

REPUBLIK ÖSTERREICH ■ DATENSCHUTZ RAT

BALLHAUSPLATZ 2, A-1014 WIEN

GZ • BKA-817.386/0003-DSR/2010

TELEFON • (+43 1) 53115/2527

FAX • (+43 1) 53115/2702

E-MAIL • DSRPOST@BKA.GV.AT

DVR: 0000019

An das
Präsidium des Nationalrates
Parlament
PerMail:'begutachtungsverfahren
@parlament.gv.at'

**Betreff: Stellungnahme des Datenschutzrates
Entwurf eines Bundesgesetzes, mit dem das
Telekommunikationsgesetz 2003 (TKG 2003) geändert werden soll
(Umsetzung der Vorratsdatenspeicherungs-Richtlinie 2006/24/EG)**

In der Anlage wird die Stellungnahme des Datenschutzrates zu dem im Betreff genannten Gesetzesentwurf übermittelt.

Anlage

15. Jänner 2010
Für den Datenschutzrat:
Der Vorsitzende:
MAIER

Elektronisch gefertigt

REPUBLIK ÖSTERREICH ■ **DATENSCHUTZRAT**

BALLHAUSPLATZ 2, A-1014 WIEN
GZ • BKA-817386./0003-DSR/2010
TELEFON • (+43 1) 53115/2527
FAX • (+43 1) 53115/2702
E-MAIL • DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für Verkehr,
Innovation und Technologie

Per Mail:
'maria-theresia.roehsler@bmvit.gv.at'
alfred.stratil@bmvit@gv.at
christian.singer@bmvit.gv.at

**Betrifft: Stellungnahme des Datenschutzrates
Entwurf eines Bundesgesetzes, mit dem das
Telekommunikationsgesetz 2003 (TKG 2003) geändert werden soll
(Umsetzung der Vorratsdatenspeicherungs-Richtlinie 2006/24/EG)**

Der **Datenschutzrat** hat in seiner 193. Sitzung am 14. Jänner 2010 **einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Allgemeines

Mittels vorgelegtem Ministerialentwurf für eine Novelle des TKG 2003 soll die „Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden [...] im innerstaatlichen Bereich umgesetzt werden.

Nicht zuletzt mit Blick auf die **Grundrechtssensibilität** der Materie und die sich daraus resultierenden rechtlichen und politischen Implikationen hat sich Österreich außer Stande gesehen, die mit 15. September 2007 abgelaufene Umsetzungsfrist zu

wahren. In einem Teilbereich bestand gemäß Art. 15 Abs. 3 der RL 2006/24/EG die Möglichkeit, mittels Erklärung deren Anwendung betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail bis 15. März 2009 zurückzustellen. Davon hat Österreich Gebrauch gemacht.

Inzwischen ist gegen Österreich ein **Vertragsverletzungsverfahren** nach Art. 226 EGV wegen Versäumung der Umsetzungsfrist beim Gerichtshof der EG anhängig. Aktuell ist Österreich aufgefordert, bis zum 24. Dezember 2009 zu einer Erwiderung der Europäischen Kommission vom 12. Oktober 2009 Stellung zu nehmen.

Der nunmehr vorliegende Entwurf für eine Novelle des TKG 2003 soll sowohl den Umsetzungspflichten aus der besagten RL Rechnung tragen, als auch dazu beitragen, ein im Anschluss an eine Verurteilung durch den Gerichtshof wegen Nichtumsetzung potentiell zusätzlich drohendes kostspieliges Sanktionsverfahren gemäß Art. 228 Abs. 2 EGV zu vermeiden.¹

II. Zur Datenschutzproblematik im Allgemeinen

Die Richtlinie 2006/24/EG zielt - vereinfacht gesagt - darauf ab, die **Telekommunikationsdaten** (inkl. Standortdaten beim Mobilfunk) der **gesamten Bevölkerung unabhängig von betriebs- oder verrechnungstechnischen Erfordernissen** bzw. länger als dies für solche Zwecke erforderlich zu **speichern**. Dies soll der Erleichterung der nachträglichen Ermittlung, Feststellung und Verfolgung von „schweren Straftaten“ dienen.

Gem. Art. 8 der seit 1. Dezember 2009 in Kraft befindlichen Charta der Grundrechte der Europäischen Union (kurz: GRC) dürfen „personenbezogene Daten nur nach Treu und Glauben **für festgelegte Zwecke** und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden“. Schon vor dem Inkrafttreten der GRC ergab sich dieser Grundsatz insbesondere aus Art. 5 lit. b der Datenschutz-Konvention des Europarates sowie Art. 6 Abs. 1 lit. b EG-DSRL.

¹ Letzteres Verfahren ermöglicht es der Kommission, gegen Mitgliedstaaten wegen Nichtbeseitigung eines mit einem Urteil des Gerichtshofes festgestellten Vertragsverstoßes (hier: der Nichtumsetzung einer RL) vorzugehen. Trifft ein Mitgliedstaat die sich aus dem Urteil ergebenden Maßnahmen nicht innerhalb der von der Kommission zur Beantwortung ihrer mit Gründen versehenen Stellungnahme festgelegten Frist, kann die Kommission wiederum eine Klage gemäß Art. 228 Abs. 2 UAbs. 2 EGV beim Gerichtshof erheben. Zutreffendenfalls beantragt sie in der Klage die Höhe des von dem betreffenden Mitgliedstaat zu zahlenden Pauschalbetrages oder Zwangsgeldes, die sie den Umständen nach für angemessen hält. Der feste Mindestpauschalbetrag beträgt für Österreich € 2.420.000,- (Näheres zum Sanktionsverfahren nach Art. 228 EGV in Rundschreiben BKA-670.746/0008-V/7/2009).

Wesentlich ist, dass der/die **Zweck(e)** einer Datenverwendung **ausreichend konkret** sein und **im Vorhinein** feststehen müssen.

Die Anordnung einer Speicherpflicht von Telekommunikationsdaten ohne Bezug zu einer Straftat und dies für die Gesamtheit der Kommunikationsteilnehmer scheint mit den vorgenannten Grundsätzen insbesondere im Hinblick auf den Grundsatz der Verhältnismäßigkeit in einem Spannungsverhältnis zu stehen.

Hinsichtlich der Vereinbarkeit derartiger Datenspeicherungen mit Art. 8 der Europäischen Menschenrechtskonvention (EMRK) scheint insbesondere die jüngste Rsp des Gerichtshofs für Menschenrechte von Relevanz:

In seinem Urteil in der Rs. S. und Marper vom 4.12.2008 gelangt der EGMR – im Kontext der staatlichen Speicherung von erkennungsdienstlichen Daten – zum Schluss, dass die umfassende und wahllose Befugnis zur Speicherung von Fingerabdrücken, Zellproben und DNA-Profilen **von verdächtigten, aber nicht verurteilten Personen, keinen gerechten Ausgleich** zwischen den widerstreitenden **öffentlichen und privaten Interessen trifft** und der belangte Staat in dieser Hinsicht jeden akzeptablen Ermessensspielraum überschritten hat. Die umstrittene Speicherung begründe daher einen **unverhältnismäßigen Eingriff** in das Recht auf Achtung des Privatlebens, der nicht als in einer demokratischen Gesellschaft notwendig angesehen werden kann. Daher stellte der EGMR in diesem Fall einstimmig eine Verletzung von Art. 8 EMRK fest. Das Urteil ist im vorliegenden Zusammenhang deshalb **von besonderem Gewicht, weil selbst die Speicherung personenbezogener Daten von Personen, die einmal im Verdacht standen, eine strafbare Handlung begangen zu haben, vom EGMR als Verletzung des Art. 8 EMRK betrachtet wird**. Umso mehr ist nicht auszuschließen, dass aus Sicht des EGMR die völlig verdachtsunabhängige Speicherung von Vorratsdaten eine Verletzung dieses Konventionsrechts bewirken könnte.

Auf diesen Aspekt hat die Republik Österreich im Übrigen auch im Rahmen des von der Kommission gegen Österreich angestrengten Vertragsverletzungsverfahrens (siehe im Vorabschnitt) ausdrücklich hingewiesen.

Eine verbindliche Feststellung hinsichtlich der Vereinbarkeit der Vorratsdatenspeicherungs-RL mit dem (seit 1. 12. 2009 auf Grund des Vertrags von Lissabon verbindlichen) Art. 8 GRC bzw. Art. 8 EMRK bleibt freilich dem EuGH anheimgestellt. Soweit die RL 2006/24/EG den Mitgliedstaaten einen Spielraum überlässt, nämlich hinsichtlich der Nutzung gespeicherter Daten für die Aufklärung

von anderen als „schweren“ Straftaten, obläge die Klärung der Vereinbarkeit einer bezüglichen Speicherpflicht bzw. einschlägiger Nutzungsmöglichkeiten den Verfassungsgerichten.

III. Zur bisherigen Positionierung des Datenschutzrates

Vor dem obigen Hintergrund bzw. im Lichte der einschlägigen internationalen und nationalen Rechtsgrundlagen zum Datenschutz und zur Privatsphäre, wie sie schon vor Inkrafttreten der GRC zu beachten waren, hat der Datenschutzrat bereits im **September 2002** festgehalten, „dass die Frage der Verhältnismäßigkeit einer zwingenden Anordnung der flächendeckenden Speicherung von Verkehrsdaten für Zwecke der Strafverfolgung über jenen Zeitraum hinaus, in dem sie für die Übertragung der Nachricht oder für die Gebührenabrechnung und die Bezahlung von Zusammenschaltungen notwendig sind, [...] in keiner Weise geklärt“ sei und sich gegen eine Zustimmung zu einer derartigen Regelung ausgesprochen“.² Diese Haltung hat der Datenschutzrat im **Juni 2004** einstimmig bekräftigt.³

Mit Beschluss vom **20. Oktober 2005** stellte der Datenschutzrat dann fest, „**dass eine anlasslose, verdachtsunabhängige undifferenzierte Speicherung des Telekommunikationsverhaltens der Gesamtbevölkerung wohl, unabhängig von der Speicherdauer, als eine unverhältnismäßige Maßnahme einzustufen und als solche mit Art. 8 EMRK und § 1 Abs. 2 DSG 2000 unvereinbar ist**“. „Eine lückenlose Strafverfolgung würde vermutlich auch durch das Instrument der zwangsweisen Vorratsdatenspeicherung nicht erreicht, da offenbar auch technische Umgehungsmöglichkeiten bestehen“.⁴ **Strikt abgelehnt wurde damals die durchgehende Dokumentation von Standortdaten von Mobilfunkgeräten, da dies die Erstellung von detaillierten Bewegungsprofilen ermöglichen würde. Ebenso striktest abgelehnt wurde die Einbeziehung von Inhaltsdaten wie sie beim Surfen im Internet oder bei der Kommunikation in sog. Chatrooms anfallen. Und abgelehnt hat der Datenschutzrat schließlich auch eine Einbeziehung der „Prävention“ als Speicherzweck.**⁵ Zudem abgelehnt wurde die

² Beschluss des Datenschutzrates vom 2. September 2002, GZ 817.222/006-DSR/2002, betreffend die vorhaltende Speicherung von Verkehrsdaten für Zwecke der Strafverfolgung.

³ Vgl. TOP 4 des Beschlussprotokolls der 170. Sitzung des Datenschutzrates am 15. Juni 2004, Seite 16.

⁴ Vgl. Stellungnahme des Datenschutzrates vom 20. Oktober 2005, GZ 817.222/0010-DSR/2005, zur Frage der sog. Vorratsdatenspeicherung, Seite 3.

⁵ Vgl. ebenda, Seiten 3 und 4.

zusätzliche Speicherung von Daten durch die Provider, die von diesen nicht schon für betriebstechnische Zwecke erzeugt werden oder nicht bei ihnen anfallen.⁶

Auch nach der Verabschiedung RL 2006/24/EG bekräftigte der DSR anlässlich seiner 175. Sitzung am 16. Mai 2007 in seiner Stellungnahme zur damals geplanten TKG-Novelle zur Umsetzung der Vorratsdatenspeicherung neuerlich seine Bedenken gegenüber der flächendeckenden Speicherung von Vorratsdaten für Zwecke der Strafverfolgung.

Er merkte explizit an, „dass die anlasslose, verdachtsunabhängige undifferenzierte Speicherung des Telekommunikationsverhaltens der Gesamtbevölkerung, unabhängig von der Speicherdauer, Fragen der Verhältnismäßigkeit und der Vereinbarkeit solcher Maßnahmen mit Art. 8 EMRK und § 1 Abs. 2 DSG 2000 aufwirft“.⁷

Hervorgehoben hat der Datenschutzrat bei dieser Gelegenheit, dass **im Rahmen der innerstaatlichen Umsetzung der ursprüngliche Zweck und Anlass für die Erlassung der Richtlinie zu beachten sei, nämlich die Bekämpfung von Terrorismus und organisierter Kriminalität** (vgl. Erwägungsgründe 7, 8, 9, 10 der RL 2006/24/EG). Der dem nationalen Gesetzgeber verbleibende rechtspolitische Gestaltungsspielraum müsse insbesondere den datenschutzrechtlichen Grundsätzen der Zweckbindung sowie der Verhältnismäßigkeit Rechnung tragen.⁸

IV. Allgemeine Bemerkungen zum vorliegenden Entwurf

- Der Datenschutzrat begrüßt, dass das BMVIT angesichts der Sensibilität der Materie das Ludwig Boltzmann Institut für Menschenrechte beauftragt hat, einen Entwurf auszuarbeiten. Der darauf beruhende nunmehr zur Begutachtung ausgesendete Entwurf scheint vom Bemühen des BMVIT getragen, bei der Umsetzung der RL 2006/24/EG bezüglich der Eingriffstiefe grundsätzlich nicht über das von der RL geforderte Mindestmaß hinsichtlich der Speicherfrist und des Anwendungsumfanges hinauszugehen. In diesem Zusammenhang ist zu bemerken, dass über das Mindestmaß hinausgehende Umsetzungen in anderen Mitgliedstaaten starke Kritik erfahren haben und zT durch die Judikatur eingeschränkt oder

⁶ Vgl. ebenda.

⁷ Vgl. Beschluss des Datenschutzrates vom 16. Mai 2007, GZ BKA-817.304/0003-DSR/2007, betreffend TKG-Novelle zur Umsetzung der Richtlinie über Vorratsdatenspeicherung, Seite 1.

⁸ Vgl. ebenda, Seite 2.

aufgehoben wurden: So setzte zB das deutsche Bundesverfassungsgericht das überschießende Umsetzungsgesetz aus und ordnete per einstweiliger Verfügung an, dass die Verwendung nur für die Bekämpfung schwerer Straftaten möglich sein darf (Beschluss 1 BvR 256/08). Weiters ist die rumänische Umsetzung der Vorratsdatenspeicherungsrichtlinie vom Verfassungsgericht in Bukarest für verfassungswidrig erklärt worden.

Ein wesentlicher Gesichtspunkt jedes staatlichen Informationseingriffs ist – abgesehen von dessen Verhältnismäßigkeit im allgemeinen – die Relation zwischen der jeweiligen Eingriffstiefe bzw. –breite einerseits und den gleichzeitig in Betracht kommenden unabhängigen Kontrollinstanzen sowie wirksamen Rechtsschutzinstrumenten andererseits. Als unbestritten gilt, dass eine ununabhängige Kontrolle am ehesten durch Gerichte oder vergleichbare gerichtsförmige Einrichtungen gewährleistet werden kann.

Eingriffe in das verfassungsgesetzlich gewährleistete Fernmeldegeheimnis sind zufolge Art. 10a StGG nur auf Grund einer richterlichen Genehmigung zulässig.

Nach dem vorliegenden Entwurf soll allerdings gemäß §§ 98 Abs. 2 und 99 Abs. 5 Z 2 eine Nutzung von Kommunikationsdaten in bestimmten Fällen („Gefahrenabwehr“) auch ohne eine solche gerichtliche Genehmigung zulässig sein. Der Entwurf schlägt daher – offenbar zur Herstellung der Verfassungskonformität – vor, §§ 98 Abs. 2 und 99 Abs. 5 Z 2 TKG im Verfassungsrang zu beschließen.

Der Datenschutzrat weist in diesem Zusammenhang darauf hin, dass Judikatur des Verfassungsgerichtshofes zur hier gegenständlichen Frage der Reichweite des Schutzbereiches des Fernmeldegeheimnisses gemäß Art. 10a StGG bis dato nicht existiert. Auch in der Literatur werden zu dieser Frage unterschiedliche Auffassungen vertreten. Auch hat der Datenschutzrat zur Kenntnis genommen, dass die Bundesregierung in ihrer Äußerung im Verfahren vor dem Verfassungsgerichtshof G 31/08 vom 7. Mai 2008 die Auffassung vertreten hat, dass der Schutzbereich des Fernmeldegeheimnisses nur den Inhalt der Kommunikation, nicht jedoch die Verbindungsdaten, erfasst.

Vor diesem Hintergrund sieht sich der Datenschutzrat derzeit außer Stande, abschließend die Notwendigkeit zur Erlassung der beiden genannten Bestimmungen als Verfassungsbestimmungen zu beurteilen.

Zugleich hält der Datenschutzrat fest, dass sich die oben angesprochene Grundsatzfrage eines ausgewogenen Verhältnisses zwischen Ermächtigungen für staatliche Informationseingriffe und adäquaten Kontroll- und Rechtsschutzinstrumentarien aber auch unabhängig von der Frage der inhaltlichen Reichweite des verfassungsgesetzlich gewährleisteten Fernmeldegeheimnisses stellt.

Unbeschadet dessen legen es die seit dem Inkrafttreten des Art 10a StGG (1. Jänner 1975) eingetretenen rasanten technologischen Entwicklungen auf dem Gebiete des Fernmeldewesens (Digitalisierung, Mobilfunkdienste; Multimedia-Anwendungen etc) nahe, sich grundsätzlich mit der Frage einer möglichen Weiterentwicklung bzw. Neubewertung dieser Norm zu befassen. Nur auf diesem Wege kann möglicherweise gewährleistet werden, dass das verfassungsrechtliche Fernmeldegeheimnis seiner Funktion im Zeitalter der elektronischen Massenkommunikation gerecht werden kann.

Was den gegenständlichen Entwurf einer TKG-Novelle betrifft, so bedürfte es im Übrigen unter dem Gesichtspunkt der Datenschutzlegistik bzw. dem der möglichst „grundrechtsschonenden“ Umsetzung diverser Nachbesserungen.

2. Der Datenschutzrat bedauert, dass es keinen abgestimmten Begutachtungsentwurf zwischen den mit diesen Fragen befassten Bundesministerien gibt. Damit sind wesentliche Fragen offen. So ist weiter strittig, ob die Umsetzung der Vorratsdatenspeicherungs-Richtlinie auch Änderungen des Sicherheitspolizeigesetzes (SPG), der Strafprozessordnung (StPO) und anderer Materiengesetze erfordert.

Bekannt gewordene Forderungen des Bundesministeriums für Inneres (Schreiben vom 11.1.2010) und des Bundesministeriums für Justiz (Schreiben vom 13.1.2010) gehen über die Vorratsdatenspeicherungs-Richtlinie (2006/24/EG) hinaus und können daher nicht Gegenstand des derzeitigen Begutachtungsverfahrens sein. Dasselbe gilt für Problemstellungen, die sich nach der Entscheidung des Obersten Gerichtshofes vom 14.7.2009 (4 Ob 41/09x - LSG/Tele2) wegen einer fehlenden Rechtsvorschrift und dem Speicherverbot nach dem TKG hinsichtlich des

Auskunftsanspruches zur Rechtsverfolgung von Eingriffen in Urheber- und Leistungsschutzrechte im Internet ergeben.

Eine Verarbeitung und Speicherung von Verkehrsdaten zu anderen Zwecken auf Basis einer anderen Rechtsgrundlage als der Richtlinie zur Vorratsdatenspeicherung müsste gesondert – außerhalb dieses Gesetzesvorhabens – geregelt werden.

Der Datenschutzrat verkennt nicht die Notwendigkeit der ausreichenden Erfüllung sicherheitspolizeilicher Aufgaben und strafrechtlicher Ermittlungen und Kontrollen. Entscheidend ist dabei, dass diese in rechtsstaatlich einwandfreier Form erfolgen und je nach Eingriffsintensität der Rechtsschutz Betroffener und die Informationsverpflichtungen ausgebaut werden. Zu prüfen ist daher, in welcher Form und in welchem Umfang die durch die zit. Entscheidung des OGH vorliegenden Beschränkungen von Ermittlungen durch geeignete gesetzliche Maßnahmen ausgeglichen werden können.

Die Stellungnahme des Datenschutzrates zum gegenständlichen Gesetzesvorhaben muss sich daher in Anbetracht dieser Situation auf die Umsetzung der Vorratsdatenspeicherungs-Richtlinie beschränken. Zu anderen diskutierten und gewünschten Regelungen kann vom Datenschutzrat erst dann Stellung genommen werden, wenn zwischen den Ressorts abgestimmte und ausformulierte Gesetzesvorschläge vorgelegt werden.

V. Schlussfolgerungen

Gestützt auf seine Überlegungen in den Vorabschnitten

- erinnert der Datenschutzrat an seine bisherigen Äußerungen und Beschlüsse;
- betont der Datenschutzrat, dass in einem liberalen demokratischen Rechtsstaat die Wahrung eines angemessenen Gleichgewichts zwischen dem Recht auf Privatsphäre und dem öffentlichen Interesse an der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit sowie einer angemessenen Verfolgung von Straftaten bedingt, dass mit der Ermittlung personenbezogener Daten verbundene Ermittlungs- bzw. Verfolgungsmaßnahmen grundsätzlich nur bei Vorliegen von ausreichend konkreten Verdachtsmomenten gesetzt werden dürfen;

- vertritt der Datenschutzrat auch vor diesem Hintergrund weiterhin die Auffassung, dass das Instrument der Vorratsdatenspeicherung mit Art. 8 EMRK sowie mit Art. 8 der Europäischen Grundrechtecharta, insbesondere unter den Gesichtspunkten der Eignung und Verhältnismäßigkeit, in einem gravierenden Spannungsverhältnis steht;
- betont der Datenschutzrat, dass sich insbesondere aus dem Verhältnismäßigkeitsgebot die Forderung ergibt, den bei der Umsetzung der RL 2006/24/EG verbleibenden Gestaltungsspielraum dafür zu verwenden, die mit der Anordnung einer Vorratsdatenspeicherung einhergehenden Grundrechtseingriffe möglichst zu begrenzen;
- begrüßt der Datenschutzrat den Vorschlag des BMVIT soweit dieser den Versuch unternimmt, sich hinsichtlich der grundrechtsbelastenden Anordnungen auf eine „Mindestumsetzung“ der RL 2006/24/EG zu beschränken;
- betont der Datenschutzrat zugleich das Erfordernis einer möglichst restriktiven Definition „schwerer Straftaten“, die sich am grundsätzlichen Ziel und Zweck der Vorratsdatenspeicherrichtlinie (der Bekämpfung organisierter Kriminalität und des Terrorismus) orientiert;
- bekräftigt der Datenschutzrat in diesem Zusammenhang seine Einschätzung der generellen Einbeziehung von Vergehen, die ausschließlich im Wege der Telekommunikation begangen werden, in den Kreis jener Straftaten, zu deren Verfolgung auf Vorratsdaten zurückgegriffen werden darf, als unverhältnismäßig iSd Art. 1 Abs. 2 DSG 2000 (sowie auch des Art. 8 EMRK);
- ist der Datenschutzrat der Auffassung, dass das Schutzniveau für Betroffene, in deren Kommunikations- bzw. Fernmeldegeheimnis eingegriffen wird, grundsätzlich nicht davon abhängen darf, ob der Eingriff aus präventiven oder repressiven Gründen erfolgt; diesbezüglich ist insbesondere sicherzustellen, dass etwa das Schutzniveau nach der Strafprozessordnung in der Praxis nicht durch ein willkürliches Ausweichen auf Befugnisse nach anderen Materiengesetzes unterlaufen werden kann;
- ist der Datenschutzrat der Auffassung, dass die Verarbeitung und Speicherung von Verkehrsdaten zu anderen Zwecken und damit auf Basis einer anderen Rechtsgrundlage als in der Richtlinie zur Vorratsdatenspeicherung angesprochen gesondert – außerhalb des hier diskutierten Gesetzesvorhabens (TKG) – geregelt werden müsste;

- verkennt der Datenschutzrat nicht die Notwendigkeit ausreichender Instrumente für strafrechtliche Ermittlungen sowie zur polizeilichen Aufgabenerfüllung, sofern diese in rechtsstaatlich einwandfreier Form eingesetzt werden und sofern je nach Eingriffsintensität der Rechtsschutz Betroffener und die Informationsverpflichtungen ausgebaut werden;
- ist der Datenschutzrat der Überzeugung, dass insbesondere im Lichte des Instruments der Vorratsdatenspeicherung Begleitmaßnahmen erforderlich erscheinen, um das Bewusstsein der zuständigen Organe in den Sicherheitsbehörden und in der Justiz für die Sensibilität von Eingriffen in das Fernmeldegeheimnis zu stärken und so einen verhältnismäßigen Einsatz der bezüglichen Instrumente zu gewährleisten;
- macht der Datenschutzrat darauf aufmerksam, dass die Vorratsdatenspeicherung in Verbindung mit bereits bestehenden Überwachungsmöglichkeiten geeignet erscheint, die Arbeitsgrundlage bestimmter Berufsgruppen (insbesondere Journalisten) in Frage zu stellen (Stichwort: „Informantenschutz“, Redaktionsgeheimnis). Er regt daher dringend an, begleitend zur Umsetzung der Vorratsdatenspeicherrichtlinie zu untersuchen, inwieweit den angesprochenen Bedrohungen auch durch gesetzgeberische Maßnahmen entgegengewirkt werden kann;
- ist sich der Datenschutzrat bewusst, dass die Vorratsdatenspeicherung mit beachtlichen kostenmäßigen Mehrbelastungen für die Telekommunikationswirtschaft einhergeht und deshalb der Frage staatlicher Kompensationen besondere Bedeutung beizumessen ist;
- weist der Datenschutzrat darauf hin, dass mit 1. Dezember 2009 die Charta der Grundrechte der Europäischen Union (kurz: GRC) in Kraft getreten und zum Bestandteil des sog. Primärrechts geworden ist. Damit ist insbesondere deren Art. 8 („Schutz personenbezogener Daten“) als verbindlicher Maßstab zur Beurteilung der Gemeinschaftsrechtskonformität der Vorratsdatenspeicherrichtlinie heranzuziehen;
- hält der Datenschutzrat - entsprechend der in Punkt 1.2.5. des Stockholmer Programmes geäußerten Forderung einer Bewertung von Rechtsakten der Union eine Evaluierung der RL 2006/24/EG auf europäischer Ebene – allenfalls auch mit dem möglichen Ergebnis einer Aufhebung der RL – für angebracht. Die zuständigen Bundesminister/innen sollen daher in diesem Sinn eine Bewertung der Vorratsdatenspeicherungsrichtlinie insbesondere hinsichtlich ihrer Eignung zur

Bekämpfung organisierter Kriminalität und des Terrorismus und der Verhältnismäßigkeit der Maßnahmen auf europäischer Ebene anregen.

- Die Stellungnahme des Datenschutzrates zum gegenständlichen Gesetzesvorhaben beschränkt sich mangels ergänzender abgestimmter Gesetzesvorschläge aus dem Bundesministerium für Inneres und dem Bundesministerium für Justiz auf die Umsetzung der Vorratsdatenspeicherungs-Richtlinie und bleibt allgemein gehalten.
- Der Datenschutzrat fordert daher die fachzuständigen Ressorts auf, auf der Grundlage des vorliegenden Begutachtungsentwurfs einer TKG-Novelle ein abgestimmtes legistisches Gesamtpaket (Stichworte: StPO, SPG, UrhG) zu erstellen, welches in Ergänzung des bzw. in Abstimmung mit dem TKG die offenen Rechtsprobleme auf dem Felde der Speicherung und Nutzung von Telekommunikationsdaten für andere Zwecke als zur Erbringung der Telekommunikationsdienstleistungen klärt. Der Datenschutzrat hält es für unverzichtbar, dass er auch mit dem überarbeiteten und abgestimmten legistischen Paket rechtzeitig vor der Beschlussfassung einer Regierungsvorlage befasst wird, um eine qualifizierte Diskussion zu führen und eine fundierte Stellungnahme abgeben zu können.

15. Jänner 2010
Für den Datenschutzrat:
Der Vorsitzende:
MAIER

Elektronisch gefertigt