Verein Arbeitskreis Vorratsdaten Österreich (AKVorrat.at),
ZVR: 140062668
Kirchberggasse 7/5
1070 Wien
info@akvorrat.at

Wien, 26. Oktober 2014

Betreff: Stellungnahme des Arbeitskreis Vorratsdaten im Begutachtungsverfahren des 2. Abgabenänderungsgesetz 2014 (68/ME) BMF

Für den AKVorrat: Ing. Dr. iur Christof Tschohl

Der AKVorrat nimmt zu dem Begutachtungsentwurf wie folgt Stellung:

Artikel 9: Änderungen der Bundesabgabenordnung

1. In § 158 wird folgender Abs. 4d eingefügt:

„(4d) Zum Zweck der Durchführung von Abgaben- oder Monopolverfahren sind die Kriminalpolizei, die Staatsanwaltschaften und die Gerichte ermächtigt, nach der StPO ermittelte personenbezogene Daten, die für solche Verfahren bedeutsam sind, an die Abgabenbehörde zu übermitteln, wenn Grund zur Annahme besteht, dass Abgabenvorschriften oder Monopolvorschriften verletzt worden sind oder sein können."

Nach Ansicht des AKVorrat stellt diese Befugnis im Falle ihres Inkrafttretens einen unverhältnismäßigen Eingriff in das Grundrecht auf Datenschutz gem. § 1 DSG 2000 sowie in das Grundrecht auf Privatsphäre gem. Art. 8 EMRK und wäre daher verfassungswidrig.

Die Bundesregierung führt selbst in den erläuternden Bemerkungen zu dieser Norm aus: *„Als Folge der Aufhebung des § 140 Abs. 3 StPO durch den VfGH (1.10.2013, G 2/2013) erweist sich eine ausdrückliche Ermächtigung als erforderlich, abgabenrechtlich bzw. monopolrechtlich bedeutsame Umstände, die der Kriminalpolizei, einer Staatsanwaltschaft oder einem Gericht in nach der StPO geführten Ermittlungsverfahren bekannt werden, der für die Durchführung von Abgaben- bzw. Monopolverfahren zuständigen Verwaltungsbehörde zu übermitteln."*

Der Verfassungsgerichtshof (VfGH) hat mit diesem Urteil die Bestimmung des § 140 Abs. 3 StPO aufgehoben, weil die dort normierte pauschale Befugnis zur Verwertung strafgerichtlicher Ermittlungsergebnisse in anderen Gerichts- oder Verwaltungsverfahren eine Verletzung des Grundrechts auf Datenschutz bewirkt.

Der VfGH stellt klar im genannten Urteil klar, dass es zwar „dem Gesetzgeber durch das Grundrecht auf Datenschutz nicht von vornherein untersagt [ist], die Zulässigkeit einer Datenverwendung als Beweismittel in anderen Verfahren als in jenem, in dem diese Daten rechtmäßig ermittelt wurden, vorzusehen, jedoch ist ein solcher Eingriff gemäß § 1 DSG 2000 iVm Art. 8 Abs. 2 EMRK auf das erforderliche, geeignete und verhältnismäßige Maß zu beschränken (vgl. VfSlg. 18.975/2009 mwN).

Der Gesetzgeber darf daher die Verwertung von personenbezogenen Daten, die in einem Strafverfahren erhoben wurden, in sonstigen (gerichtlichen oder verwaltungsbehördlichen) Verfahren nur insoweit vorsehen, als der Zweck der Datenverwendung in diesen Verfahren ein öffentliches Interesse verfolgt, welches das Interesse des Betroffenen an der Geheimhaltung (bzw. Löschung) der Daten übersteigt“ (VfGH G 2/2013 - 17, 01.10.2013, RZ 27).

Wie schon die Aufgehobene Bestimmung des § 140 Abs. 3 StPO bewirkt auch der vorgeschlagene § 158 Abs. 4d BAO, dass in ordnungsgemäßer Weise ermittelte Ergebnisse iSd § 134 Z 5 StPO, die in Verwaltungsverfahren nach der Bundesabgabenordnung – auf welche Weise auch immer – bekannt werden, in diesen anderen Verfahren schlechthin als Beweismittel Verwendung finden können. „Dies ohne weitere Kautelen, wie etwa jene eines inhaltlichen Zusammenhanges des anderen Verfahrens mit dem Strafverfahren, in dem die Ergebnisse produziert wurden sowie jene der Gewichtung der Bedeutung der Ermittlungsergebnisse für die mit dem anderen Verfahren verfolgten öffentlichen oder berechtigten Interessen einer am anderen Verfahren beteiligten Person einerseits und des Grundrechtseingriffs für den Betroffenen durch die Weiterverwendung seiner aus einem Strafverfahren stammenden personenbezogenen Daten andererseits.“ (VfGH G 2/2013 - 17, 01.10.2013, RZ 28).

Die Norm hat somit den Inhalt, dass jedwede personenbezogenen Daten, sofern sie im Strafverfahren zulässigerweise ermittelt wurden, in jedwedem Verwaltungsverfahren nach der Bundesabgabenordnung verwendet werden dürfen, völlig unabhängig davon, ob ein Zusammenhang mit Finanzstrafverfahren besteht und eine gewisse Schwere der zu Ermittelnden Tat den Eingriff rechtfertigen könnte.

Nun will die Bundesregierung ausdrücklich die durch die Aufhebung entstandene „Lücke“ für den Bereich der Abgaben- und Monopolverfahren durch die vorgeschlagene Bestimmung schließen. Dabei wird jedoch – nicht einmal im Ansatz und weder in der Norm noch in den Erläuterungen – auf jene Auflagen Bezug genommen, welche der VfGH in seiner Begründung zur Gesetzesaufhebung formuliert.

Das Problem ist insbesondere, dass hier für Verwaltungsverfahren unabhängig von deren konkreten oder abstrakten Bedeutung und Schwere personenbezogene Daten verfügbar gemacht werden sollen, selbst wenn deren Ermittlung nach der Strafprozessordnung (StPO) nur bei einem gewissen Schweregrad zulässig sind. Die StPO enthält nämlich ein differenziertes System der Befugnisse zur Ermittlung personenbezogener Daten und Ausübung von Befehls- und Zwangsbefugnissen vor allem im 8. Hauptstück der StPO. Dort gibt es Einschränkungen bestimmter Ermittlungsbefugnisse in Relation zum Schweregrad der aufzuklärenden Straftat im Hinblick auf die Höchststrafdrohung. Begleitend gibt es prozessuale Sicherungsmaßnahmen wie insbesondere den Vorbehalt der gerichtlichen Bewilligung, die gerade die Wahrung der Recht- und Verhältnismäßigkeit im Einzelfall garantieren sollen. Bei einer erweiterten Beweisverwertung im Verfahren nach der BAO nach der vorgeschlagenen Bestimmung fehlt demgegenüber jeder Ansatz, die Wahrung der Verhältnismäßigkeit des Grundrechtseingriffs generell abstrakt oder im konkreten Einzelfall zu garantieren. Das einzige Kriterium ist, ob die Daten bzw. Informationen *„für solche Verfahren bedeutsam sind“*.

Nach Auffassung des AKVorrat ist die vorgeschlagene Bestimmung zu Ziffer 1 der Novelle daher als verfassungswidrig abzulehnen.

Artikel 10: Änderung des Finanzstrafgesetzes

3. In § 98 wird folgender Abs. 5 angefügt:

„(5) Beweismittel und Ermittlungsergebnisse einschließlich personenbezogener Daten, die in einem gerichtlichen Strafverfahren, Verwaltungsstrafverfahren oder Abgabenverfahren gewonnen werden, dürfen für Zwecke der Finanzstrafrechtspflege und damit zusammenhängender Abgabenverfahren übermittelt und verwendet werden."

Nach Ansicht des AKVorrat stellt diese Befugnis im Falle ihres Inkrafttretens einen unverhältnismäßigen Eingriff in das Grundrecht auf Datenschutz gem. § 1 DSG 2000 sowie in das Grundrecht auf Privatsphäre gem. Art. 8 EMRK und wäre daher verfassungswidrig.

Die größten Bedenken erzeugt der pauschal gewährte Zugriff auf personenbezogene Daten, die einem gerichtlichen Strafverfahren gewonnen werden, für Zwecke der Finanzstrafrechtspflege und damit zusammenhängender Abgabenverfahren. Die gegenständlich vorgeschlagene Befugnis enthält keine Unterscheidung, ob es sich um ein Finanzstrafverfahren in der Zuständigkeit der ordentlichen Gerichte (vgl. § 53 FinStrG) oder der Finanzstrafbehörden handelt. Es gibt keine Berücksichtigung der Frage, ob die selben Beweismittelerhebungen in dem Finanzstrafverfahren selbst erhoben werden dürften. Der für das Datenschutzgrundrecht zentrale Grundsatz der Zweckbindung (vgl. § 6 DSG) wird auf diese Weise vollkommen missachtet.

Damit erzeugt die vorgeschlagene Bestimmung genau dieselben Bedenken, die den VfGH zur Aufhebung des § 140 Abs. 3 StPO veranlasst haben. Um Wiederholungen zu vermeiden, wird im Übrigen auf die Ausführungen zu Artikel 9 (Änderungen der Bundesabgabenordnung) verwiesen.

Nach Auffassung des AKVorrat ist die vorgeschlagene Bestimmung zu Ziffer 3 der Novelle daher jedenfalls insofern als verfassungswidrig abzulehnen, als sie die Verwendung von strafgerichtlich gewonnenen Beweisergebnissen normiert.

4. § 99 wird wie folgt geändert:

a) In Abs. 1 wird folgender Satz angefügt: „Elektronische Daten sind in einem allgemein gebräuchlichen Dateiformat in strukturierter Form so zu übermitteln, dass diese elektronisch weiterverarbeitet werden können."

b) Es wird folgender Abs. 3a eingefügt: „(3a) Bei Verdacht auf ein vorsätzliches Finanzvergehen, ausgenommen Finanzordnungswidrigkeiten, ist die Finanzstrafbehörde auf Anordnung des Vorsitzenden des Spruchsenates, dem gemäß § 58 Abs. 2 unter den dort vorgesehenen Voraussetzungen die Durchführung der mündlichen Verhandlung und die Fällung des Erkenntnisses obliegen würde, berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 –TKG 2003, BGBl. I Nr. 70/2003) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz – ECG, BGBl. I Nr. 152/2001) auch folgende Auskünfte zu verlangen:

1. über die Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung;

2. über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war.

Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen. Die Anordnung des Vorsitzenden des Spruchsenates hat schriftlich und mit einer Begründung versehen zu ergehen. Nach Beendigung der Ermittlungsmaßnahme hat die Finanzstrafbehörde die Anordnung des Vorsitzenden des Spruchsenates dem Beschuldigten und den von der Durchführung der Ermittlungsmaßnahme Betroffenen unverzüglich zuzustellen. Die Zustellung kann jedoch aufgeschoben werden, solange durch sie der Zweck dieses oder eines anderen Verfahrens gefährdet wäre."

Nach Ansicht des AKVorrat stellt diese Befugnis im Falle ihres Inkrafttretens einen unverhältnismäßigen Eingriff in das Grundrecht auf Datenschutz gem. § 1 DSG 2000 sowie in das Grundrecht auf Privatsphäre gem. Art. 8 EMRK und wäre daher verfassungswidrig.

Mit der vorgeschlagenen Bestimmung sollen die Finanzstrafbehörden praktisch ohne Einschränkung die Identität eines Teilnehmers hinter einer IP-Adresse ermitteln dürfen. Schon die vorgeschlagene Bestimmung des § 99 Abs. 3a Z 1 FinStrG macht deutlich, dass in der praktischen Ermittlungsarbeit zunächst einmal der Inhalt (eine Nachricht, ein aufgerufener Dienst, ein Eintrag in einem online-Forum, etc) bekannt ist. In einer mehrgliedrigen Ermittlungskette wird dem bekannten Inhalt zunächst eine IP-Adresse zugeordnet, zu der in einem weiteren Schritt der Inhaber des Internet-Anschlusses ausgeforscht wird. Die Befugnis ist daher, wie schon die vergleichbaren Bestimmungen des § 76a Abs 2 StPO sowie § 53 Abs. 3a SPG (nach der SPG Novelle 2007), eher vergleichbar mit den Befugnissen zur Inhaltsüberwachung als an den auf Verkehrsdaten beschränkten Auskünften über Daten einer Nachrichtenübermittlung (vgl. § 135 StPO).

Der Inhalt ist also schon vorher bekannt, bleibt aber ohne die Zugangsdatenauskunft, die erst den Personenbezug herstellt, anonym. Die Information darüber, welchem Teilnehmer eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, stellt sozusagen den „missing link" her, um öffentlich bekannte oder bei einem Dienstanbieter ausgeforschte Kommunikationsinhalte mit einer bestimmten Person zu verbinden. Zwar dürfen Internet-Zugangsanbieter nicht aufzeichnen, welche Internetseiten vom Teilnehmer aufgerufen wurden. Allerdings sind viele Internetseiten bzw -dienste technisch derart konzipiert, dass bei Zugriffen auf diese Seiten oder Dienste die IP-Adresse des Teilnehmers sowie der Zeitpunkt des Zugriffs durch den Host- oder Content-Provider protokolliert und bei manchen Anwendungen auch mit bestimmten Inhalten verknüpft wird (zB bei Einträgen in einem Online-Forum). Bei vielen Online-Diensten existieren auch Aufzeichnungen über das konkrete Nutzungsverhalten (zB Einkäufe bei Amazon.com, EBay, Suchanfragen bei Google, …).

Gleichzeitig lässt sich daraus noch nicht ableiten, ob der Anschlussinhaber auch mit dem Urheber der Kommunikation ident ist. Die Information ist vielmehr bloß ein erster Ermittlungsansatz. Die Zuordnung von Verbindungsdaten (insb IP-Adressen) zu einer bestimmten Person lässt selbst keine Rückschlüsse darüber zu, ob diese Person auch tatsächlich am fraglichen Kommunikationsvorgang beteiligt war. Hierzu bedarf es weiterer konkretisierender Indizien, welche gerade bei der Erforschung von Kommunikationsvorgängen im Internet häufig schwer fassbar sind. Anschaulich lässt sich eine IP-Adresse als eine Art KFZ-Kennzeichen auf dem „Datenhighway" beschreiben. Vielfach wird daher eine Art „IT-Lenkererhebung" erforderlich sein, um Aussagekraft und Zuverlässigkeit der ermittelten Daten beurteilen zu können; denn eine reine Gefährdungshaftung für Inhaber von Internet- oder Telefonanschlüssen ist der österreichischen Rechtsordnung bislang nicht bekannt. Der Aussagekraft und mit ihr verbunden dem tatsächlichen Nutzen der Daten für den angestrebten Zweck kommen für die Verhältnismäßigkeit der behördlichen Befugnisse entscheidende Bedeutung zu, die bereits abstrakt in jeden Abwägungsvorgang mit einzubeziehen sind.

Die Textierung ist offenbar weitgehend der ähnlichen Befugnis aus dem Sicherheitspolizeigesetz nachgebildet, allerdings sogar weniger eingeschränkt als die sicherheitspolizeiliche Befugnis nach §

53 Abs. 3a SPG. Dort besteht zumindest die formale Einschränkung, dass die Ermittlung durch die Sicherheitsbehörden nur dann zulässig ist, „wenn dies zur Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben erforderlich ist.“ Die hier vorgeschlagene Bestimmung enthält nicht einmal diese rudimentäre Zweckbindung, die sich allerdings schon aus dem DSG 2000 ergibt.

Unabhängig davon ist die pauschale Ausweitung der Befugnisse von Sicherheitsbehörden auf Finanzstrafbehörden – ohne Beschränkung auf den Bereich des gerichtlichen Finanzstrafrechts – unverhältnismäßig. Das SPG ist im Vergleich dazu „strafrechtsakzessorisch“, das bedeutet, dass die vergleichbaren Befugnisse nach § 53 Abs. 3a SPG nur im Hinblick auf einen „gefährlichen Angriff“ statthaft sind. Ein solcher liegt aber nach § 16 SPG im Wesentlichen nur vor bei der „Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die vorsätzlich begangen“ wird und nicht nur ein Privatanklagedelikt darstellt. Darüber hinaus lässt das SPG Auskünfte zu IP-Adressen nur in den Fällen der ersten allgemeinen Hilfeleistung zu, wobei hier ausdrücklich eine konkrete Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen bestehen muss.

Im Gegensatz dazu fehlt den hier vorgeschlagenen Ermittlungsbefugnissen nach dem FinStrG jegliche Einschränkung im Hinblick auf eine gewisse Schwere und Bedeutung der Sache. Zur Vermeidung von Wiederholungen wird insofern auf die Ausführungen oben zu Z 1 der Novelle verwiesen.

Darüber hinaus erfüllt der nach § 58 Abs. 2 FinStrG zur Anordnung der Maßnahme berufene Spruchsenat als Organ der Finanzstrafbehörde nicht die Voraussetzungen einer unabhängigen Kontrolleinrichtung, um im Einzelfall angemessene Sicherungen zur Wahrung der Verhältnismäßigkeit zu garantieren. In diesem Sinne hat der VfGH mit Urteil vom 23.1.2004 zu G363/02 Teile des § 22 Militärbefugnisgesetz (MBG) als verfassungswidrig aufgehoben, weil den dort normierten Ermittlungs- und Überwachungsbefugnisse keine ausreichenden Rechtsschutzgarantien zur Seite gestellt waren. Der selbe Befund trifft auch auf die gegenständlich vorgeschlagenen Befugnisse zu.

Schließlich ist zu bedenken, dass die gegenständlichen IP-Adressen in § 92 Abs. 3 Z 26 TKG als Zugangsdaten und damit als Unterfall der Verkehrsdaten vom Schutz des Kommunikationsgeheimnisses nach § 93 TKG erfasst sind. Eine Konsequenz daraus ist insbesondere, dass die Übermittlung solcher Daten nach § 99 Abs. 1 TKG nur zulässig sind, wenn zu der jeweiligen gesetzlichen Auskunftsbefugnis im TKG selbst eine korrespondierende Norm diese Übermittlung grundsätzlich zulässt. Das im TKG geschaffene System der abschließenden Aufzählung der Fälle zulässiger Datenverwendung soll Rechtssicherheit schaffen und dient dem datenschutzrechtlichen Transparenzgebot. Eine Regelung wie die hier vorgeschlagene ohne korrespondierende Novellierung im TKG wäre schon deshalb im Ergebnis unwirksam, weil § 99 TKG hierzu als lex spezialis zu sehen ist.

Daneben müsste für solche Auskunftsbefugnisse für die Finanzstrafbehörden auch ein Zugang über die „Durchlaufstelle“ nach der Datensicherheitsverordnung zum TKG geschaffen werden, um die speziellen Datensicherheitsanforderungen zum Schutz des Fernmelde- und Kommunikationsgeheimnisses zu wahren.

Nach Auffassung des AKVorrat ist die vorgeschlagene Bestimmung zu Ziffer 4 b) der Novelle daher als verfassungswidrig abzulehnen.

5. § 120 wird wie folgt geändert:

(…)

c) In Abs. 3 werden folgende Sätze angefügt:

„Darüber hinaus sind die Finanzstrafbehörden berechtigt, auf automationsunterstütztem Wege Einsicht in das elektronische Kriminalpolizeiliche Informationssystem (EKIS) zu nehmen. Die Sicherheitsbehörden haben den Finanzstrafbehörden auch sonstige personenbezogene Daten, insbesondere solche, die in der zentralen Informationssammlung gemäß § 57 des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991, erfasst sind, zu übermitteln, soweit diese für die Durchführung eines Finanzstrafverfahrens erforderlich sind."

Nach Ansicht des AKVorrat stellt diese Befugnis im Falle ihres Inkrafttretens einen unverhältnismäßigen Eingriff in das Grundrecht auf Datenschutz gem. § 1 DSG 2000 sowie in das Grundrecht auf Privatsphäre gem. Art. 8 EMRK und wäre daher verfassungswidrig.

Wie bereits die Datenschutzbehörde in ihrer Stellungnahme ausführt, scheint der vorliegende Entwurf – im Gegensatz zur Übermittlung von Daten aus der zentralen Informationssammlung – einen völlig uneingeschränkten Zugriff der Finanzstrafbehörden auf das Polizeisystem EKIS zu ermöglichen. Wie die Datenschutzbehörde vertritt auch der AKVorrat die Ansicht, dass dies im Widerspruch zum verfassungsgesetzlich normierten Grundsatz der Verhältnismäßigkeit bei Eingriffen in das Grundrecht auf Datenschutz steht.

Völlig richtig hebt die Datenschutzbehörde in ihrer Stellungnahme hervor, dass der Verfassungsgerichtshof verlangt, dass eine Ermächtigungsnorm iSd § 1 Abs. 2 DSG 2000 ausreichend präzise, also für jedermann vorhersehbar, bezeichnet, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung der Daten für die Wahrnehmung konkreter Verwaltungsaufgaben zulässig ist (vgl. VfSlg. 16.369/2001). Der jeweilige Gesetzgeber muss somit iSd § 1 Abs. 2 DSG 2000 eine materienspezifische Regelung in dem Sinn vorsehen, dass die Fälle zulässiger Eingriffe in das Grundrecht auf Datenschutz konkretisiert und begrenzt werden.

Der AKVorrat schließt sich hierzu der Sicht der Datenschutzbehörde an, dass daher dafür Sorge zu tragen wäre, dass die Finanzstrafbehörden nur Einsicht in jene Daten erhalten, die sie für die Führung von Finanzstrafverfahren unbedingt benötigen, keinesfalls aber einen uneingeschränkten Pauschalzugriff. Im Übrigen wird zur Vermeidung unnötiger Redundanz auf die Argumentation der Datenschutzbehörde verwiesen.

Fazit

Abschließend äußert der AKVorrat Bedenken an der Praxis des Gesetzgebers, weitgehende Überwachungsbefugnisse in Beigesetzen zu verankern. In diesem Zusammenhang soll auf die Novelle des Verwaltungsgerichtsbarkeits-Begleitgesetz-Wehrrecht – VwGBG-W vom Februar 2013 erinnert werden, mit welchem dem Militärgeheimdienst Zugriff auf Foren und Vorratsdaten ermöglicht werden sollte[1]. Durch diese Praxis entsteht der Eindruck grundlegende Befugnisse des Staates, welche das Grundrecht auf Datenschutz einschränken und das Gleichgewicht zwischen Freiheit und Sicherheit verändern, abseits einer öffentlichen Diskussion verankern zu wollen.

[1] Siehe http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00469/index.shtml und http://www.unwatched.org/20130206_Vorratsdaten_und_Forenueberwachung_fuer_Militaergeheimdienste