VEREINIGUNG DER ÖSTERREICHISCHEN RICHTERINNEN UND RICHTER

Bundesvertretung
Richter und Staatsanwälte

An das Präsidium des Nationalrats
begutachtungsverfahren@parlament.gv.at

An das Bundesministerium für Justiz
team.s@bmj.gv.at

Wien, am 21. August 2017

Bundesgesetz, mit dem die Strafprozessordnung 1975 geändert wird (Strafprozessrechtsänderungsgesetz 2017)

GZ.: BMJ-S578.031/0008-IV 3/2017

Die Vereinigung der österreichischen Richterinnen und Richter (unter Einbeziehung der Fachgruppe Grundrechte und interdisziplinärer Austausch, der Fachgruppe Strafrecht sowie umfangreicher Anmerkungen aus der Praxis) und die Bundesvertretung Richter und Staatsanwälte in der GÖD erstatten zum oben angeführten Gesetzesvorhaben folgende

S t e l l u n g n a h m e :

1. Allgemein:

Technischer Fortschritt darf keine „blinden Flecken“ im Bereich der Strafverfolgung hinterlassen. Die technische Weiterentwicklung verschiedener Kommunikationsformen und das geänderte Nutzerverhalten erfordern Maßnahmen, die auch in Zukunft eine umfassende und effektive Aufklärung und Verfolgung von Straftaten sicherstellen. Es besteht daher unzweifelhaft Regelungsbedarf, sodass diese Gesetzesinitiative grundsätzlich begrüßt wird. Stets zwingende Voraussetzungen für solch erforderliche Grundrechtseingriffe sind jedoch eine strenge Verhältnismäßigkeitsprüfung, vorangehende staatsanwaltschaftliche Prüfung, richterliche Bewilligung bzw Ablehnung im Einzelfall und daran anschließende Rechtsschutzmöglichkeiten. Diesen Anforderungen wird der Entwurf teilweise nicht gerecht und werden die Bedenken unten im Detail ausgeführt.

Neue Aufklärungsinstrumente erfordern zwingend auch zusätzliche personelle und damit auch finanzielle Ressourcen. Diese sind vor Inkrafttreten der Regelung auch im Bereich der Justiz (und nicht nur im Innenressort, das die wirkungsorientierte Folgenabschätzung ausschließlich nennt) sicherzustellen.

Schmerlingplatz 11, Postfach 26, A-1011 Wien
T +43 1 52152 303644, F +43 1 52152 303643
ute.beneke@richtervereinigung.at
www.richtervereinigung.at

2. im Besonderen:

Transparenz der gesetzgeberischen Intention:

Durch die Verwendung eines „technischen Verständnisses“ des Begriffs „Nachricht“ (welcher von einem „sozialen“ unterschieden wird) fällt jede verschlüsselte Übermittlung von Daten „über ein Kommunikationsnetz oder einen Dienst der Informationsgesellschaft“ unter die vorgeschlagene Maßnahme der Überwachung verschlüsselter Nachrichten (§ 134 Z 3a StPO). Damit ist auch jedes (verschlüsselte) „Übermitteln eines Datenpakets an einen Cloud-Server“ (etwa auch von Dokumenten eines Textverarbeitungsprogramms) oder „das Abspeichern von E-Mail-Entwürfen über ein Webmail-Programm“ erfasst, ohne dass der Nutzer des Computers iS eines herkömmlichen strafrechtlichen Begriffsverständnisses (vgl *Lewisch* in WK^2 StGB § 119 Rz 9a) Gedankeninhalte einem (oder mehreren) anderen (bewusst) mitteilt. Lediglich das Abspeichern auf einer lokalen Festplatte oder das Übermitteln auf einen USB-Stick fiele nicht darunter (ausdrücklich etwa S 9 der Erläuterungen). Auch wenn dies einem schon bisher zu § 134 Z 3 StPO vertretenen technischen Begriffsverständnis entsprechen soll (so S 5 der Erläuterungen), ermöglicht erst die vorgeschlagene Installation eines Programms in einem Computersystem (Schadsoftware) samt „Remote-Zugriff“ auf das System dessen weitgehende „Online-Überwachung“. So gesehen geht es nicht bloß um die Schließung einer Lücke, die sich durch die Verlagerung von Kommunikationsverhalten auf internetbasierte, verschlüsselte Dienste ergeben hat. Die mehrfach betonte Abgrenzung zur „Online-Durchsuchung“ (die bloß lokal abgespeicherte Daten beträfe) wird – zumal in Zeiten zunehmender Nutzung dislozierter Speicherkapazitäten („Clouds“) – stark relativiert.

Die vorgeschlagene Maßnahme greift daher wohl nicht bloß in das Fernmeldegeheimnis ein, sondern darüber hinaus in ein – in der deutschen Rsp eigenständig anerkanntes – „IT-Grundrecht“ (ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ [vgl dazu *Reindl-Krauskopf*, WK-StPO § 134 Rz 58/3 und die in den Erläuterungen auf S 8 zusammengefassten Ausführungen von *Zerbes*]). Ob die im Entwurf vertretene Position tatsächlich aus der dort zitierten Entscheidung des deutschen BVerfG (2 BvR 1454/13 [welche nur das Aufrufen von Websites, also das Surfverhalten einer Person betraf]) ableitbar ist, erscheint fraglich.

Sollte das Anliegen des Entwurfs hingegen (auch) sein, aus der dislozierten Speicherung von Daten („Clouds“) entstehenden Schwierigkeiten bei (unter eigenen Voraussetzungen zulässiger) Sicherstellung oder Beschlagnahme entgegenzuwirken, wäre eine (systemkonforme) Regelung im ersten Abschnitt des 8. Hauptstücks der StPO zu überlegen.

Intensität des Grundrechtseingriffes:

Aus den zuvor genannten Gründen wird die im Entwurf vertretene Ansicht, die Überwachung verschlüsselter Nachrichten (§ 134 Z 3a StPO) sei von der Intensität des Grundrechtseingriffes mit der (bereits bestehenden) Überwachung von Nachrichten (§ 134 Z 3 StPO) vergleichbar, nicht geteilt. Neben der – zumindest vorübergehenden – Beeinträchtigung des Computersystems durch die Schadsoftware und der umfassenden Überwachungsmöglichkeit ist auch die vorgeschlagene Möglichkeit des (geheimen) Eindringens in durch das Hausrecht geschützte Räume samt Durchsuchung von Behältnissen und Überwindung spezifischer Sicherheitsvorkehrungen zur

Vorbereitung der eigentlichen Überwachung zu berücksichtigen. Zwar bedarf dies einer gesonderten gerichtlichen Bewilligung (§ 137 Abs 1 StPO), doch ist ein vergleichbarer (geheimer) Grundrechtseingriff derzeit nur im Zusammenhang mit der optischen und akustischen Überwachung von Personen („Lausch- und Spähangriff“) vorgesehen (§ 136 Abs 2 StPO). Höhere Eingriffsschranken (im Vergleich zur herkömmlichen Überwachung von Nachrichten) sind daher aus diesem Grund und nicht bloß aus Gründen der Schonung von Polizeiressourcen (vgl S 10 der Erläuterungen) gerechtfertigt. Eine Angleichung der Zulässigkeitsvoraussetzung noch vor Ende der Befristung (von 5 Jahren) wird daher nicht befürwortet.

Begleitende Maßnahmen:

Grundsätzlich positiv sind die begleitenden Maßnahmen zur Vermeidung von Missbrauch der Überwachung verschlüsselter Nachrichten zu sehen. Das vorgeschlagene Verwendungsverbot (§140 Abs 1 StPO) scheint aber durch die ausdrückliche Bezugnahme auf die Begriffsdefinition von „Ergebnis“ (§ 134 Z 5) zu eng, weil darunter – soweit hier von Interesse – bloß „die verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten und Informationen im Sinne von Z 3 sowie damit in Zusammenhang stehende Daten im Sinn des § 76a und des § 92 Abs 3 Z 4 und 4a TKG“ gemeint sind. Auf einer lokalen Festplatte abgespeicherte sonstige Daten, die im Zuge einer – unter Überschreitung der Befugnis – vorgenommenen „Online-Durchsuchung“ ermittelt werden, wären also von diesem Verwendungsverbot bei wortgetreuer Gesetzesinterpretation nicht erfasst (ebenso wenig sonstige Informationen, die beim geheimen Eindringen in die Wohnung nach § 135a Abs 3 StPO „zufällig“ gewonnen werden).

Akustische Überwachung in Fahrzeugen:

Schließlich wird keine Begründung für die (kriminalpolitische) Notwendigkeit der (neuen) Möglichkeit, eine akustische Überwachung in Fahrzeugen unter vereinfachten Voraussetzungen (des § 135 Abs 3 StPO) durchzuführen, gegeben. Die Erläuterungen beschränken sich auf das Argument, eine solche Überwachung sei – wegen des fehlenden Eingriffs in das Hausrecht – weniger eingriffsintensiv als die (bestehende) akustische Überwachung von Personen (§ 136 StPO). Abgesehen davon, dass auch diese Maßnahme die Verletzung des Hausrechts keineswegs zwingend voraussetzt (vgl § 136 Abs 2 StPO), umfasst der Begriff „Fahrzeug“ nicht bloß (private) Pkw, sondern etwa auch Massenbeförderungsmittel, deren akustische Überwachung mit einem (gravierenden) Eingriff in Grundrechte (einer unter Umständen größeren Zahl) von Dritten verbunden wäre.

3. Weitere Anmerkungen im Detail:

Lokalisierung einer technischen Einrichtung:

Die Schaffung einer eigenen gesetzlichen Grundlage für die Feststellung von geographischen Standorten und der IMSI unter Einsatz technischer Mittel wird ausdrücklich begrüßt. Nachdrücklich hinzuweisen ist jedoch auf Folgendes:

Den Erläuterungen zu Folge soll zur Durchführung der Maßnahme der sogenannte IMSI-Catcher zum Einsatz gelangen. Da die Erläuterungen darauf nicht eingehen, ist jedoch anzumerken, dass es mit IMSI-Catchern offenbar auch möglich ist, Mobilfunkgeräte abzuhören[1], also den Inhalt der über das Mobiltelefon abgewickelten Gespräche zu überwachen. Wird ein Gespräch mittels IMSI-Catcher überwacht, so handelt es sich dabei nicht um eine Überwachung von Nachrichten im Sinne des § 134 Z 3 StPO, die durch Mitwirkung der Mobilfunkbetreiber erfolgt, sondern vielmehr um eine akustische Überwachung von Personen im Sinne des § 134 Z 4 StPO. Da eine solche Überwachung wohl in aller Regel in Unkenntnis der betroffenen Person(en) erfolgen wird, wird es sich in aller Regel um einen sogenannten „großen Lauschangriff" handeln, für den § 136 Abs. 1 Z 3 StPO äußerst enge Zulässigkeitsvoraussetzungen festlegt (drohende Freiheitsstrafe von mehr als zehn Jahren oder strafbare Handlungen im Rahmen krimineller Organisationen oder terroristischer Vereinigungen samt zusätzlicher Bedingungen). Ob mit allen IMSI-Catchern eine akustische Überwachung möglich ist, oder ob es auch IMSI-Catcher gibt, die nur Standortdaten und die IMSI auslesen, ist uns nicht bekannt; ebenso, ob mit den von den Sicherheitsbehörden verwendeten IMSI-Catchern die Überwachung von Gesprächen möglich ist. Dies sollte aber jedenfalls vor Verabschiedung des Gesetzes geprüft werden. Zwar ist der Missbrauch von Abhörgeräten strafrechtlich sanktioniert (§ 120 StGB) und ist davon auszugehen, dass die Sicherheitsbehörden IMSI-Catcher nur bei Vorliegen der rechtlichen Voraussetzungen zur akustischen Überwachung von Personen einsetzen. Da hier ein äußerst sensibler Bereich des Schutzes der Privatsphäre betroffen ist, sollte durch geeignete zusätzliche Maßnahmen sichergestellt werden, dass der IMSI-Catcher zur akustischen Überwachung nur unter den engen Voraussetzungen des § 136 Abs. 1 StPO verwendet wird.

Zur Überwachung verschlüsselter Nachrichten:

Die Einführung dieser neuen Überwachungsmöglichkeit wird ausdrücklich begrüßt, weil aus der Praxis bekannt ist, dass sich insbesondere kriminelle und terroristische Vereinigungen, wohl aber auch kriminelle Organisationen bei der Begehung strafbarer Handlungen gezielt verschlüsselter Internetkommunikation bedienen, um sich der herkömmlichen Überwachung von Nachrichten zu entziehen. Immer wieder verlaufen aus diesem Grund Ermittlungen gegen diese Gruppen letztendlich ergebnislos.

Nicht geteilt wird hingegen die Auffassung der eingesetzten Expertengruppe, wonach zwischen der inhaltlichen Überwachung von SMS (also der herkömmlichen Überwachung von Nachrichten) einerseits und der inhaltlichen Überwachung von WhatsApp-, Viber- und sonstiger verschlüsselter

[1] http://www.zeit.de/digital/mobil/2014-09/mobilfunk-imsi-catcher-handy und http://www.handynummerorten.eu/imsi-catcher-helfer-bei-der-polizeilichen-ueberwachung/#einsatz; beides abgerufen am 28.7.2017

Kommunikation (also der geplanten Überwachung verschlüsselter Nachrichten) andererseits kein Wertungsunterschied bestehe. Anders als die Kommunikation per SMS sind nämlich die erwähnten im Wege des Internets übermittelten Nachrichten verschlüsselt, und es ist davon auszugehen, dass die Nutzer diese neuen Kommunikationsmittel (neben vielen anderen Vorteilen, die internetbasierte Kommunikation zweifelsohne bietet) auch deshalb nutzen, weil sie sich davon einen erhöhten Schutz ihrer Kommunikation vor Eingriffen Dritter erhoffen. Zudem ist es für die Überwachung verschlüsselter Nachrichten erforderlich, geheim Programme auf privaten Computersystemen zu installieren. Die Überwachung verschlüsselter Nachrichten ist daher ein deutlich intensiverer Grundrechtseingriff als die Überwachung unverschlüsselter SMS-Kommunikation, weshalb auch die Voraussetzungen für die Überwachung verschlüsselter Nachrichten enger zu fassen sind als jene für die Überwachung der SMS-Kommunikation.

Vor diesem Hintergrund wird es zwar grundsätzlich begrüßt, dass im Entwurf schon jetzt zumeist höhere Schranken für die Überwachung verschlüsselter Nachrichten vorgesehen sind als für die herkömmliche Überwachung von Nachrichten. Allerdings sieht der Entwurf vor, dass die Überwachung verschlüsselter Nachrichten zur Aufklärung aller Straftaten zulässig sein soll, die der Zuständigkeit des Landesgerichts als Schöffen- oder Geschworenengericht (§ 31 Abs. 2 und 3 StPO) unterliegen (§ 135a Abs. 1 Z 3 StPO). § 31 Abs. 2 und 3 StPO listen vorwiegend Verbrechen, aber auch einige Vergehen auf. So fällt in die Zuständigkeit des Landesgerichts als Geschworenengericht etwa das Vergehen der Herabwürdigung des Staates und seiner Symbole nach § 248 StGB, das mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen ist (§ 31 Abs. 2 Z 5 StPO) oder das Vergehen der Aufforderung zu mit Strafe bedrohten Handlungen und Gutheißung mit Strafe bedrohter Handlungen nach § 282 StGB, das mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen ist (§ 31 Abs. 2 Z 11 StPO). In die Zuständigkeit des Landesgerichts als Schöffengericht fällt etwa auch das Hauptverfahren für das Vergehen der schweren gemeinschaftlichen Gewalt nach § 274 Abs. 1 StGB (§ 31 Abs. 3 Z 5 StPO), das mit Freiheitsstrafe bis zu zwei Jahren bedroht ist.

Die Zulässigkeit einer Überwachung verschlüsselter Nachrichten sollte davon abhängen, ob sie zum angestrebten Erfolg in angemessenem Verhältnis steht. Dies hängt ganz maßgeblich davon ab, mit welcher Strafe die jeweils aufzuklärende Straftat bedroht ist. In diesem Sinne knüpft auch die Zulässigkeit der schon jetzt in der StPO normierten Maßnahmen der Überwachung von Nachrichten oder der optischen und akustischen Überwachung – Entführungen ausgenommen – an die Strafdrohung an, ohne auf einen Deliktskatalog zu verweisen. Der bislang beschrittene Weg sollte weiter gegangen werden sollte. Die Einführung eines Verweises auf die Deliktskataloge des § 31 Abs. 2 und 3 StPO und damit einer dynamischen Verweisung würde schon jetzt – wie gezeigt – dazu führen, dass die Überwachung verschlüsselter Nachrichten zur Aufklärung von Delikten zum Einsatz gelangen könnte, bei denen dies wohl außer Verhältnis zur Schwere der Tat stünde (etwa bei § 248 StGB). Dazu kommt, dass insbesondere in jüngerer Vergangenheit die Zuständigkeit des Landesgerichts als Schöffengericht häufig legistischem Wandel unterlag, und dass die Frage, ob der Einzelrichter oder das Gericht als Schöffen- oder als Geschworenengericht entscheiden soll, häufig von rechtspolitischen Erwägungen abhängt, die mit der Frage der Verhältnismäßigkeit der Durchführung einer Ermittlungsmaßnahme in keinerlei Zusammenhang steht; dies könnte in Hinkunft zu vollkommen unerwünschten Ergebnissen führen. Eine derartige Situation besteht übrigens derzeit schon in Deutschland, wo Ermittlungsmaßnahmen jeweils nur zur Aufklärung von in Katalogen angeführten Straftaten zulässig sind, was mitunter willkürlich erscheint. Ein Verweis auf Deliktskataloge sollte daher unbedingt vermieden werden. Wie bei den schon bestehenden Ermittlungsmaßnahmen sollte an eine konkrete Strafdrohung angeknüpft werden, wobei angeregt wird, die Maßnahme für die Dauer der fünf Jahre, für die sie vorerst eingeführt werden soll, auf

Verbrechen (§ 17 Abs. 1 StGB) zu beschränken.

Anmerkungen zu § 135a StPO:

Z 16 des Entwurfes sieht vor, dass § 135a Abs. 2 Z 1 StPO lautet wie folgt:

„Eine Überwachung verschlüsselter Nachrichten ist überdies nur dann zulässig, wenn das Programm nach Beendigung der Ermittlungsmaßnahme funktionsunfähig ist oder ohne dauerhafte Schädigung oder Beeinträchtigung des Computersystems, in dem es installiert wurde, und der in ihm gespeicherten Daten entfernt werden kann, (…)“

Dazu ist Folgendes anzumerken:

1. Ob das Programm nach Beendigung der Maßnahme funktionsunfähig ist, lässt sich im Zeitpunkt der Bewilligung der Maßnahme gewöhnlich nur bedingt beurteilen. Es wird daher vorgeschlagen, stattdessen die Voraussetzung vorzusehen, dass das Programm mit einem Mechanismus ausgestattet sein muss, mit dem es (aller Voraussicht nach) nach Beendigung der Maßnahme funktionsunfähig gemacht werden kann.
2. Aus dem Wort „oder“ könnte sich allenfalls erschließen, dass eine dauerhafte Schädigung des Computersystems in Kauf zu nehmen wäre, wenn das Programm nach Beendigung der Ermittlungsmaßnahme (nur) funktionsunfähig wird, aber im betroffenen Computersystem (schädigend) erhalten bleibt. Kann es hingegen entfernt werden, darf eine solche Schädigung nicht eintreten. Eine diesbezügliche legistische Klarstellung, wonach stets bei strenger ex ante-Prüfung keine Schädigung zu befürchten ist, wird angeregt.

Gemäß § 135a Abs. 3 StPO soll es zulässig sein, in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume einzudringen und Behältnisse zu durchsuchen, um die Installation des Programms zur Überwachung verschlüsselter Nachrichten in dem Computersystem zu ermöglichen. Vom Durchsuchen sonstiger Orte und Gegenstände (etwa von Fahrzeugen) ist hingegen nicht die Rede. Vermutlich wird davon ausgegangen, die §§ 119ff StPO böten eine ausreichende Grundlage für deren Durchsuchung. Dazu ist jedoch anzumerken, dass die Durchsuchung von Orten und Gegenständen gemäß § 119 Abs. 1 StPO – soweit hier wesentlich – nur zulässig ist, wenn anzunehmen ist, dass sich dort Gegenstände befinden, die sicherzustellen oder auszuwerten sind. Computersysteme, in die ein Überwachungsprogramm eingeschleust werden soll, werden jedoch regelmäßig nicht sicherzustellen oder auszuwerten sein, sondern (mit Ausnahme der vorgenommenen Installation) möglichst unverändert an Ort und Stelle zu belassen sein, um zu verhindern, dass der Betroffene Kenntnis von der Überwachung erlangt. Es wird daher angeregt, die Befugnisse auf andere Orte und Gegenstände auszuweiten oder (dies wäre vermutlich die legistisch elegantere Variante) die §§119ff StPO zu ergänzen und die Zulässigkeit der Durchsuchung von Orten und Gegenständen (allenfalls auch Personen?) auch für den Fall für zulässig zu erklären, in dem dies zur Durchführung einer Maßnahme nach § 135a StPO erforderlich ist.

Beschlagnahme von Briefen:

Nicht unproblematisch ist der beabsichtigte Entfall des § 137 Abs. 2 StPO und damit des Erfordernisses, der von der Sicherstellung betroffenen Person längstens binnen 24 Stunden eine Bestätigung über die Sicherstellung zuzustellen und sie über ihre Rechte zu informieren, sowie des

Rechtes, auf die Durchführung eines sogenannten „Sichtungsverfahrens“ nach § 112 StPO zu bestehen.

Das Argument, es sei erforderlich, die Möglichkeit zu schaffen, aus ermittlungstaktischen Gründen die Information der betroffenen Person aufzuschieben, ist zwar verständlich und nachvollziehbar; es könnte aber auch in Bezug auf jegliche andere Sicherstellung, die die Ermittlungen gefährden könnte (etwa die eines KFZ des Beschuldigten), gleichermaßen ins Treffen geführt werden. Dennoch ist bislang ein Aufschub in § 111 StPO nicht vorgesehen, was – soweit ersichtlich – bislang offenbar auch zu keinen größeren praktischen Problemen geführt hat.

Der geplante Entfall des Verweises in § 137 Abs. 2 StPO auf § 112 StPO führt seinerseits zu einer nicht unproblematischen Differenzierung zwischen vom Briefgeheimnis umfassten Sendungen an oder von den in § 112 StPO genannten Geheimnisträgern und deren sonstigen schriftlichen Aufzeichnungen. In den Erläuterungen wird dazu argumentiert, die Staatsanwaltschaft habe ohnedies die Ergebnisse der Beschlagnahme, also den Inhalt der Briefe, zu prüfen und (nur) jene Teile zu den Akten zu nehmen, die für das Verfahren von Bedeutung seien und als Beweismittel verwendet werden dürften. Damit wird aber in diesem Bereich der Telos des § 112 StPO in Frage gestellt, soll doch diese Bestimmung gerade verhindern, dass die Ermittlungsorgane Einblick in die Unterlagen erhalten, solange sie nicht von einem Gericht gesichtet und freigegeben wurden.

Redaktionelles:

a) Zu Z 8: Unklar erscheint, weshalb sich nach der Wortfolge „sonstigen Diensteanbieters“ der Verweis auf die §§ 13, 16 und 18 Abs. 2 des E-Commerce-Gesetzes findet, die den Ausschluss der Verantwortlichkeit des Diensteanbieters bei Durchleitung (§ 13 ECG), Hosting (§ 16 ECG) und weiters „die in den §§ 13 und 16 genannten Diensteanbieter“ (§ 18 Abs. 2 ECG) nennen, wo doch §3 Z 2 ECG die Legaldefinition des Begriffs „Diensteanbieter“ enthält.

b) Zu Z 17: Der (implizite) Verweis auf § 135 Abs. 3 Z 1, 2 und 3 StPO wirkt sinnstörend, weil dort jeweils vom „Inhaber der technischen Einrichtung“ bzw. von der „technischen Einrichtung“ die Rede ist. Es bedürfte einer eigenständigen, auf die Überwachung in Fahrzeugen zugeschnittenen, Regelung.

c) Zu Z 21: In § 138 Abs. 1 Z 3 wäre wohl die Wendung „oder Überwachung verschlüsselter Nachrichten“ nach der Wendung „akustische Überwachung“ einzufügen.

d) Zu Z 32: Zwischen den Wendungen „136 Abs. 1 Z 2“ und „Abs. 1a“ wäre ein „und“ zu ergänzen.

Mag. Werner Zinkl	*Mag. Christian Haider*
Präsident	Vorsitzender