhalb einer Stunde nach Erhalt der Entfernungsanordnung zu entfernen (Art. 3 Abs. 1 und 3) oder den Zugang zu terroristischen Inhalten zu sperren. Von hinreichend begründeten Dringlichkeitsfällen abgesehen sollte nach dem den Art. 3 Abs. 2 der Verordnung erläuternden ErwG 17 die zuständige Behörde dem Hostingdiensteanbieter mindestens 12 Stunden, bevor sie erstmals eine Entfernungsanordnung gegenüber diesem Hostingdiensteanbieter erlässt, Informationen über Verfahren und geltende Fristen bereitstellen. Hinreichend begründete Dringlichkeitsfälle liegen dann vor, wenn der Umstand, dass die Entfernung von Inhalten oder die Sperrung des Zugangs zu den terroristischen Inhalten später als eine Stunde nach Erhalt der Entfernungsanordnung erfolgt, zu einem ernsthaften Schaden führen würde, beispielsweise in Situationen, in denen das Leben oder die körperliche Unversehrtheit einer Person unmittelbar bedroht sind, oder wenn solche Inhalte laufende Ereignisse

zeigen, bei denen dem Leben oder der körperlichen Unversehrtheit einer Person Schaden zugefügt wird. Die Regelungen in Art. 3 (insb. in Abs. 4) enthalten hinreichend konkrete (auch verfahrensrechtliche) Vorgaben, die die Behörde einzuhalten hat und schreiben neben dem Mindestinhalt der Anordnung auch vor, dass dazu ein Formular wie in Anhang 1 der Verordnung ausgewiesen verwendet werden muss. Die KommAustria kann nach dem vorliegenden System daher derartige Entfernungsanordnungen sowohl gegenüber den ihrer Rechtshoheit unterliegenden Anbietern als auch gegenüber ausländischen Anbietern erlassen.

- Überprüfung der Entfernungsanordnungen von Behörden anderer Mitgliedstaaten (Art. 4)

In diesem Verfahren für grenzüberschreitende Entfernungsanordnungen müssen die zuständigen Behörden (dh. die Behörde, die eine Anordnung erlässt, und die für den Hostingdiensteanbieter nach dem Niederlassungsprinzip an sich zuständige Behörde) zusammenarbeiten; dies bedeutet, dass die Entfernungsanordnung von der jeweils für das Sachgebiet zuständigen Behörde eines Mitgliedstaates auch gegenüber einem Anbieter erlassen werden kann, der seine Hauptniederlassung in einem anderen Mitgliedstaat hat. Diesfalls ist der Behörde des Niederlassungsstaates eine Kopie der Anordnung zu übermitteln. Der Behörde des Niederlassungsstaates (also im Fall eines der österreichischen Rechtshoheit unterliegenden Anbieters die KommAustria) kommt das Recht zu, von sich aus die Entfernungsanordnung innerhalb von 72 Stunden nach Erhalt zu überprüfen. Bei Feststellung eines Verstoßes gegen die Verordnung oder die Grundrechtecharta erlässt die Behörde des Niederlassungsstaates eine begründete Entscheidung. Auch der Hostingdiensteanbieter und der Inhalteanbieter können innerhalb von 48 Stunden nach Erhalt einen begründeten Antrag auf Überprüfung der Anordnung stellen. Nach ErwG 20 der Verordnung soll es bei dieser Überprüfung um die Feststellung gehen, ob die Anordnung einen schwerwiegenden oder offenkundigen Verstoß gegen diese Verordnung oder die in der Charta verankerten Grundrechte enthält oder ob dies nicht der Fall ist. Wenn bei der Prüfung ein derartiger Verstoß festgestellt wird, verliert die Entfernungsanordnung nach Art. 4 Abs. 6 ihre Rechtswirkung.

- Überwachung der Durchführung der von Hostingdiensteanbietern zur Verhinderung der Verbreitung terroristischer Inhalte ergriffenen Maßnahmen (Art. 5)

Wenn ein Anbieter aufgrund einer Entscheidung der zuständigen Behörde (Abs. 4) als „*terroristischen Inhalten ausgesetzt*“ zu qualifizieren ist, hat er spezifische Maßnahmen zu ergreifen, wobei er selbst über die zu treffenden, in Art. 5 Abs. 2 beispielhaft aufgezählten Maßnahmen unter besonderer Beachtung der Kriterien der Eignung, Zielgerichtetheit und Verhältnismäßigkeit (Abs. 3) entscheidet. Die Verordnung zählt diverse Instrumente auf, wie etwa

- geeignete technische und operative Maßnahmen und Kapazitäten, um terroristische Inhalte zu ermitteln und unverzüglich zu entfernen/sperren
- Meldemechanismen und Kennzeichnungstools für NutzerInnen
- Mechanismen zur stärkeren Sensibilisierung für terroristische Inhalte wie Forenmoderation.

Der betroffene Anbieter muss der Behörde über die gesetzten Maßnahmen berichten (Abs. 5). Die Behörde beurteilt auf der Grundlage der Berichte die Implementierung der spezifischen Maßnahmen. Bei dieser Beurteilung ist zu bedenken, dass – wie ErwG 23 dies ausführt – die Hostingdiensteanbieter bei der Durchführung der Maßnahmen dafür sorgen sollen, dass das Recht der Nutzer auf Meinungs- und Informationsfreiheit sowie die Medienfreiheit und der Medienpluralismus gewahrt bleiben. Zusätzlich sollten die Hostingdiensteanbieter Schutzvorkehrungen treffen, um unbeabsichtigte oder irrtümliche Entscheidungen zu vermeiden, die dazu führen, dass nicht-terroristische Inhalte entfernt oder gesperrt werden. Laut ErwG 24 sollte die Behörde bei ihrer Überprüfung feststellen können, „*ob die Maßnahmen wirksam und verhältnismäßig sind und ob der Hostingdiensteanbieter – sofern automatisierte Verfahren zum Einsatz kommen – über die notwendigen Kapazitäten für die menschliche Aufsicht und Überprüfung verfügt. Bei der Bewertung der Wirksamkeit und Verhältnismäßigkeit der Maßnahmen sollten die zuständigen Behörden die einschlägigen Parameter berücksichtigen, einschließlich der Anzahl der gegenüber dem Hostingdiensteanbieter erlassenen Entfernungsanordnungen, der Größe und wirtschaftlichen Leistungsfähigkeit des Hostingdiensteanbieters und der Wirkung seiner Dienste bei der Verbreitung terroristischer Inhalte, z. B. unter Berücksichtigung der Zahl der Nutzer in der Union, sowie der Vorkehrungen, die getroffen wurden, um den Missbrauch seiner Dienste für die Verbreitung terroristischer Online-Inhalte zu bekämpfen.*“

Gelangt die Behörde zur Auffassung, dass die Maßnahmen nicht geeignet, zielgerichtet oder auch nicht verhältnismäßig sind, so hat sie den Anbieter zur Ergreifung der erforderlichen Maßnahmen aufzufordern (Art. 5 Abs. 6). Dazu hebt ErwG 25 (in Erläuterung von Art. 5 Abs. 8) nochmals besonders hervor, dass dabei weder eine allgemeine Pflicht zur Überwachung oder zum aktiven Forschen nach Hinweisen noch

eine Verpflichtung zur Anwendung automatisierter Werkzeuge (Tools) auferlegt werden darf, jedoch Hostingdiensteanbieter die Möglichkeit haben sollten, automatisierte Werkzeuge (Tools) anzuwenden, wenn sie dies für geeignet und erforderlich halten, um den Missbrauch ihrer Dienste für die Verbreitung terroristischer Online-Inhalte wirksam zu bekämpfen.

- Weitere Aufgaben

Aus den weiteren Artikeln der Verordnung ergeben sich basierend auf der Funktion der „zuständigen" Behörde noch folgende Aufgaben und Verpflichtungen, die keiner weiteren Durchführung im vorliegenden Gesetzesvorhaben bedürfen, weil sie hinreichend konkret schon auf unionsrechtlicher Ebene angeordnet sind:

- Art. 8: Erstellung und Veröffentlichung jährlicher Transparenzberichte mit den in Abs. 1 genannten Mindestangaben über die Entscheidungs- und Sanktionspraxis auch auf Basis der Transparenzberichte der Anbieter (Art. 7);
- Art. 14 Abs. 1 bis 4 und 6: Wechselseitige Verständigung, Abstimmung und Zusammenarbeit mit den Behörden anderer Mitgliedstaaten und mit Europol

Hierzu ist auf die ErwG 36 bis 40 zu verweisen. Das dahinterstehende Anliegen ist in der Vermeidung von Doppelarbeit und gegenseitiger Behinderung sowie in der Reduktion des Aufwands bei den betroffenen Hostingdiensteanbietern zu sehen. „*Wenn eine zuständige Behörde von der zuständigen Behörde eines anderen Mitgliedstaats über eine bereits bestehende Entfernungsanordnung informiert wird, sollte sie keine Entfernungsanordnung zum gleichen Sachverhalt erlassen*." ErwG 38 hebt hierzu hervor, dass für die wechselseitige Information geeignete und sichere Kommunikationskanäle oder -mechanismen vorgesehen sein sollten, die die fristgerechte Übermittlung der relevanten Informationen ermöglichen. ErwG 39 weist zu Art. 14 Abs. 4 darauf hin, dass „*die speziell dafür von Europol entwickelten Werkzeuge wie die aktuelle Verwaltungsanwendung für die Meldung von Internetinhalten (Internet Referral Management application) oder deren Nachfolger zu nutzen*" wären.

Zu Abs. 2:

Mit Abs. 2 wird – wie schon in § 17 Abs. 1 KOG eindeutig geregelt – hervorgehoben, dass auch im Bereich der Vollziehung der einschlägigen Rechtsvorschriften zur Bekämpfung der Verbreitung von terroristischen Online-Inhalten die RTR-GmbH die fachliche und administrative Unterstützung der KommAustria übernimmt. Aus dem Zusammenhalt mit § 18 Abs. 1 KOG ergibt sich auch, dass die RTR-GmbH diesbezüglich im Rahmen ihrer Tätigkeit als Geschäftsstelle für die KommAustria ausschließlich an die Aufträge und fachlichen Weisungen des Vorsitzenden und der Mitglieder gebunden ist. Dies gilt daher auch für die Einrichtung der in Abs. 2 angesprochenen (und von Art. 12 Abs. 2 der Verordnung vorgegebenen) Kontaktstelle der Behörde. Die RTR-GmbH kann hier auch bei der Gestaltung des entsprechenden öffentlich zugänglichen Informationsportals auf umfassende Erfahrung aufgrund ihrer bisherigen Tätigkeit als Servicestelle in unterschiedlichsten Bereichen zu verweisen. Nach dem Wortlaut der Verordnung muss es bei der Behörde (dh. im unmittelbaren Umfeld der KommAustria) eine Stelle zur Bearbeitung von Ersuchen um Klarstellung und Rückmeldungen im Zusammenhang mit den erlassenen Entfernungsanordnungen geben, deren Kontaktdaten auch öffentlich zugänglich sind.

In datenschutzrechtlicher Hinsicht wird die RTR-GmbH, Fachbereich Medien, soweit sie dabei personenbezogene Daten verarbeitet, als Auftragsverarbeiterin der KommAustria tätig (vgl. Art. 2 Z 5 [§ 17 Abs. 1 KOG]).

Zum Rechtsbehelf (Art. 9 der Verordnung):

Sowohl Hostingdiensteanbieter als auch Inhalteanbieter müssen gegen sie betreffende Entscheidungen der zuständigen Behörde einen „wirksamen *Rechtsbehelf*" erheben können (vgl auch ErwG 32 der Verordnung). Dieser Voraussetzung ist schon durch das geltende Verfahrensrecht entsprochen, indem sämtliche Entscheidungen der mit diesem Gesetzesvorhaben für zuständig erklärten KommAustria vor dem Bundesverwaltungsgericht (vgl. § 36 KOG) in Beschwerde gezogen werden können. Einem Inhalteanbieter wird schon aufgrund der Tatsache, dass der von ihm zu verantwortende Inhalt von einer Entfernung oder Sperre betroffen ist, in allen die Entfernung oder Sperre betreffenden Verfahren der KommAustria (Entfernungsanordnung nach Art. 3 der Verordnung und auch Entscheidung über die Prüfung der Anordnung nach Art. 4) Parteistellung (vgl. § 8 AVG) zukommen.

Zu § 3:

Die Direktion Staatsschutz und Nachrichtendienst (DSN) betreibt mehrere Meldestellen, von denen eine die gemäß § 4 Z 2a des Bundesgesetzes über die Organisation, Aufgaben und Befugnisse des Verfassungsschutzes (Staatsschutz- und Nachrichtendienst-Gesetz – SNG) eingerichtete „Meldestelle Extremismus und Terrorismus" darstellt, deren Aufgabe die Entgegennahme von Hinweisen über

extremistische oder terroristische Inhalte, die unter Nutzung von Online-Diensten verbreitet oder übermittelt werden, umfasst. Der vorgeschlagenen Bestimmung liegt die Auffassung zugrunde, dass die DSN – in ihrer Funktion als Meldestelle iSd § 4 Z 2a SNG – Kenntnis von terroristischen Online-Inhalten erlangt, die auch in den Zuständigkeitsbereich der KommAustria fallen, und sie daher die KommAustria über das Einlangen einer derartigen Meldung zu informieren und ihr dabei unter einem auch die für eine Entscheidung über die Erlassung einer Entfernungsanordnung nach Anhang 1 der Verordnung erforderlichen – und soweit bei der DSN vorhandenen – Angaben zu übermitteln hat (Abs. 1). Dadurch soll sichergestellt werden, dass die KommAustria ihrer zugewiesenen Aufgabe nachkommen kann, selbst wenn die Meldung nicht direkt bei der KommAustria, sondern bei der Meldestelle der DSN einlangen sollte.

Die Wendung „ohne unnötigen Aufschub“ ist dabei so zu verstehen, dass die Meldung grundsätzlich sogleich nach Meldungseingang von der DSN an die KommAustria übermittelt wird, jedoch in Einzelfällen, bei denen eine dringliche sicherheits- oder kriminalpolizeiliche Ermittlungsmaßnahme geboten erscheint, die Übermittlung solange aufgeschoben werden kann als sicherheits- und kriminalpolizeiliche Gründe überwiegen.

Abs. 3 erfasst den – umgekehrten und angesichts des eigentlichen zentralen Aufgabengebietes der KommAustria im Bereich der Medienregulierung anzunehmenderweise selteneren – Fall, dass die KommAustria „unmittelbar“ Kenntnis von (möglichen) terroristischen Online-Inhalten erlangt. Damit in diesem Fall auch die DSN Kenntnis von diesen Inhalten erlangt und sie ihrer Funktion als zentraler Stelle zum Schutz vor terroristisch motivierter Kriminalität nachkommen kann, hat die KommAustria die betreffende Meldung an die DSN weiterzuleiten. Unter einem hat die KommAustria die DSN aufzufordern, ihr die Gründe, die für oder gegen eine Einstufung des konkreten Materials als terroristischer Inhalt sprechen, mitzuteilen.

Aus Art. 14 der Verordnung („Zusammenarbeit zwischen Hostingdiensteanbietern, zuständigen Behörden und Europol“) ergibt sich das Erfordernis einer Zusammenarbeit mit den zuständigen Behörden anderer Staaten und Europol. Darauf nimmt Abs. 2 Bezug und regelt, dass die DSN für den Fall, dass die KommAustria nicht über die technischen Möglichkeiten verfügt, Informationen an Europol oder Strafverfolgungsbehörden in anderen EU-Mitgliedstaaten zu übermitteln hat, soweit die DSN über die technischen Möglichkeiten zum Einsatz der in Art. 14 Abs. 4 lit. a der Verordnung genannten speziellen (auch der von Europol eingeführten) Verfahren verfügt.

Die sachliche Rechtfertigung dieser Regelung liegt darin, dass die DSN bereits über Erfahrung in der Zusammenarbeit mit Europol und ausländischen Strafverfolgungsbehörden und daher zu diesem Zweck in der Regel bereits über die erforderlichen technischen Möglichkeiten, wie gesicherte Kommunikationskanäle (etwa mit Europol), verfügt.

Der zulässige Umfang der im Rahmen des Zusammenarbeitsverfahrens nach § 3 Abs. 2 von der KommAustria an die DSN zu übermittelnden Daten ergibt sich aus den in § 2 Abs. 1 genannten Zwecken in Verbindung mit den dort verwiesenen Bestimmungen der Verordnung, dh. insb. der in Art. 3 der Verordnung genannte Anhänge I (Formular für Entfernungsanordnungen), II (Formular für Rückmeldungen nach der Entfernung oder Sperrung terroristischer Inhalte) und III (Formular Unterrichtung über die Unmöglichkeit der Ausführung der Entfernungsanordnung). Die DSN ist diesfalls datenschutzrechtlicher Verantwortlicher gemäß Art. 4 Z 7 DSGVO.

Alle diese Schritte sind angesichts der Zeit-Sensibilität des Themas ohne unnötigen Aufschub (Abs. 1) bzw. unverzüglich (Abs. 3) zu setzen und (vermeidbare) Verzögerungen – wie etwa Nachfragen aufgrund unvollständiger Angaben – hintanzuhalten.

Weiters haben sich die DSN und die KommAustria in regelmäßigen Abständen über alle relevanten Fragen auszutauschen.

Zu § 4:

Diese Bestimmung regelt die Voraussetzungen, unter denen die KommAustria im Einzelfall unbedingt erforderliche personenbezogenen Daten verarbeiten darf, die Dauer der Aufbewahrung und die Löschpflicht. Durch die Bezugnahme auf die in §§ 2 und 3 normierten Aufgaben wird sichergestellt, dass die KommAustria zB auch im Hinblick auf § 3 Abs. 3 relevante Inhalte und damit unmittelbar zusammenhängende personenbezogene Daten an die DSN übermitteln darf.

Im zuletzt genannten Fall (wie auch im Zusammenhang mit § 3 Abs. 2) ist zu bedenken, dass – anders als im Verhältnis zwischen KommAustria und RTR (vgl. Art. 2 Z 5 [§ 17 Abs. 1 KOG]) – die DSN nicht als Auftragsverarbeiterin der KommAustria tätig wird; vielmehr besteht zwischen beiden kein Weisungszusammenhang und beide sind Verantwortliche im Sinne der DSGVO. Im Hinblick auf die

DSN regelt § 3 die Zulässigkeit des Datenaustausches mit der KommAustria. Die diesbezügliche Dokumentation des Tätigwerdens der DSN nach diesem Bundesgesetz wird auf § 13a SPG gestützt.

Die Zulässigkeit der Verarbeitung von besonderen Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO) und von strafrechtlich relevanten personenbezogenen (im Sinn von Art. 10 DSGVO) ergibt sich vorliegend aus Art. 9 Abs. 2 lit. g (erhebliches öffentliches Interesse) bzw. Art. 10 erster Satz DSGVO, jeweils in Verbindung mit den Verpflichtungen aus der gegenständlichen Verordnung.

Als spezifische Maßnahmen (im Sinne des Art. 9 Abs. 2 lit. g DSGVO bzw. geeignete Garantien (im Sinne des Art. 10 DSGVO) kann insb. auf die strenge Zweckbindung (§ 4 Abs. 1) und die limitierte Speicherdauer (dh. die Löschfrist gem. § 4 Abs. 2) verwiesen werden.

Im Hinblick auf die Aufbewahrungspflicht bzw. die Frist, nach deren Ablauf die betreffenden Inhalte zu löschen sind, ist darauf hinzuweisen, dass hier nicht die im Verwaltungsverfahren üblichen Skartierungsfristen, sondern kürzere Fristen zur Anwendung kommen sollen, einerseits weil es in der Regel um besonders sensible personenbezogene Inhalte (wie etwa Videos, auf denen die Opfer terroristischer Anschläge zu sehen sind) gehen dürfte, andererseits weil dies der in der Verordnung vorgesehenen Sechs-Monats-Frist entspricht (Art. 6 Abs. 2). Die Sechs-Monats-Frist soll auch für Inhalte, von denen die KommAustria nach § 2 Abs. 1 Kenntnis erlangt hat, gelten, um eine Lücke zu vermeiden und möglichst alle Sachverhalte den vorgesehenen datenschutzrechtlichen Aufbewahrungs- und Löschfristen zu unterwerfen.

Mit Abs. 3 soll festgehalten werden, dass die DSN personenbezogenen Daten, die sie in Vollziehung des § 3 verarbeitet, auch zur Erfüllung ihrer sonstigen, gesetzlich übertragenen Aufgaben weiterverarbeiten darf; unbedingte Erforderlichkeit zur jeweiligen Aufgabenerfüllung vorausgesetzt. Dies kommt insb. zur Erfüllung sicherheits- und kriminalpolizeilicher Aufgaben, die sich aufgrund einer Meldung über einen terroristischen Inhalt an die KommAustria in weiterer Folge ergeben können, in Betracht.

In diesem Kontext ist auch auf die in Art. 22 B-VG normierte Verpflichtung der Behörden zur wechselseitigen Hilfeleistung im Rahmen ihres gesetzmäßigen Wirkungsbereiches hinzuweisen.

Zu § 5:

Diese Norm, derzufolge sich jeder Hostingdiensteanbieter unverzüglich für eine Zustellung durch einen Zustelldienst im Sinne der §§ 28b und 35 des Zustellgesetzes anzumelden und dabei anzugeben hat, dass es keine Zeiträume gibt, innerhalb derer die Zustellung ausgeschlossen ist, orientiert sich an der bewährten Bestimmung des § 5 Abs. 3 des Kommunikationsplattformen-Gesetzes. Ein Hostingdiensteanbieter, der dieser Verpflichtung nicht entspricht, begeht eine Verwaltungsübertretung und ist mit einer Geldstrafe gemäß § 7 Abs. 1 Z 1 zu bestrafen.

Zu § 6:

Gemäß Art. 21 der Verordnung ist ein Monitoring vorgesehen, demzufolge von den Mitgliedstaaten Informationen über die ergriffenen Maßnahmen an die Kommission spätestens bis zum 31. März jeden Jahres übermittelt werden sollen. Dazu haben die Mitgliedstaaten von „ihren zuständigen Behörden und den ihrer Gerichtsbarkeit [richtig wohl: Rechtshoheit] unterstehenden Hostingdiensteanbietern Informationen über die Maßnahmen“ einzuholen. Die Regelungen in § 6 Abs. 1 und 2 dienen folglich der Vorbereitung dieser Berichterstattung des für die Vollziehung dem Grundsatz nach zuständigen Bundeskanzlers an die Kommission und durch die Vorlaufzeiten in Abs. 1 und 2 der Sicherstellung einer fristgerechten Übermittlung. Der unionsrechtlichen Vorgabe zufolge sind der Kommission für ihre Evaluierung über die weiteren Schritte (Bericht der Kommission gemäß Art. 22 der Verordnung und Evaluierung nach Art. 23 leg.cit.) folgende Angaben zu übermitteln:

- die Anzahl der erlassenen Entfernungsanordnungen und die Anzahl der entfernten oder gesperrten Elemente mit terroristischem Inhalt sowie wie schnell die Entfernung oder Sperrung stattfand;
- spezifische Maßnahmen nach Art. 5, einschließlich der Anzahl der entfernten oder gesperrten Elemente mit terroristischem Inhalt und wie schnell die Entfernung oder Sperrung erfolgt ist;
- Anzahl der von den zuständigen Behörden angeforderten Zugriffe auf von Hostingdiensteanbietern nach Art. 6 gespeicherte Inhalte;
- Anzahl der eingeleiteten Beschwerdeverfahren und der von Hostingdiensteanbietern unternommenen Maßnahmen nach Art. 10;
- Anzahl der eingeleiteten behördlichen oder gerichtlichen Überprüfungsverfahren und der von der zuständigen Behörde nach nationalem Recht erlassenen Entscheidungen.

Entsprechend ErwG 48 der Verordnung geht es darum, dass Informationen über die Umsetzung der Verordnung gesammelt und die Transparenzberichte der Hostingdiensteanbieter genutzt werden können

und der betreffende Mitgliedstaat diese, wo notwendig, durch ausführlichere Informationen, wie beispielsweise die eigenen Transparenzberichte gemäß dieser Verordnung, ergänzen.

Die Transparenzberichte der Hostingdiensteanbieter, die in einem bestimmten Kalenderjahr Maßnahmen gegen die Verbreitung terroristischer Inhalte ergriffen haben oder zur Ergreifung von Maßnahmen aufgefordert wurden, haben entsprechend Art. 7 Abs. 3 der Verordnung mindestens folgende Angaben zu enthalten:

a) Informationen über die Maßnahmen des Hostingdiensteanbieters im Zusammenhang mit der Ermittlung und Entfernung oder Sperrung terroristischer Inhalte;

b) Informationen über die Maßnahmen, die der Hostingdiensteanbieter trifft, um gegen ein erneutes Erscheinen von Online-Materialien vorzugehen, die zuvor entfernt oder gesperrt wurden, weil sie als terroristische Inhalte erachtet wurden, insb. wenn automatisierte Verfahren verwendet wurden;

c) Anzahl der nach Entfernungsanordnungen oder spezifischen Maßnahmen entfernten oder gesperrten Elemente mit terroristischem Inhalt und Anzahl der Entfernungsanordnungen, nach deren Erhalt der Inhalt gemäß Art. 3 Abs. 7 UAbs. 1 und Abs. 8 UAbs. 1 nicht entfernt oder gesperrt wurde, einschließlich der Gründe dafür;

d) Anzahl und Ergebnis der vom Hostingdiensteanbieter bearbeiteten Beschwerden gem. Art. 10;

e) Anzahl und Ergebnis der vom Hostingdiensteanbieter eingeleiteten behördlichen oder gerichtlichen Überprüfungsverfahren;

f) Anzahl der Fälle, in denen der Hostingdiensteanbieter infolge eines behördlichen oder gerichtlichen Überprüfungsverfahrens Inhalte wiederherstellen oder entsperren musste;

g) Anzahl der Fälle, in denen der Hostingdiensteanbieter die Inhalte nach Prüfung einer Beschwerde des Inhalteanbieters wiederhergestellt oder entsperrt hat.

Gemäß Art. 8 der Verordnung muss die zuständige Behörde jährlich einen Bericht über ihre Tätigkeit im Rahmen der Verordnung veröffentlichen. Die Regelung des § 6 Abs. 3 dient folglich der Konkretisierung der Art der Veröffentlichung und orientiert sich an der Berichterstattung über die Tätigkeit der KommAustria nach anderen Rechtsvorschriften, wie etwa dem KoPl-G oder dem 9b. Abschnitt des AMD-G, die ebenfalls im gemeinsamen Tätigkeitsbericht von KommAustria, Telekom-Control-Kommission und RTR-GmbH zu erfolgen hat. Die Berichte nach Art. 8 der Verordnung unterscheiden sich von den nach § 6 Abs. 2 dem Bundeskanzler vorzulegenden Berichten dahingehend, dass sie ausgewählte Tätigkeiten der zuständigen Behörde umfassen, nicht aber auch Maßnahmen der Hostingdiensteanbieter. Der unionsrechtlichen Vorgabe zufolge haben die Transparenzberichte mindestens folgende Angaben zu enthalten:

a) Zahl der nach Art. 3 erlassenen Entfernungsanordnungen, nach welcher sich die Anzahl der Entfernungsanordnungen gemäß Art. 4 Abs. 1 richtet, die Zahl der nach Art. 4 überprüften Entfernungsanordnungen sowie Angaben dazu, wieweit die betroffenen Hostingdiensteanbieter diesen Anordnungen nachgekommen sind, einschließlich der Anzahl der Fälle, in denen terroristische Inhalte entfernt oder gesperrt wurden sowie der Anzahl der Fälle, in denen dies nicht der Fall war;

b) Zahl der Entscheidungen gemäß Art. 5 Abs. 4, 6 oder 7 sowie Angaben dazu, wieweit die Hostingdiensteanbieter diesen Entscheidungen nachgekommen sind, einschließlich einer Beschreibung der spezifischen Maßnahmen;

c) Zahl der Fälle, in denen gegen Entfernungsanordnungen oder Entscheidungen gemäß Art. 5 Abs. 4 und 6 behördliche oder gerichtliche Überprüfungsverfahren eingeleitet wurden, sowie Angaben zu den Ergebnissen der jeweiligen Verfahren;

d) Zahl der Entscheidungen, mit denen Sanktionen gemäß Art. 18 verfügt wurden, einschließlich einer Beschreibung der Art der verfügten Sanktionen.

Die Transparenzberichte der zuständigen Behörde dürfen gemäß Art 8 Abs. 2 keine Angaben enthalten, die laufende Tätigkeiten zur Verhinderung, Erkennung, Ermittlung oder Verfolgung terroristischer Straftaten oder die nationalen Sicherheitsinteressen beeinträchtigen könnten.

Zu § 7:

Die Bestimmung enthält als zweites zentrales Element des Gesetzesvorhabens die Regelungen über die Sanktionen im Fall von Verstößen gegen die einschlägigen Verhaltensanweisungen und Handlungspflichten der Verordnung. Gemäß Art. 18 der Verordnung müssen Vorschriften über Sanktionen, die bei Verstößen der der österreichischen Rechtshoheit unterliegenden

Hostingdiensteanbieter gegen diese Verordnung zu verhängen sind, erlassen und alle für die Anwendung der Sanktionen erforderlichen Maßnahmen getroffen werden.

Während ErwG 45 der Verordnung den Grundsatz „ne bis in idem“ sowie die Wahrung der Verhältnismäßigkeit hervorhebt, enthält er auch den Hinweis, dass Sanktionen „*unterschiedliche Formen annehmen können, darunter die förmliche Verwarnung bei geringfügigen Verstößen oder finanzielle Sanktionen bei schwerwiegenderen oder systematischen Verstößen*“. Die Mitgliedstaaten sollten außerdem „*sicherstellen, dass Sanktionen bei Verstößen gegen diese Verordnung nicht dazu führen, dass nicht terroristische Materialien entfernt werden.*“

Aus den vorgenannten Gründen sieht § 7 einen abgestuften Katalog an Sanktionen vor. Im Hinblick auf den Grad des Verschuldens genügt zur Strafbarkeit fahrlässiges Verhalten (vgl. § 5 Abs. 1 VStG, hinsichtlich § 7 Abs. 2 und 3 dieses Entwurfs siehe allerdings auch § 5 Abs. 1a VStG). Allenfalls kommt bei Verstößen nach Abs. 1 auch eine Ermahnung gemäß § 45 Abs. 1 VStG in Frage (vgl. den vorstehend zitierten ErwG 45 der Verordnung).

Nach der Vorgabe der Verordnung müssen sich die Sanktionen allerdings auf folgende Verstöße „*beschränken*“: Art. 3 Abs. 3 und 6, Art. 4 Abs. 2 und 7, Art. 5 Abs. 1, 2, 3, 5 und 6, Art. 6, 7, 10 und 11, Art. 14 Abs. 5, Art. 15 Abs. 1 und Art. 17.

Art. 18 Abs. 1 der Verordnung verlangt explizit, dass die Sanktionen „*wirksam, verhältnismäßig und abschreckend*“ sind. Dementsprechend sieht die innerstaatliche Regelung in den Abs. 1 bis 3 aus general- und spezialpräventiven Überlegungen drei im Hinblick auf die Höhe der Strafe gestaffelte Schritte für jeweils dem Typus und ihrer Auswirkung nach vergleichbare Deliktskategorien vor. Auf den Grad der Unzulänglichkeit kann durch die Höhe der Geldstrafe innerhalb dieser Stufen (arg „*bis zu*“) Bedacht genommen werden.

Entsprechend diesem Hintergrund ist die Sanktionsstaffelung für jene Verstöße, auf deren Verfolgung sich die Mitgliedstaaten zu „*beschränken*“ haben, so konstruiert, dass auch der Bedeutung und Tragweite der Rechtsverletzung im Hinblick auf ihre Wirkung auf die Allgemeinheit Rechnung getragen wird:

Die Strafdrohung für die in Abs. 1 angeführten Tatbestände beträgt „*bis zu 50 000 Euro*“. In diesem Absatz sind ihrem überwiegenden Anteil nach Verstöße gegen die aus der Verordnung resultierenden diversen Bekanntgabe-, Informations-, Unterrichtungs-, Berichterstattungs- oder Benachrichtigungsverpflichtungen zusammengefasst. Im Hinblick auf § 7 Abs. 1 Z 9 lit. a und b ist festzuhalten, dass die Verpflichtung nach Art. 15 Abs. 2 der Verordnung, in den Informationen über die Kontaktstelle die Amtssprachen anzugeben, in denen eine Kontaktaufnahme mit der Kontaktstelle möglich ist und in denen der weitere Austausch im Zusammenhang mit Entfernungsanordnungen stattfindet, nicht sanktionsbewehrt ist, weil die Auflistung in Art. 18 Abs. 1 der Verordnung keinen Verweis auf Art. 15 Abs. 2 enthält.

Die Strafdrohung für die in Abs. 2 angeführten Tatbestände umfasst angesichts der gegenüber den Verstößen nach Abs. 1 größeren Bedeutung für das ordnungsgemäße Funktionieren des Systems der Bekämpfung von terroristischen Inhalten eine Bandbreite von „*bis zu 500 000 Euro*“. Davon erfasst sind Verpflichtungen zur Ausgestaltung der Nutzungsbedingungen, die Pflicht zur Veranlassung spezifischer Maßnahmen, die im Sinne der Meinungsäußerungsfreiheit normierte Verpflichtung zur Wiederherstellung von entfernten Inhalten (nach behördlicher oder eigener Prüfung), die Verpflichtung, die spezifischen Maßnahmen nach einer behördlichen Entscheidung anzupassen, sowie die Verpflichtung zur Bereitstellung eines wirksamen und zugänglichen Beschwerdemechanismus. Von ähnlicher zentraler Bedeutung für ein reibungsloses Funktionieren des Systems der Zusammenarbeit zwischen Behörden und Anbietern im Kampf gegen den Missbrauch von Hostingdiensten sind die Informationspflichten im Fall von Kenntnissen über terroristische Inhalte und die Pflicht zur Bestellung eines anordnungsbefugten gesetzlichen Vertreters.

Nach Abs. 3 mit einer Strafdrohung von „*bis zu 1 Mio Euro*“ versehen sind schließlich solche Verstöße, die für die öffentliche Sicherheit (vgl. ErwG 10 der Verordnung) und die öffentliche Ordnung eine besonders große Bedrohung darstellen und für die Bürgerinnen und Bürger, ja für die Gesellschaft insgesamt besonders schwerwiegende negative Folgen haben können (vgl. ErwG 5 der Verordnung). Für jene Fälle, in denen ein Hostingdiensteanbieter der entsprechenden behördlichen Anordnung zur Entfernung oder Sperrung des als „terroristisch“ eingestuften Inhalts nicht schnellstmöglich nachkommt, ist daher (abgesehen von der Regelung in Abs. 4) die schärfste Sanktion vorgesehen, um die Bekämpfung der Verbreitung effektiv werden zu lassen.

In Bezug auf die einzelnen mit Strafsanktion bewehrten Bestimmungen der Verordnung ist anhand der auf sie bezogenen ErwG noch Folgendes zum Verständnis festzuhalten:

Unter den in Art. 6 genannten, vom Hostingdiensteanbieter zu speichernden „*zugehörigen Daten*“ (vgl. § 7 Abs. 1 Z 4 dieses Entwurfs) sind nach ErwG 26 der Verordnung „*beispielsweise Teilnehmerdaten, insbesondere Daten, die sich auf die Identität des Inhalteanbieters beziehen, sowie Zugangsdaten umfassen, darunter das Datum und die Uhrzeit der Nutzung und die Anmeldung bei und Abmeldung von dem Dienst, zusammen mit der IP-Adresse, die der Internetzugangsanbieter dem Inhalteanbieter zuweist*“, zu verstehen.

Der aufgrund von Art. 10 der Verordnung vom Hostingdiensteanbieter verpflichtend vorzusehende Beschwerdemechanismus (vgl. § 7 Abs. 2 Z 5 und 6 sowie § 7 Abs. 1 Z 7 dieses Entwurfs) stellt laut ErwG 33 der Verordnung „*eine notwendige Schutzvorkehrung gegen die irrtümliche Entfernung oder Sperrung von Online-Inhalten dar, wenn der Inhalt im Rahmen der Meinungs- und Informationsfreiheit geschützt*“ ist. Die Hostingdiensteanbieter sollten daher „*benutzerfreundliche Beschwerdeverfahren einrichten*“ und dafür sorgen, dass Beschwerden unverzüglich und „*in voller Transparenz gegenüber dem Inhalteanbieter*“ bearbeitet werden.

Zur Verpflichtung des Hostingdiensteanbieters nach Art. 14 Abs. 5 der Verordnung (vgl. § 7 Abs. 2 Z 7 des Entwurfs) legt deren ErwG 41 dar, dass im Sinn der Verhältnismäßigkeit die Unterrichtungspflicht nicht bedeuten soll, dass sich die Hostingdiensteanbieter aktiv um Nachweise der von Abs. 5 verlangten unmittelbaren Bedrohung von Leben oder einer vermuteten terroristischen Straftat bemühen müssen. „*Als betreffender Mitgliedstaat sollte der Mitgliedstaat gelten, der für die Ermittlung und strafrechtliche Verfolgung der genannten terroristischen Straftaten zuständig ist, und zwar auf der Grundlage der Staatsangehörigkeit des Täters bzw. des potenziellen Opfers der Straftat oder des Erfolgsorts der terroristischen Handlung. Im Zweifelsfall sollten Hostingdiensteanbieter die Informationen an Europol übermitteln, das entsprechend seinem Mandat die entsprechenden Folgemaßnahmen ergreift, auch durch die Weiterleitung dieser Informationen an die zuständigen nationalen Behörden. Die zuständigen Behörden der Mitgliedstaaten sollten die Möglichkeit haben, solche Informationen zu nutzen, um Ermittlungsmaßnahmen zu ergreifen, die nach den Unions- oder nationalen Rechtsvorschriften zur Verfügung stehen*.“ In dem dargestellten Sinn wird dem Hostingdiensteanbieter allerdings angesichts der Dringlichkeit der Verständigung nicht eine Detailrecherche über mögliche Täter oder Opfer oder den Tatort zuzumuten sein, um überhaupt bestimmen zu können, welche Strafverfolgungsbehörde in welchem Staat aufgrund welches Anknüpfungspunktes zuständig sein könnte und an wen die Information zu richten wäre.

Zur in Art. 15 Abs. 1 geregelten Pflicht des Hostingdiensteanbieters (vgl. § 7 Abs. 1 Z 9 des vorliegenden Gesetzentwurfs), eine Kontaktstelle zu benennen oder einrichten, führt ErwG 42 der Verordnung aus, dass diese Stelle „*in einer speziellen – internen oder ausgelagerten – Einrichtung bestehen*“ sollte, die die elektronische Übermittlung von Entfernungsanordnungen ermöglicht, sowie „*technisch oder personell so ausgestattet ist, dass eine unverzügliche Bearbeitung solcher Anordnungen möglich ist. Die Kontaktstelle muss sich nicht in der Union befinden*.“ Damit terroristische Inhalte innerhalb einer Stunde nach Eingang der Entfernungsanordnung entfernt oder gesperrt werden, „*sollte die Kontaktstelle eines Hostingdiensteanbieters, der terroristischen Inhalten ausgesetzt ist, ständig rund um die Uhr erreichbar sein. In den Informationen über die Kontaktstelle sollte die Sprache angegeben werden, in der die Kontaktstelle erreicht werden kann. Um die Kommunikation zwischen den Hostingdiensteanbietern und den zuständigen Behörden zu erleichtern, wird den Hostingdiensteanbietern empfohlen, die Kommunikation in einer der Amtssprachen der Unionsorgane, in der ihre Nutzungsbedingungen verfügbar sind, zu ermöglichen.*“

Der Verweis in § 7 Abs. 4 auf die Erhöhung der Strafdrohung entspricht der Vorgabe des Art. 18 Abs. 3 der Verordnung, während § 7 Abs. 5 deutlich macht, dass die in Art. 18 Abs. 2 der Verordnung angeführten Erschwernis- und Milderungsgründe und an Sachlichkeitsüberlegungen orientierten Bemessungsgrundsätze zu berücksichtigen sind. Diese sind

- die Art, Schwere und Dauer des Verstoßes;
- die Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde;
- frühere Verstöße des Hostingdiensteanbieters;
- die Finanzkraft des Hostingdiensteanbieters;
- die Bereitschaft des Hostingdiensteanbieters, mit den zuständigen Behörden zusammenzuarbeiten;
- die Art und Größe des Hostingdiensteanbieters, insb. ob es sich um ein Kleinstunternehmen oder ein kleines oder mittleres Unternehmen handelt;
- das Maß des Verschuldens des Hostingdiensteanbieters unter Berücksichtigung der technischen und organisatorischen Maßnahmen, die vom Hostingdiensteanbieter ergriffen wurden, um der Verordnung nachzukommen.

Zur Höhe einer von einer Verwaltungsbehörde verhängten Geldstrafe ist auf die Rechtsprechung des Verfassungsgerichtshofs hinzuweisen, derzufolge sich die Höhe der angedrohten Sanktion im Ergebnis als kein taugliches Mittel für die Abgrenzung des gerichtlichen Strafrechts und des Verwaltungsstrafrechts erweist und der Gesetzgeber durch Art. 91 BVG nicht verpflichtet ist, Verfahren über die Verhängung der in § 99d BWG angedrohten Geldstrafen angesichts deren spezifischer Funktion im gerichtlichen Strafrecht und im Verwaltungsstrafrecht in die Zuständigkeit der ordentlichen (Straf-)Gerichte zu übertragen (vgl. das Erkenntnis des Verfassungsgerichtshofs vom 13. Dezember 2017, G 408/2016 ua., Rz 62 ff).

Zu § 9:

Wie bereits oben erwähnt gilt die Verordnung seit dem 7. Juni 2022 unmittelbar in jedem Mitliedstaat. Da die gegenständliche flankierende gesetzliche Maßnahme zur Verordnung zu diesem Zeitpunkt noch nicht in Kraft getreten war, hat die Kommission gegen die Republik Österreich – wie gegen zahlreiche andere Mitgliedstaaten auch – ein Vertragsverletzungsverfahren (Nr. 2022/2111) eingeleitet.

Zur Vermeidung einer – von Art. 7 Abs. 1 EMRK verpönten – Rückwirkung einer Strafbestimmung wird normiert, dass das ganze Bundesgesetz – mit Ausnahme der Strafbestimmung (§ 7) – mit 1. Juli 2023 in Kraft tritt, § 7 hingegen erst mit dem Ablauf des Tages der Kundmachung im Bundesgesetzblatt.

Zu Art. 2 (Änderung des KommAustria-Gesetzes)

Zu § 2 Abs. 1 und 3, § 3, § 13 Abs. 4 und § 18 Abs. 3 Z 1:

Bei den Änderungen in § 2 handelt es sich um die erforderlichen Anpassungen des KommAustria-Gesetzes im Aufgabenkatalog der Behörde und bei den Zielbestimmungen. Außerdem ist für die Festlegung der Zuständigkeit auch eine Zuweisung der Aufgaben vorzunehmen. Um den von der Verordnung angestrebten Schutz der öffentlichen Sicherheit wirksam zu gewährleisten und rasch die entsprechenden Maßnahmen zu veranlassen und die diesbezüglichen Entscheidungen ohne unnötigen Aufschub treffen zu können, sieht das Gesetzesvorhaben durch die Ergänzung von § 13 Abs. 4 die Zuständigkeit eines Einzelmitglieds vor. Im Hinblick auf die neu hinzukommenden Aufgaben, die auch eine jederzeitige Erreichbarkeit zur Erlassung von Entfernungsanordnungen voraussetzen, wird mit der Änderung in § 3 eine Erhöhung der Mitgliederzahl der Behörde von fünf auf sieben Personen vorgeschlagen.

Die nunmehr neu hinzukommenden Aufgabenstellungen im Zusammenhang mit der gegenständlichen Verordnung, die neben der Führung von Verwaltungs(-straf)verfahren auch die Lösung neuartiger Rechtsfragen mit sich bringen, bedingen eine Erhöhung der Zahl der Mitglieder der KommAustria.

Die Ergänzung in § 18 Abs. 3 Z 1 dient der Klarstellung.

Zu § 17 Abs. 1:

Da eine derartige Bestimmung bislang nicht im KOG enthalten ist, soll sie zur Klarstellung des datenschutzrechtlichen Verhältnisses zwischen der unterstützend tätigen RTR-GmbH, Fachbereich Medien, und der gemäß DSGVO verantwortlichen KommAustria eingefügt werden. Die sich aus dieser Rollenverteilung ergebenden Pflichten sind in einer Auftragsverarbeitungs-Vereinbarung im Sinne des Art. 28 Abs. 3 DSGVO festzulegen.

Zu § 35 Abs. 1c:

Bei den dieser Änderung zugrundeliegenden Überlegungen spielen die Darlegungen des VfGH im Erkenntnis VfSlg 17.326/2004 eine tragende Rolle. An der Erfüllung der die Bekämpfung der Verbreitung terroristischer Inhalte betreffenden Aufgaben und Ziele, die in § 2 KOG umschrieben sind, besteht eindeutig ein weitaus überwiegendes Interesse der Allgemeinheit, das sich vom Interesse der Marktteilnehmer an einem geordneten Rundfunkmarkt deutlich unterscheidet. Insoweit muss daher auch die Finanzierung einer solchen Aufgabe durch die Allgemeinheit, somit aus Steuermitteln, erfolgen. Betrachtet man daher das „Gewicht der die Allgemeinheit berührenden Aufgaben und Ziele“, nämlich den Schutz der öffentlichen Sicherheit und die Stärkung des Vertrauens der NutzerInnen in das Online-Umfeld oder auch die Erhöhung der Schutzvorkehrungen für die Meinungsfreiheit (wie es etwa ErwG 1 der Verordnung formuliert), ist eine Finanzierung aus öffentlichen Mitteln geboten.

Hinzu tritt auch die Tatsache, dass der Kreis der zumindest potentiell von der Regulierung erfassten Unternehmen größer ist als bei der kleinen Anzahl an „Regulierten“ im Fall des KoPl-G und auch im Fall des 9b. Abschnitts des AMD-G (in Verbindung mit § 35a KOG). Es sprechen daher auch verwaltungsökonomische Überlegungen dafür, im Hinblick auf das weitere angestrebte Ziel der Rechtssicherheit und Verhinderung des Missbrauchs von Hostingdiensten für terroristische Zwecke die Finanzierung aus öffentlichen Mitteln zu bestreiten.

Zu § 39:

Aus § 36 KOG ergibt sich, dass das Bundesverwaltungsgericht in jenen Fällen als Beschwerdeinstanz entscheidet, in denen die KommAustria belangte Behörde ist. Abweichend vom in § 13 Abs. 1 VwGVG normierten allgemeinen Prinzip der aufschiebenden Wirkung von Beschwerden wird im Fall von Entfernungsanordnungen und der Überprüfung von Entfernungsanordnungen sowie für Entscheidungen über die Angemessenheit von Maßnahmen (wie auch schon für andere Rechtsmaterien nach dem ORF-G, dem PrR-G, dem AMD-G und dem TKG) normiert, dass einer Beschwerde keine derartige Wirkung zukommt. Auf diese Weise wird auch sichergestellt, dass im Sinne des Rechts auf Meinungsäußerungsfreiheit Entscheidungen, wonach eine Entfernung nicht gerechtfertigt war, sofort wirksam werden. Das BVwG kann aber etwa in eben diesem Sinn einer Entfernungsanordnung auch auf Antrag aufschiebende Wirkung zuerkennen.

Zu § 44:

Mit der Regelung zu den vorbereitenden Maßnahmen soll sichergestellt sein, dass die notwendigen organisatorischen Schritte und die Vorausplanung für die Auswahl des zusätzlich benötigten Personals rechtzeitig in Angriff genommen werden können.

Zu § 45 Abs. 20:

Die aktuellen (fünf) Mitglieder der KommAustria wurden per 1. Oktober 2022 für die Dauer von sechs Jahren ernannt. Damit im Lauf des Jahres 2028 alle (sieben) Mitglieder gemeinsam bestellt werden können, ist vorzusehen, dass die beiden zusätzlichen Mitglieder nicht für volle sechs Jahre bestellt werden, sondern dass ihre Bestellung gleichzeitig mit den aktuellen (fünf) Mitgliedern ausläuft.